HACIA UN NUEVO MARCO JURÍDICO EUROPEO DE LA PROTECCIÓN DE DATOS PERSONALES*

ANTONIO TRONCOSO REIGADA

Profesor Titular de Derecho Constitucional. Universidad de Cádiz

Revista Española de Derecho Europeo 43
Julio-Septiembre 2012
págs. 25 a 184

SUMARIO: I. PRIMACÍA Y EFECTO DIRECTO DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES DE LA UNIÓN EUROPEA. LA OBLIGACIÓN DE INAPLICACIÓN Y LA DEROGACIÓN DE LAS NORMAS DE DERECHO INTERNO INCOMPATIBLES CON EL DERECHO DE LA UNIÓN. II. LA NECESIDAD DE UN NUEVO MARCO NORMATIVO EUROPEO. III. LA PROTECCIÓN DE DATOS PERSONALES EN UN MUNDO GLOBALIZADO E INTERCONECTADO. IV. LAS DIVERGENCIAS EN LA PROTECCIÓN DE LOS DATOS PERSONALES ENTRE LOS ESTADOS MIEMBROS. V. UN NUEVO MARCO JURÍDICO COHERENTE Y HOMOGÉNEO DE PROTECCIÓN DE DATOS: LA PROPUESTA DE REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS. VI. REFLEXIÓN FINAL.

I. PRIMACÍA Y EFECTO DIRECTO DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES DE LA UNIÓN EUROPEA. LA OBLIGACIÓN DE INAPLICACIÓN Y LA DEROGACIÓN DE LAS NORMAS DE DERECHO INTERNO INCOMPATIBLES CON EL DERECHO DE LA UNIÓN

* La primera parte de este estudio trata de mostrar los motivos principales que justifican la modificación del marco normativo europeo de protección de datos personales, es decir, cuáles son las razones que nos han llevado hasta aquí. La segunda parte se centra en examinar las novedades que presenta la propuesta de Reglamento general de protección de datos personales, en relación con la Directiva 95/46/CE y con la legislación de los países de la Unión Europea. Este estudio no pretende abordar un análisis en profundidad de los principios y derechos de protección de datos personales –y de los problemas que estos plantean en algunos supuestos–, no sólo porque excedería del objeto del presente trabajo, sino porque el autor de estas páginas ya lo ha hecho en el tratado *La protección de datos personales. En busca del equilibro*, Tirant lo Blanch, Valencia, 2010, 1.990 páginas, que recibió el Premio de Investigación de la AEPD del Ministerio de Justicia de ese año.

RESUMEN: La Comisión Europea ha aprobado una Propuesta de Reglamento General de Protección de Datos, que derogará la actual Directiva 95/46/CE y desplazará las leyes de los Estados miembros. Este estudio analiza las principales razones para impulsar la aprobación de este nuevo marco normativo europeo: la aprobación del Tratado de Lisboa; los profundos cambios que han vivido las TICs en los últimos años, con la aparición de Internet y de las redes sociales virtuales; las divergencias en la protección de datos personales entre los diferentes Estados miembros que obstaculizan el mercado interior y el ejercicio de este derecho fundamental, haciendo una mención especial a la Sentencia del Tribunal de Justica de la Unión Europea, de 24 de noviembre de 2011, que afirmó la incorrecta trasposición de la Directiva por parte de la legislación española. Por último, este estudio analiza el articulado de la propuesta de Reglamento, señalando las principales novedades en lo relativo al ámbito de aplicación territorial, las obligaciones del responsable, el fortalecimiento de las autoridades de control y los principios y derechos, haciendo una mención especial al derecho al olvido en Internet y a la libertad de información.

PALABRAS CLAVE: Derecho a la protección de datos personales, derecho a la privacidad, Reglamento General de Protección de Datos, derecho al olvido, transparencia administrativa, libertad de información, autorregulación, autoridades independientes.

ABSTRACT: The European Commission has adopted a Proposal for a General Data Protection Regulation, which will repeal the actual Directive 95/46/EC and and displace the laws of the Member States. This study analyzes the main reasons to promote the adoption of this new European regulatory framework: the adoption of the Lisbon Treaty, the profound changes that ICTs have experienced in recent years with the arrival of the Internet and social networking, the differences in the protection of personal data among different Member States which impede the internal market and the exercise of this fundamental right, with special mention to the Court of Justice of the EU, judgment of 24.9.2011, which stated the incorrect transposition of the Directive by the Spanish legislation. Finally, this study analyzes the text of the proposed regulation, pointing out the main changes with regard to the territorial scope, general obligations of the controller, the strengthening of the supervisory authorities, the principles and rights, making special mention of the right to be forgotten in the online environment and the freedom of information.

KEYWORDS: Right to protection of personal data, right to privacy, General Data Protection Regulation, the right to be forgotten in the online environment, administrative transparency, freedom of information, self-regulation, independent authorities.

La Comisión Europea está impulsando la configuración de un nuevo marco jurídico europeo para la protección de los datos personales[1], a través de la aprobación el 25 de enero de 2012 de una Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos –un Reglamento general de protección de datos–, que derogará la actual Directiva 95/46/CE– y de una Propuesta de Directiva del Parlamento Europeo y del Consejo 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 la libre circula-

Este trabajo se enmarca dentro del Proyecto de investigación «Transparencia administrativa y protección de datos personales» –DER2012-39629– del Ministerio de Economía y Competitividad.

1. Comunicación de la Comisión "La protección de la privacidad en un mundo interconectado. Un Marco Europeo de Protección de Datos para el siglo XXI", COM (2012) 9 final.

ción de dichos datos[2] . Estas iniciativas legislativas han sido presentadas como un avance para fortalecer la protección de los datos personales en la Unión Europea.

El Reglamento general de protección de datos personales tendrá un alcance general, será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro –art. 288 TFUE–, no requiriendo transposición alguna, por lo que su aprobación desplaza a la normativa española de protección de datos personales, en especial, a la Ley Orgánica 15/1999, de 13, de Protección de Datos (LOPD), y a su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RPDP) –así como a la legislación autonómica y a su normativa reglamentaria desarrollo-[3]. Así, la primacía y el efecto directo del Derecho de la Unión Europea implican la obligación de los poderes públicos, especialmente del poder judicial y de la Administración, de inaplicar aquellos preceptos de la LOPD y del RPDP que sean incompatibles con el Reglamento de la Unión Europea. Sin embargo, los poderes públicos, tanto el Legislador como el Gobierno, tienen la obligación, por razones de seguridad jurídica, de derogar las normas de Derecho interno incompatibles con el Derecho de la Unión. Los Estados miembros no podrán mantener en vigor normas nacionales contrarias al Reglamento general de protección de datos personales, aunque sus poderes públicos –poder judicial y Administración– procedan a su inaplicación, respetando el Derecho de la Unión. Téngase en cuenta que la primacía del Derecho de la Unión Europea no es supremacía y no afecta a la validez de las normas internas[4].

---

2. COM (2012) 10 final y COM (2012) 11 final. El contenido de ambas propuestas tiene el interés de mostrar cuál es la posición inicial de la Comisión. No obstante, estos textos han que ser vistos con la necesaria cautela porque presumiblemente serán objeto de modificaciones en su tramitación tanto en el Parlamento Europeo como en el Consejo. Hay tres Informes que analizan el nuevo marco normativo: la Opinión 1/2012, de 23 de marzo, del Grupo de Trabajo sobre Protección de Datos del Artículo 29; el Informe del Supervisor Europeo de Protección de Datos, de 14 de marzo de 2012, y el Dictamen del Comité Económico y Social, de 23 de mayo de 2012.
3. Cfr. GORDILLO PÉREZ, L. I., *Constitución y ordenamientos supranacionales*, CEPC, Madrid, 2012, esp. pp. 37-101. El Derecho de la Unión Europea opera en el interior de cada Estado conforme a sus características propias: eficacia directa, primacía absoluta y aplicación efectiva y uniforme en toda la Unión. La primacía del Derecho de la Unión, también del Derecho derivado institucional, en este caso del Reglamento general de protección de datos personales, opera desde su publicación en el Diario Oficial de la Unión Europea –que satisface de esta forma el principio de publicidad del art. 9.3 CE–, y su recepción en el Derecho Interno se produce desde la fecha de entrada en vigor. El art. 91 de la propuesta de Reglamento señala que entrará en vigor al día siguiente de su publicación en el DOUE, si bien será aplicable a partir de dos años de esta fecha, habilitándose de esta forma una *vacatio legis* que permitirá adecuar los ordenamientos jurídicos de los Estados miembros
4. La distinción entre primacía y supremacía no es conceptualmente evidente. Sin embargo, el Tribunal Constitucional, en la Declaración 1/2004, de 13 de diciembre, señala: "Primacía y supremacía son categorías que se desenvuelven en órdenes diferenciados. Aquélla, en el de la aplicación de normas válidas; ésta, en el de los procedimientos de normación. La supremacía se sustenta en el carácter jerárquico superior de una norma y, por ello, es fuente de validez de las que le están infra ordenadas, con la consecuencia,

Por tanto, la aprobación del Reglamento general de protección de datos supondrá unas obligaciones para el Legislador y para el Gobierno, que deben velar por la calidad y por la armonía en el Derecho interno. La aplicación efectiva y uniforme del contenido del Reglamento general de protección de datos personales va a requerir de un desarrollo y de una actividad de ejecución, no sólo de las instituciones europeas sino de las autoridades de los países miembros[5]. El Parlamento nacional intervendrá en la ejecución del Reglamento general de protección de datos, en la medida en que su aprobación obliga a la derogación de preceptos de una Ley en vigor, que, además, desarrollan un derecho fundamental[6]. El ejercicio por parte del Parlamento nacional de la función legis-

---

pues, de la invalidez de éstas si contravienen lo dispuesto imperativamente en aquélla. La primacía, en cambio, no se sustenta necesariamente en la jerarquía, sino en la distinción entre ámbitos de aplicación de diferentes normas, en principio válidas, de las cuales, sin embargo, una o unas de ellas tienen capacidad de desplazar a otras en virtud de su aplicación preferente o prevalente debida a diferentes razones. Toda supremacía implica, en principio, primacía (de ahí su utilización en ocasiones equivalente, así en nuestra Declaración 1/1992, FJ 1), salvo que la misma norma suprema haya previsto, en algún ámbito, su propio desplazamiento o inaplicación. La supremacía de la Constitución es, pues, compatible con regímenes de aplicación que otorguen preferencia aplicativa a normas de otro Ordenamiento diferente del nacional siempre que la propia Constitución lo haya así dispuesto, que es lo que ocurre exactamente con la previsión contenida en su art. 93, mediante el cual es posible la cesión de competencias derivadas de la Constitución a favor de una institución internacional así habilitada constitucionalmente para la disposición normativa de materias hasta entonces reservadas a los poderes internos constituidos y para su aplicación a éstos. En suma, la Constitución ha aceptado, ella misma, en virtud de su art. 93, la primacía del Derecho de la Unión en el ámbito que a ese Derecho le es propio, según se reconoce ahora expresamente en el art. I-6 del Tratado."

5. El principio de cooperación leal supone la obligación de los poderes públicos nacionales de adoptar todas las medidas generales o particulares apropiadas para asegurar el cumplimiento de los Tratados y de los actos de las Instituciones –art. 4.3 TUE–, asegurando el efecto útil del Derecho de la Unión, respetando lógicamente el principio de autonomía institucional.
6. El Tribunal de Justicia ha señalado que el mero mantenimiento en vigor –aún sin aplicación– de normas internas incompatibles con el Derecho de la Unión crea una situación de hecho ambigua, dejando a las personas afectadas en un estado de incertidumbre en cuanto a las posibilidades de acogerse al Derecho de la Unión. Por ello, el Tribunal de Justicia exige que la incompatibilidad entre el Derecho de la Unión, incluso de efecto directo, y una norma nacional sea eliminada definitivamente mediante disposiciones internas de carácter obligatorio que tengan el mismo valor jurídico que las que deben ser modificadas. Hay que tener en cuenta, además, que el Tribunal Constitucional, en la Sentencia 58/2004, de 19 de abril, ha señalado que el eventual juicio de incompatibilidad de una norma legal interna con el derecho de la Unión no puede depender exclusivamente de un juicio subjetivo del aplicador del derecho, esto es, de su propia autoridad, sino que debe estar revestido de ciertas cautelas y garantías. Así, el Tribunal Constitucional no permite al juez nacional que, por su propia autoridad, inaplique la ley interna sino que tiene que plantear la cuestión prejudicial o esperar su derogación. Este criterio estaría en contradicción con la STJCE, de 9.03.1978, as. *Simmenthal*, que no vincula la inaplicación de la ley interna al planteamiento de la cuestión prejudicial. La derogación por parte del Parlamento y del Gobierno, tanto a nivel estatal como autonómico, de los preceptos de la LOPD, de la legislación autonómica y de la normativa reglamentaria de desarrollo, evita el planteamiento por parte del juez nacional de la cuestión prejudicial

lativa en la actividad de ejecución del Reglamento debe hacerse sin olvidar que al tratarse de un Reglamento no sólo éste presenta un alto nivel de detalle y de especificación, sino también que existe la obligación del Parlamento nacional de respetar lo establecido en el Reglamento, lo que limita en gran medida la amplitud del debate político y el margen de maniobra del Legislador. No hace falta incorporar el Reglamento –que es obligatorio en todos sus elementos y no requiere transposición– al Derecho interno pero sí es necesario aplicarlo. El desarrollo y ejecución del Reglamento general de protección de datos personales también requerirá la derogación por parte del Gobierno de la normativa reglamentaria de desarrollo de la LOPD incompatible con el Reglamento y la adopción de normas administrativas que se adecúen al nuevo Reglamento General de protección de datos, lo que incluye también la reorganización de servicios administrativos y la atribución de algunas competencias y facultades a la Agencia de Protección de Datos –aunque en menor medida en nuestro país–[7].

Por último, hay que tener en cuenta que la transposición que la normativa española hizo de la Directiva 95/46/CE[8] se ha visto severamente cuestionada por la Sentencia del Tribunal de Justicia de la Unión Europea, de 24 de noviembre de 2011, que ha resuelto la cuestión prejudicial planteada por la Sala de lo Contencioso Administrativo del Tribunal Supremo con arreglo al art. 267 TFUE –a través de la Resolución de 15 de julio de 2010[9]– y que finalmente ha llevado

---

para determinar el grado de inaplicación de la normativa nacional y, sobre todo, elimina las incertidumbres que generarían las eventuales contradicciones entre los distintos jueces nacionales que no planteen la cuestión prejudicial y decidan sobre la aplicación o inaplicación de preceptos de la LOPD y del RPDP, en virtud del mandato a todos los poderes públicos de aplicación del Derecho de la Unión, eludiendo las anomalías que genera un control difuso. Cfr. PÉREZ TREMPS, P., «La jurisdicción constitucional y la integración europea», *REDE*, núm. 29, 2009, pp. 19-48; tempranamente MANGAS MARTÍN, A., «La obligación de derogar o modificar el Derecho interno incompatible con el Derecho comunitario: evolución jurisprudencial», *RIE*, núm. 1987-2, pp. 311-337. Cfr. sobre la cuestión SSTJ, de 15.10.1996, as. *Comisión c. Italia*, (168/85), y de 26.10.1995, as. *Comisión c. Luxemburgo* (C-151/1994). Cfr. también MANGAS MARTÍN, A., «El Derecho de la Unión y el Derecho español», en MANGAS MARTÍN, A., y LIÑÁN NOGUERAS, D. J., *Instituciones y Derecho de la Unión Europea*, 6ª ed. Tecnos, Madrid, 2010, pp. 467-486; y PÉREZ TREMPS, P., «Las fuentes internacionales y supranacionales», en *Derecho Constitucional*, I. 8ª ed., Tirant lo Blanch, Valencia, 2010, pp. 95-115.

7. Idénticas obligaciones le corresponden a los legisladores y gobiernos autonómicos que han aprobado normas sobre protección de datos personales.
8. Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24.10.1995, 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. Cfr. Heredero Higueras, M., *La Directiva Comunitaria de protección de los datos de carácter personal*. Tecnos, Madrid, 1998 –especialmente las pp. 17-49 que explican el proceso negociador–; ARENAS RAMIRO, M., *El derecho fundamental a la protección de datos personales en Europa*, Tirant lo Blanch, Valencia, 2006, pp. 191-376; GUERRERO PICÓ, M. C., *El impacto de Internet en el Derecho fundamental a la protección de datos de carácter personal*, Civitas, Cizur Menor, 2006, pp. 55-134; TÉLLEZ AGUILERA, A., *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores*, Edisofer, Madrid, 2002, pp. 329-349.
9. Las Sentencia del TJUE lleva a cabo una interpretación del art. 7.f) de la Directiva 95/46/CE, en los asuntos acumulados C-468/10 y C-469/10, presentada en el marco de litigios en el que son partes la Asociación Nacional de Establecimientos Financieros de

al Tribunal Supremo, en su reciente Sentencia de 8 de febrero de 2012, a anular el art. 10.2.b) del RPDP por incorporar exigencias adicionales para la legitimación del tratamiento de datos personales sin consentimiento y por excluir la ponderación de los derechos e intereses en conflicto en cada caso concreto, lo que modificaba el alcance de la Directiva 95/46/CE. El efecto directo que esta Sentencia del Tribunal de Justicia de la Unión Europea ha atribuido al art. 7.f) de la Directiva 95/46/CE, unido al principio de primacía del Derecho de la Unión, obligaría a las autoridades nacionales –tanto administrativas como judiciales–, en virtud de la Sentencia *Simmenthal*, a inaplicar los arts. 6.2 y 11.2.b) de la LOPD en aquello que sea incompatible con la Directiva, sin necesidad de *«pedir o esperar la remoción previa por vía legislativa o mediante cualquier otro procedimiento constitucional»*[10]. Urge, por los motivos ya señalados, en virtud de la STC 58/2004, de 19 de abril –que obliga al juez nacional que quiera inaplicar la Ley interna a plantear la cuestión prejudicial o a esperar su derogación– y a falta del planteamiento de la cuestión prejudicial en relación con estos dos preceptos legales, que el Legislador derogue y modifique estos preceptos legales en aquello que sea incompatible con la Directiva –en relación con la interpretación que de la misma ha hecho la STJUE, de 24.11.2011–, evitando la situación de incertidumbre sobre el desplazamiento o no de estos preceptos legales en virtud del efecto directo del art. 7.f) de la Directiva.

II. LA NECESIDAD DE UN NUEVO MARCO NORMATIVO EUROPEO

A) La aprobación del Tratado de Lisboa y los cambios en las tecnologías de la información y la comunicación: del fichero de datos personales a la computación en la nube y al Internet de las Cosas.

Son distintos los motivos que animan a la Comisión a modificar el marco normativo de protección de datos personales[11]. El art. 16 del TFUE, introducido en el Tratado de Lisboa, establece que «[t]oda persona tiene derecho a la protec-

---

Crédito (ASNEF) y la Federación de Comercio Electrónico y Marketing Directo (FECEMD). Esta Sentencia se analiza *infra* apdo. IV.B).

10. Como señalaremos más adelante, la cuestión prejudicial tenía que haberse también planteado en relación con estos dos preceptos de la LOPD, de los cuales el art. 10.2.b) RPDP es su desarrollo reglamentario. Cfr. más en profundidad *infra* apdo. IV.C).

11. La Comunicaciones de la Comisión ya citada –COM (2012) 9 final– y la Exposiciones de Motivos de la propuesta de Reglamento señalan algunas razones para modificar el marco normativo, como el incremento sin precedentes del intercambio de datos a gran escala a raíz de la rápida evolución tecnológica (Considerando 5), la necesidad de que el derecho fundamental a la protección de datos personales se aplique de manera coherente en todas las políticas de la UE (Considerando 8), evitando la fragmentación y permitiendo políticas de protección de datos más integradoras, y la necesidad de generar confianza en el entorno en línea para que la economía digital pueda desarrollarse en el mercado interior (Considerando 6), dada la percepción generalizada en la opinión pública de que existen riesgos significativos en este ámbito, algo esencial en la Agenda Digital para Europa y en la Estrategia Europa 2020. Este trabajo va a profundizar en estas cuestiones y va a apuntar otras razones para la modificación del marco normativo que no aparecen explicitadas en los textos anteriores.

ción de los datos de carácter personal que le conciernan. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos». Este precepto, como señala la Comisión, constituye la nueva base jurídica para la adopción de las normas relativas a la protección de las personas físicas con respecto al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, permitiendo también la adopción de normas relativas a la libre circulación de datos de carácter personal, incluidos los datos personales tratados por los Estados miembros o por los operadores privados[12]. Además, el Tratado de Lisboa suprime la tradicional división entre pilares[13], lo que permite extender la normativa europea de protección de datos personales al ámbito policial y judicial, facilitando un mayor nivel de protección en el antes denominado tercer pilar[14], una cuestión que había sido

12. Cfr. el apdo. «Elementos jurídicos» de la propuesta de Reglamento. Inicialmente la Unión Europea contenía sólo una breve mención a la protección de datos personales dentro del Derecho comunitario originario –el artículo 286 del TCE–, introducido a través del Tratado de Ámsterdam, referido a la vigencia de este derecho en relación con los actos de las instituciones comunitarias y a su vigilancia por una Comisión independiente, lo que dio lugar a la aprobación del Reglamento (CE) n.º 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.
13. No obstante, la política exterior y de seguridad común se mantiene como algo aparte: no le es de aplicación la Carta de Derechos Fundamentales de la Unión Europea, siendo una materia que no está en el TFUE sino que se mantiene en el TUE. Además, la regulación sobre protección de datos en lo que antes se denominaba segundo pilar no es aprobada por el procedimiento antes descrito que da participación al Parlamento sino a través de decisiones del Consejo. Así, el art. 39 TUE, añadido por el Tratado de Lisboa, establece que «de conformidad con el art. 16 del TFUE y no obstante lo dispuesto en su apartado 2, el Consejo adoptará una decisión que fije las normas sobre protección de las personas físicas respecto al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del presente capítulo, y sobre la libre circulación de dichos datos». Cfr. SCIROCCO, A.,» The Lisbon Treaty and the Protection of Personal Data in the European Union», en *Dataprotectionreview*, núm 5, 2008.
14. De hecho, la fragmentación en la aplicación de la protección de datos personales en el territorio de la Unión que tanto ha criticado la Comisión no es sólo responsabilidad de los Estados –que han llevado a cabo una deficiente transposición de la Directiva 95/46/CE, como más adelante señalaremos– sino de la existencia de un régimen jurídico divergente para los distintos pilares. La propuesta de Reglamento resalta la necesidad de crear un marco general y coherente de protección de datos personales que abarque todos los ámbitos de competencia de la Unión, incluida la cooperación policial y judicial en materia penal, de manera que se alcance la plena realización de un «espacio de libertad, seguridad, justicia y de una unión económica» –Considerando 2–. Hay que tener en cuenta que la Carta de Derechos Fundamentales se aplica ahora plenamente al Título VI del TUE y a la cooperación policial y judicial. La propuesta ya citada,

reclamada reiteradamente por el Parlamento Europeo[15]. La Directiva 95/46/CE

presentada por la Comisión, de Directiva del Parlamento y del Consejo permite elevar la protección de los datos personales en los tratamientos por parte de las autoridades para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, sin perjuicio de respetar su especificidad y la existencia de un margen de maniobra para los Estados, al excluirlos del ámbito de aplicación material de la propuesta de Reglamento –art. 2– y regularlos por una Directiva. Hay que tener en cuenta la *Declaración nº 20 relativa al artículo 16 del TFUE*, aneja al Tratado de Lisboa, donde se señala que la Conferencia «declara que, siempre que las normas sobre protección de datos de carácter personal que hayan de adoptarse con arreglo al artículo 16 puedan tener una repercusión directa en la seguridad nacional, habrán de tenerse debidamente en cuenta las características específicas de la cuestión. Recuerda que la legislación actualmente aplicable (véase, en particular, la Directiva 95/46/CE) contiene excepciones específicas a este respecto». También existe una *Declaración nº 21 relativa a la protección de datos de carácter personal en el ámbito de la cooperación judicial en materia penal y de la cooperación policial*, aneja al Tratado de Lisboa, donde se señala que «la Conferencia reconoce que podrían requerirse normas específicas para la protección de datos de carácter personal y la libre circulación de dichos datos en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial que se basen en el artículo 16 del Tratado de Funcionamiento de la Unión Europea, en razón de la naturaleza específica de dichos ámbitos». En todo caso, el antiguo art. 30 del TUE –antiguo art. K.2– señalaba en el ámbito del tercer pilar que la recogida, almacenamiento, tratamiento, análisis e intercambio de información pertinente, en particular mediante Europol –incluida las relativas a las operaciones financieras sospechosas–, tenía que desarrollarse con sujeción a las disposiciones correspondientes en materia de protección de datos personales. Además, los Estados siempre han tenido que respetar los principios del Convenio 108 del Consejo de Europa, de 28 de enero de 1981. Hay que destacar en este último ámbito la Recomendación de 1987 del Comité de Ministros del Consejo de Europa encaminado a regular la utilización de datos de carácter personal en el sector de la policía –Recomendación R (87) 15m de 17 de septiembre de 1987–.

15. El Parlamento Europeo había criticado en el pasado el retraso de la Comisión en la presentación de un instrumento legal de protección de datos para el tercer pilar, que garantizara el mismo nivel de protección en el primer y en el tercer pilar. El *Report of the European Parliament on the First Report on the implementation of the Data Protection Directive* señaló: «Deplores the extremely serious delays that have occurred within the Commission in this matter and urges it to propose within the first half of 2004, as announced, a 'legal instrument' on the protection of privacy in the third pillar; this instrument should be binding in nature and aimed at guaranteeing in the third pillar the same level of data protection and privacy rights as in the first pillar; it should harmonise, according to these high standards, the current rules on privacy and data protection concerning Europol, Eurojust and all other third-pillar organs and actions, as well as any exchange of data between them and with third countries and organisations» _COM (2003) 265 _C5-0375/2003-2003/2153 (INI)_ *http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm_*. Hay que recordar también que el Parlamento Europeo ya había abogado en su Resolución sobre el Programa de Estocolmo, por la revisión de la Decisión Marco. Cfr. Resolución del Parlamento Europeo sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada «Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos –Programa de Estocolmo», adoptada el 25 de noviembre de 2009–. En todo caso, son múltiples las normas europeas relativas a la coordinación de las policías de los Estados miembros, que incluyen algunas garantías en relación con el intercambio de información. Lógicamente, éstas, al igual que la Recomendación 87 del Consejo de Europa, suponían un menor nivel de

excluye el tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en ese momento en el ámbito de aplicación del Derecho Comunitario, como las previstas en el Título V –la política exterior y de seguridad común– y el Título VI –la cooperación judicial y policial– del TUE, y, en cualquier caso, los tratamientos de datos personales que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal –art. 3.2 y Considerandos 13 y 16-[16]. Así, en los ámbitos de política exterior y seguridad común

exigencia. Cfr. la Decisión Marcó 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, más conocida como Decisión Marco, que supuso un avance; la Decisión 2000/641/JAI, del Consejo, de 17 de octubre de 2000, por la que se crea una Secretaría para las autoridades comunes de control de protección de datos establecidas por el Convenio por el que se establece una Oficina Europea de Policía (Convenio Europol), el Convenio relativo a la utilización de la tecnología de la información a efectos aduaneros y el Convenio de aplicación del Acuerdo de Schengen relativo a la supresión gradual de los controles en las fronteras comunes (Convenio de Schengen). Cfr. también la Decisión 2000/642/JAI, del Consejo, de 17 de octubre de 2000, relativa a las disposiciones de cooperación entre las unidades de información financiera de los Estados miembros para el intercambio de información –en relación con la prevención del uso del sistema financiero para el blanqueo de capitales–. En esta dirección, la Comisión ha impulsado la protección de datos de carácter personal también en este ámbito, tratando de establecer unas reglas comunes en el área de libertad, seguridad y justicia, en virtud del anterior TUE. Así, la Comisión había adoptado una propuesta relativa a la protección de datos personales en el ámbito de la policía y de la cooperación judicial en materia penal en el marco del principio de disponibilidad. Cfr. el documento de la Comisión. COM(2005) 475 final of 4.10.2005 COM(2005) 490 final of 12.10.2005 –*http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm*–. Como señala la Comisión, «however, until the situation concerning the ratification process of the Constitutional Treaty becomes clearer the Commission has stressed the need for more efficient procedures in the area of Freedom, Security and Justice under the current Treaties». Cfr. *Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive*, Bruselas, 7.3.2007, COM (2007) 87 –*http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm*– [lo citaremos como *Segundo Informe sobre la aplicación de la Directiva*]. Por último, hay que señalar que España nunca planteó ningún obstáculo para la aplicación de los principios de protección de datos al tercer pilar, lo que no se puede decir de todos los países europeos.

16. La Corte de Justicia en el *Asunto PNR* había reiterado que los tratamientos de datos personales que tengan como finalidad la aplicación de la Ley y la salvaguarda de la seguridad pública, incluyendo no sólo los que llevan a cabo las fuerzas y cuerpos de seguridad sino también aquellos que desarrollan empresas privadas, están excluidos de la Directiva 95/46/CE, al caer dentro del tercer pilar, una cuestión superada tras la aprobación del Tratado de Lisboa. Cfr. la STJUE, de 30.6.2006, as. *PNR*, (C-317/04 y C-318/04), relativa a la cesión desde la Unión Europea a la autoridad de los Estados Unidos de datos de los pasajeros que vuelen hasta ese país, que anuló, a instancia del Parlamento, la Decisión del Consejo relativa a la celebración del acuerdo entre la CE y EE.UU (Decisión 2004/496/CE, de 20 de mayo de 2004) y la Decisión de la Comisión sobre el carácter adecuado de los datos de los pasajeros que se transmiten a EE.UU (Decisión 2004/535/CE, de 6 de julio de 2004). El TJUE considera que el art. 95 TCE no puede constituir la base de la competencia de la Comunidad para celebrar el

y de justicia e interior, la vigencia de la normativa de protección de datos personales se movía en los terrenos de la cooperación y no de la integración[17]. Asimismo, el carácter vinculante que el Tratado de Lisboa ha dado a la Carta de Derechos Fundamentales de la Unión Europea, que en el art. 8 consagra el derecho a la protección de los datos de carácter personal de manera autónoma al derecho al respeto a la vida privada y familiar reconocido en el art. 7[18], refuerza las bases jurídicas específicas para que la Unión Europea apruebe una normativa sobre protección de datos personales aplicable a todos los ámbitos[19],

---

Acuerdo. Cfr. GONZÁLEZ VAQUÉ, L., «El Tribunal de Justicia de las Comunidades Europeas anula el Acuerdo entre la Comunidad Europea y los EEUU para la transmisión de los datos sobre pasajeros por las compañías aéreas», *REDE*, 2006, págs. 557-577; ORÓ MARTÍNEZ, C., «La anulación de la transferencia de datos personales de los pasajeros aéreos a los EEUU», *RGDE*, 11, 2006. Llama la atención que la STJUE, de 4.2.2010, *As. Comisión Europea/Reino de Suecia* (C-185/2009), declarara el incumplimiento de este Estado de la obligación de transposición en el plazo señalado de la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, 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, sin plantearse que esta materia estuviera también dentro del Tercer Pilar. En todo caso, la legislación de los Estados miembros que desarrolla el derecho fundamental a la protección de datos podía tener como ámbito de aplicación no sólo las materias que estaban entonces dentro de la esfera europea –la transposición de la Directiva– sino también materias que estaban fuera de ella, por lo que la legislación de los Estados no tenían que hacer necesariamente una distinción entre protección de datos en el primer y en el tercer pilar. Esto depende de cada Estado, no existiendo una situación uniforme en toda la Unión Europea.

17. Cfr. sobre el concepto de integración PÉREZ TREMPS, P., *Constitución Española y Comunidad Europea*, Civitas, Madrid, 1993, pp. 35-64.
18. La STJUE, de 9.11.2010, as. *Volker und Markus Schecke* y *Eifert*, señala en todo caso que el derecho a la protección de los datos de carácter personal del art. 8.1 de la Carta se halla íntimamente ligado al derecho al respeto a la vida privada reconocido en el art. 7 de la Carta. Cfr. MARTÍN Y PÉREZ DE NANCLARES, J., «Artículo 8. Protección de datos de carácter personal», en MANGAS MARTÍN, A., (Dir.), *Carta de los Derechos Fundamentales en la Unión Europea*, Fundación BBVA, 2008, pp. 223-255, donde se analizan los trabajos de la Convención –pp. 227-228–. Cfr. también RUIZ MIGUEL, C., «El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico», *RDCE*, núm. 14, 2003, pp. 7-43. Aunque inicialmente la Carta no tuvo fuerza normativa plena, ha servido para que el TJUE se pronunciara expresamente sobre el derecho fundamental a la protección de datos en su labor de interpretación de la Directiva 95/46/CE, en las Sentencias *Österreichischer Rundfunk* –STJCE, de 20.5.2003– y *Lindquist* –STJCE, de 6.11.2003–. Cfr. el análisis efectuado por ARENAS RAMIRO, M., *op. cit.* pp. 246-248.
19. Así, la propuesta de Reglamento, teniendo ya su fundamentación en la Carta, no habla ya del derecho a la intimidad en lo que respecta al tratamiento de los datos personales –como hacía el art. 1.1 de la Directiva 95/46/CE– sino del derecho a la protección de datos personales –art. 1.2–, tal como es proclamado en el art. 8 de la Carta. En la misma dirección, el Considerando 1 parte del derecho a la protección de datos personales, reconocido en el art. 16.1 TFUE y en el art. 8.1 de la Carta. No obstante, si bien el art. 6 del TUE reconoce los derechos y libertades enunciados en la Carta de Derechos Fundamentales de la Unión Europea, «la cual tendrá el mismo valor jurídico que los Tratados», también señala que las disposiciones de la Carta «no ampliarán en modo alguno las competencias de la Unión, tal como se definen en los Tratados». La Unión

suprimiendo las limitaciones establecidas en la Directiva. Como es sabido, la malograda Constitución Europea, que también reconocía el derecho fundamental a la protección de datos –arts. I-51 y II-68– y suprimía la división entre pilares, permitía que la aplicación del derecho de la Unión y la tutela de las instituciones europeas no se circunscribieran al primer pilar, contribuyendo a superar las limitaciones del art. 3.2 de la Directiva 95/46/CE[20].

Además, la iniciativa para aprobar un nuevo marco europeo de protección de datos es también consecuencia de los profundos cambios producidos en las tecnologías de la información y la comunicación en los últimos diecisiete años desde la aprobación de la Directiva en 1995 –y en los últimos veinte años desde la elaboración de sus primeros borradores, de los que trae causa, en nuestro país, la ya derogada LORTAD y, en gran medida, la actual LOPD–. La normativa europea y nacional de protección de datos regula y define los ficheros de datos personales –aunque también albergue el concepto de tratamiento–, algo característico de la primera etapa de desarrollo de la informática dominada por los grandes ordenadores –la de la macro-informática– y de la segunda etapa caracterizada por la extensión de los ordenadores personales –la de la micro-informática–, pero no alcanza a regular y ni siquiera a entrever lo que serían las siguientes grandes etapas en la historia de la informática, caracterizadas por el desarrollo y la rapidez de Internet, por los eficaces motores de búsqueda, por la aparición y universalización de las redes sociales virtuales[21], por los servicios de computación en nube –*Cloud Computing*– o por la reciente problemática que supone el denominado «Internet de las Cosas» –*Internet of Things* (IoT)[22]–. La

---

dispone en este punto de competencias compartidas con los Estados miembros sobre mercado interior, sobre el espacio de libertad, seguridad y justicia y sobre el desarrollo tecnológico –art. 4 TFUE–.

20. Como señala la Comisión en el *Segundo Informe de aplicación de la Directiva*, cit., «[t]he ratification of the Constitutional treaty may open new perspectives. The Constitutional Treaty would have an enormous impact in this field. It would enshrine in Article II-68 the right to protection of personal data in Article 8 of the Charter of Fundamental Rights. It would also create a specific and self-standing legal basis for the Union to legislate in this matter in Article I-51, paving the way for adopting instruments applicable in all sectors». Cfr. sobre la cuestión DE MIGUEL SÁNCHEZ, N., «El derecho a la protección de datos personales en el Tratado por el que se instituye una Constitución para Europa», *RAP*, núm. 169, 2006, pp. 301-335; GUERRERO PICÓ, M. C., «El derecho fundamental a la protección de los datos de carácter personal en la Constitución europea», *RDCE*, 2005, pp. 293-332; y más ampliamente ÁLVAREZ CONDE, E. y GARRIDO MAYOL, V., (Dirs.), *Comentarios a la Constitución Europea*, Valencia, Tirant lo Blanch, 2005.

21. En una de las mesas redondas de la *Conferencia Internacional de Autoridades de Protección de Datos y Privacidad*, celebrada en Madrid el 4 y 5 de noviembre de 2009, estaban representadas las empresas que han protagonizado esta evolución hasta ese año: *IBM, Microsoft, Google y Facebook*.

22. El Internet de las Cosas permite la comunicación entre dispositivos y proveedores de forma automática e incluso desconocida para sus propietarios. De esta manera, muchas cosas son localizadas, identificadas, monitorizadas y controladas de forma remota a través de tecnologías como radiofrecuencia, sensores de red, pequeños servidores embebidos y colectores de energía, todos conectados utilizando Internet de última generación. Como señaló David Petraeus –Director de la CIA– «te espiaremos a través de tu

Directiva se centra en dónde están los datos, algo que tenía sentido en 1995 pero que carece de valor en la era de Internet donde sólo se sabe dónde está el interesado o donde tiene su establecimiento principal el responsable del tratamiento, no donde se encuentra la información. Si bien tanto la Directiva 95/46 CE como el Convenio 108 del Consejo de Europa reconocen principalmente principios y derechos y son tecnológicamente neutrales –y, por tanto, suficientemente flexibles–, han nacido a comienzo de los años ochenta y noventa del siglo pasado por lo que no han podido contener una referencia más expresa a los nuevos tratamientos de datos personales derivados de la revolución que se ha producido en las tecnologías de la información y de las comunicaciones[23]. Esto obliga a repensar y a reforzar la normativa europea de protección de datos personales para que contemple y regule estas nuevas realidades que, si bien aportan principalmente oportunidades y ventajas, también conllevan la aparición de nuevos riesgos. Son tales los riesgos y las amenazas que ha llegado a afirmarse que debemos resignarnos a no tener privacidad –*you already have zero privacy. Get over it*– o «si tenemos privacidad es porque alguien tolera que la tengamos»[24].

B) La importancia de la protección de datos personales en la construcción europea.

Hay que tener en cuenta que pocos derechos son tan importantes para la construcción y para hacer viable ese espacio común que hoy representa la Unión Europea como el derecho fundamental a la protección de datos personales. Si el objetivo clásico de la Unión Europea era la libre circulación de personas, mercancías y capitales, y, por tanto de datos personales[25], esto movimiento solo

---

lavavajillas». La Comisión Europea ha lanzado una consulta pública *online* para permitir a sus ciudadanos dar su opinión sobre esta cuestión a través de siete secciones: privacidad, seguridad, seguridad en infraestructuras críticas, ética, identificadores e interoperabilidad, gobernanza y estándares.

23. La propuesta de Reglamento subraya los nuevos retos para la protección de los datos personales derivados de la evolución tecnológica y de la globalización, que han transformado la vida económica y social, permitiendo a las empresas privadas y a las autoridades públicas la utilización de datos personales a gran escala; también los individuos difunden un volumen cada vez mayor de información personal a escala mundial –Considerando 5–. Al mismo tiempo la Comisión señala la existencia de una percepción generalizada entre la opinión pública de que existen riesgos significativos para la protección de las personas relacionados especialmente con las actividades en línea –Considerando 7 y Eurobarómetro especial (EB) 359, *Data Protection and Electronic Identity in the EU* (Protección de datos e identidad electrónica en la UE, 2011), en *http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf*.–.
24. La afirmación –del año 1999– pertenece al Presidente y co-fundador de *Sun Microsytems*, Scott McNealy, y es el comienzo del interesante trabajo de PIÑAR MAÑAS, J.L, «¿Existe privacidad?», en *Protección de datos personales*, Alonso Editores, México, 2010, en especial, cfr. los ataques a los que hoy está sometida la privacidad –pp. 19-25–.
25. Como señala el Considerando 5 de la Directiva, la integración económica y social resultante del establecimiento de un mercado interior previsto en el art. 7 A del Tratado implica necesariamente un aumento notable de los flujos transfronterizos de datos personales entre todos los agentes de la vida económica y social de los Estados miembros, tanto públicos como privados. La Directiva hacía una estimación de un incremento del intercambio de datos personales entre empresas establecidas en los diferentes Estados

era posible si los países que la componen disponían de un modelo de protección de datos personales homogéneo. Se hacía necesario, pues, el establecimiento de un sistema de protección de datos a escala europea que habilitara el intercambio de información personal mediante el establecimiento de estándares comunes[26]. La Directiva 95/46/CE iba encaminada a alcanzar dos de las ambiciones más antiguas del proyecto de integración europea: la realización del mercado interior –en este caso, la libre circulación de datos personales– y la protección de los derechos y libertades fundamentales de las personas físicas en lo que respecta al tratamiento de datos personales[27]. No obstante, a pesar de la preocupación europea por los derechos fundamentales y por la protección de datos personales, que posteriormente se materializó en el art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea, la Directiva 95/46/CE tiene su fundamento jurídico en el antiguo artículo 100 A del Tratado constitutivo de la Comunidad Europea y, por tanto, se basa en el mercado interior[28]. Así, la aprobación de la Directiva se justificaba por la obstaculización al mercado interior y a la libre circulación de datos personales que suponían las distintas regulaciones nacionales sobre protección de datos personales[29]. La propuesta de Reglamento reitera

---

miembros. Además, consideraba que las propias Administraciones Públicas estaban destinadas a colaborar y a intercambiar datos personales a fin de cumplir su cometido o ejercer funciones por cuenta de las administraciones de otros Estados miembros, en el marco del espacio sin fronteras que constituye el mercado interior –en similares términos se expresa el Considerando 4 de la propuesta de Reglamento–.

26. Cfr. COM (90) 314 final– SYN 287 y 288–, 13 de septiembre de 1990, p. 4.
27. Cfr. el *Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE)*, Bruselas, 15.5.2003 COM (2003) 265 *_http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm_*. Así, la Directiva 95/46/CE considera como objetivos la protección de las libertades y de los derechos fundamentales de las personas físicas y la libre circulación de los datos personales –art. 1–. El Tribunal de Justicia, en la Sentencia *Lindqvist* señala que «la Directiva 95/46/CE trata de asegurar la libre circulación de datos personales, garantizando al mismo tiempo un alto nivel de protección de los derechos e intereses de las personas a las que se refieren dichos datos» –apdo. 96–. La propuesta de Reglamento también recoge ambos objetivos –art. 1–; en esta misma dirección, su Considerando 2 señala el doble objetivo de que los tratamientos de datos personales deben estar al servicio del hombre, respetando el derecho a la protección de los datos personales, al mismo tiempo que se asume que el tratamiento de datos personales debe contribuir al progreso económico y social, al esfuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de los individuos. De hecho, dos de los tres objetivos estratégicos sobre los que la Comisión realizó la evaluación de impacto de la propuesta de Reglamento eran mejorar la dimensión del mercado interior y hacer más efectivo el ejercicio de los derechos de protección de datos por los ciudadanos.
28. En cambio, la propuesta de Reglamento tiene su fundamento no sólo en la aproximación de las legislaciones de los Estados miembros que tengan por objeto el establecimiento y el funcionamiento del mercado interior –art. 114.1 TFUE– sino también en el derecho a la protección de los datos personales –art. 16.2 TFUE–.
29. Como señala el Considerando 7 de la Directiva, las diferencias entre los niveles de protección de los derechos y libertades de las personas, especialmente de la intimidad, garantizados en las disposiciones legales y reglamentarias de los Estados miembros en relación a los tratamientos de datos personales pueden suponer un impedimento a la transmisión de datos de un Estado a otro, dificultando el ejercicio de las actividades

la previsión de la Directiva de que «la libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales» –art. 1.3–. En todo caso, a pesar de que la Unión Europea no ha sido competente tradicionalmente en derechos fundamentales[30], buena muestra de la importancia del derecho fundamental a la protección de datos personales en la construcción europea es que la primera vez que el Tribunal de Justicia de la Unión Europea afirma que los derechos fundamentales son principios generales del Derecho comunitario fue el caso *Stauder* una sentencia de 1969 que resolvía un litigio de protección de datos personales[31]. Posteriormente han sido muchos los instrumentos tanto de Derecho originario como derivado que han reconocido y desarrollado el derecho fundamental a la protección de datos per-

económicas a escala comunitaria, falseando la competencia e impidiendo que las Administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario. Por este motivo, el objetivo de la Directiva 95/46/CE era facilitar el funcionamiento del mercado interior, mediante el establecimiento de unos niveles semejantes de protección de datos personales entre los Estados miembros –en términos semejantes se expresa el Considerando 7 de la Propuesta de Reglamento-y el apdo. 1.4.3 «Justificación de la propuesta» de la Ficha Financiera Legislativa que incide en que las divergencias de normativa obstaculizan el funcionamiento del mercado interior y la cooperación entre autoridades públicas en relación con las políticas de la UE.

30. Cfr. más ampliamente MANGAS MARTÍN, A., «El compromiso con los derechos fundamentales», MANGAS MARTÍN, A. (Dir.), *Carta de los Derechos Fundamentales en la Unión Europea*, Fundación BBVA, 2008, pp. 31-75; ALONSO GARCÍA, R., «La Carta de los Derechos Fundamentales de la Unión Europea», *Gaceta jurídica de la UE y de la competencia*, núm. 209, 2000, pp. 3 y ss; ALONSO GARCÍA, R., «El triple marco de protección de los derechos fundamentales en la Unión Europea», y SAIZ ARNÁIZ, A., «La Carta de los Derechos Fundamentales de la Unión Europea y los ordenamientos nacionales: ¿qué hay de nuevo?», *Cuadernos de Derecho Público*, núm. 13, 2001, pp. 13 y ss. y 153 y ss; CORCUERA, J. (Coord.), *La protección de los derechos fundamentales en la Unión Europea*, Dykinson, Madrid, 2002; WEBER, A., «La Carta de los Derechos Fundamentales de la Unión Europea», *REDC* núm. 64, 2002, pp. 79 y ss; con anterioridad, CHUECA SANCHO, A., *Los derechos fundamentales en la Unión Europea*, Bosch, Barcelona, 1999; DÍEZ PICAZO, L.M., «¿Una Constitución sin declaración de derechos? (Reflexiones constitucionales sobre los derechos fundamentales en la Comunidad Europea)», *REDC* núm. 32, 1991.

31. STJCE, de 12.11.1969, 29-69. El demandante cuestionaba una decisión de la Comisión sobre venta de mantequilla a precio reducido a beneficiarios del régimen de asistencia social con divulgación de su nombre. Inicialmente la ausencia de un reconocimiento de derechos fundamentales en los Tratados constitutivos de la Unión Europea se superó manteniendo que los derechos fundamentales reconocidos en los textos constitucionales de los Estados miembros eran parte de los principios generales del Derecho comunitario y del acervo comunitario. El TJCE afirmó en la Sentencia *Stauder* que los derechos fundamentales se hallaban comprendidos «en los principios generales del derecho comunitario que el Tribunal garantiza», de manera que «el respeto a los derechos fundamentales forma parte integrante de los principios generales del derecho que el Tribunal de Justicia salvaguarda», salvaguardia que se inspira en «las tradiciones constitucionales comunes a los Estados miembros». Cfr., tempranamente ALONSO GARCÍA, R., *Derecho Comunitario. Sistema constitucional y administrativo de la Comunidad Europea*, Ceura, Madrid, 1994, pp. 600-665; más recientemente MANGAS MARTÍN, A., *ibídem*, pp. 34-35; ARENAS RAMIRO, M., *op. cit.* págs. 226-227.

sonales en la Unión Europea[32], a lo que se ha unido una interesante jurisprudencia del Tribunal de Justicia que ha analizado de manera indirecta este derecho fundamental[33].

---

32. Además de las ya citadas Directiva 95/46/CE, de la Carta de Derechos Fundamentales de la Unión Europea y del malogrado proyecto de Tratado que aprobaba una Constitución para Europa, hay que destacar distintas normas de Derecho Derivado institucional. Cfr. la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15.10.1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, que adaptó los principios expuestos en la Directiva 95/46/CE en normas específicas para el sector de las telecomunicaciones –donde existe un tratamiento masivo de datos de abonados y usuarios–, atribuyendo a ésta un carácter supletorio. Cfr. también la Directiva 2002/58/CE, de 12.7.2002, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas –modificada por el art. 89 de la propuesta de Reglamento–, que ha actualizado –y derogado– la Directiva 97/66/CE recogiendo la evolución de los mercados y de las tecnologías de servicios de comunicación electrónica, como Internet, con el fin de ofrecer el mismo nivel de protección de los datos personales y la intimidad para todas las tecnologías utilizadas. Esta Directiva se beneficia ya de la influencia de la Carta, ya que no sólo hace referencia a la intimidad y la vida privada de los ciudadanos, sino también al derecho fundamental a la protección de datos personales como derecho autónomo. También hay que señalar la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8.6.2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior y que hace una mención expresa a la Directiva 95/46/ CE en relación al tratamiento de datos personales; igualmente la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15.3.2006, sobre conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes de comunicaciones, por la que se modifica la Directiva 2002/58/CE. Recientemente hay que destacar la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25.11.2009, por la que se modifican la antes citada Directiva 2002/58/CE sobre privacidad y comunicaciones electrónicas, y la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, y que obliga al responsable de la web a obtener el consentimiento del usuario para instalar una *cookie* –un pequeño programa– en el navegador del internauta con la finalidad recordar datos de acceso y otras preferencias del internauta sobre el sitio web que la emite. Son útiles para facilitar determinados trámites del usuario que, gracias a las *cookies*, no debe repetirlos porque el sitio lo reconoce. Son utilizadas para ajustar la publicidad en función de la navegación del internauta. Algunos usos han despertado polémica sobre la protección de la privacidad. Las Administraciones Públicas, siguiendo a las entidades privadas, también recurren a las cookies para conocer las frecuencias, los comportamientos y los itinerarios que siguen los ciudadanos al visitar los sitios web de la Administración Cfr. VALERO TORRIJOS, J., «El uso de cookies por las Administraciones Públicas: ¿una vulneración de la normativa sobre protección de los datos personales?», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 3, 2003, pp. 173-178.

33. Así, por ejemplo, además de las Sentencias ya citadas, hay que destacar la STJCE, de 5.10.1994, as. *X vs. Comision* (C-404/92), en la que el Tribunal estudió la protección de la vida privada en el contexto de las relaciones laborales, reconociendo el derecho a mantener la reserva sobre el estado de salud, todo ello al amparo de la jurisprudencia del Tribunal Europeo de Derechos Humanos y de los principios derivados de las tradiciones constitucionales comunes a los Estados miembros. No obstante, este derecho puede sufrir limitaciones, como señala el propio artículo 8 del Convenio, lo que implica que si los servicios de contratación de las instituciones comunitarias exigen a un candi-

III. LA PROTECCIÓN DE DATOS PERSONALES EN UN MUNDO GLOBALIZADO E INTERCONECTADO

A) La necesidad de unos estándares internacionales de protección de datos personales y de un equilibro entre las diferentes visiones sobre la protección de datos personales a nivel internacional.

La protección de datos personales, si es importante dentro de la Unión Europea, lo es aún más en un mundo globalizado e interconectado. No nos referimos únicamente al intercambio transfronterizo de datos derivado del incremento de las relaciones económicas, comerciales o de investigación con otros países, especialmente del área Asia-Pacífico[34]. Los tratamientos de datos personales de la propia esfera personal o doméstica que llevan a cabo las redes sociales virtuales –*Facebook*, *MySpace*– o los motores de búsqueda –de la que la reciente polémica relativa a *Google Street View* es un buen ejemplo– o la prestación de servicios de computación en nube –*Cloud Computing*[35]– implican la existencia de constantes flujos transfronterizos de información personal para los que no siempre ha sido efectiva la normativa europea de protección de datos –y mucho menos la legislación estrictamente nacional–. Estos tratamientos de datos personales se desarrollan por Internet a través de redes internacionales cuyos usuarios y proveedores de servicios se encuentran ubicados en países diferentes y donde el servidor informático se encuentra también en un tercer país[36]. Cada vez es más complicado determinar la jurisdicción competente –cuál

---

dato que se someta a un examen médico y éste se niega, la Comisión no está obligada a soportar los riesgos derivados de su contratación. En la STJCE, de 14.9.2000, As. *Fisher* (C-369/98), se analizó la divulgación de datos de carácter personal contenidos en un fichero, resolviéndolo a partir de los criterios generales establecidos en la Directiva 95/46/CE, que, si bien no había entrado en vigor todavía en el momento en el que se planteó el asunto, remitía en su Exposición de Motivos a los principios comunes a los Estados miembros en esta materia. Cfr., más ampliamente, ARENAS RAMIRO, M., *op. cit.* pp. 225-248.

34. Recientemente he tenido la oportunidad de colaborar en el proyecto «Genetic databases for international biomedical research. The ICGC», que coordinaba la Cátedra de Derecho y Genoma Humano de la Universidad de Deusto y de la Universidad del País Vasco, donde se analizaban las cesiones de datos entre hospitales y centros de investigación sanitaria, más allá de las fronteras de la Unión Europea, especialmente con el área Asia-Pacífico.
35. Así, la Comisión Europea abrió entre abril y agosto de 2011 una consulta pública sobre *Cloud Computing* con la finalidad de establecer condiciones para la prestación de servicios de computación en nube, abordando cuestiones como la responsabilidad del tratamiento, la seguridad de la información o la autoridad de control. La Comisión se planteó si sería útil establecer un «Modelo de Acuerdo de Nivel de Servicio o de Acuerdos de Usuario Final». Las respuestas a esta consulta pública han servido para confeccionar la estrategia a seguir sobre esta cuestión, que se incluirá en la Agenda Digital de la Comisión hasta 2020.
36. Una de las características de la «nube» es que permite guardar la información en muchos lugares diferentes. Así, por ejemplo, una persona que se conecta desde su ordenador en España a una web estadounidense, que ofrece el servicio de almacenar y compartir fotografías, puede estar subiendo esa información a servidores alojados en Holanda o en cualquier otro país.

es la legislación aplicable y la autoridad para resolver las disputas– y quien es el responsable del tratamiento. Las amenazas al derecho fundamental a la protección de datos personales provienen de más allá de las fronteras de la Unión Europea[37], lo que exige que, al menos, la normativa de protección de datos personales –y en el futuro las propias instituciones de tutela– tengan también un carácter supranacional. Lógicamente, detrás de esta cuestión se esconde el debate de fondo sobre el papel regulador –principal o subsidiario– de los Gobiernos en Internet, una cuestión que fue abordada por la Cumbre del G-8 dedicada a Internet, en mayo de 2011[38]. Hay que subrayar, como hemos seña-

37. Como señala el Informe del Parlamento Europeo, «personal data protection infringements (concerning EU citizens' data) are likely to take place more in third countries than in the Member States» Cfr. *Report of the European Parliament on the First Report on the implementation of the Data Protection Directive* –COM (2003) 265 –C5-0375/ 2003-2003/2153 (INI)– *http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm*–.

38. Esta cumbre del G-8, celebrada en la ciudad francesa de Deauvill, analizó la necesidad de establecer un marco jurídico eficaz, no para frenar Internet, sino para asegurarse de que prospere sobre la base del respeto a la privacidad, a la propiedad y a los derechos de las personas, dando confianza a los usuarios, ya que la autorregulación parece insuficiente. En el discurso inaugural, Sarkozy señaló que Internet no es «un universo paralelo, liberado del imperio de la ley, sin moral y sin los principios fundamentales que gobiernan la vida social en los países democráticos». Así, resaltó que Internet es un vector de una potencia inédita para la libertad de expresión, clave en las revoluciones de Túnez y Egipto, pero que no puede escaparse de unos valores y reglas mínimos. Así, "si bien la población árabe ha mostrado que Internet no pertenece a los Estados, sin embargo, en esta tercera mundialización de la historia no puede marginarse a los Estados democráticos. Olvidar que son los representantes legítimos de la voluntad popular sería apostar por un riesgo claro, el caos democrático, la anarquía". El presidente francés enumeró los peligros de Internet y advirtió del peligro de que aparezcan nuevos monopolios donde han desaparecido otros, a la vez que se opuso a la idea de una transparencia total». Sarkozy recalcó que, si la tecnología es neutra, no lo son sus usos y que no debe permitirse que la revolución digital pueda atentar contra los derechos elementales. Por el contrario, empresas como *Google* y *Facebook* defendieron en esa Cumbre un papel subsidiario de los Gobiernos en la regulación de la Red. Así, Eric Schmidt, presidente de Google, destacó que la tecnología va más rápida que los Gobiernos, por lo cual aconseja no legislar antes de saber si la propia tecnología ofrece remedios a los problemas. Cfr. *El País*, 25.5.2011. El consejero delegado de Vodafone, Vittorio Colao, ha defendido, en cambio, la necesidad de que las empresas de Internet, como *Facebook* o *Google*, cumplan con la normativa europea en materia de seguridad y privacidad, como lo hacen los operadores de telecomunicaciones europeos, que tienen que asumir los costes de salvaguardar la legislación. Cfr. *Europa Press*, 6.6.2011.
Como hemos analizado en otro momento, Internet es, sobre todo, un instrumento de libertad y de civilización. Así, Internet es un espacio de libertad de expresión y de información, que favorece la existencia de una opinión pública libre, especialmente en los regímenes autoritarios donde están cerrados los canales tradicionales de información, como hemos visto recientemente en las revoluciones de la primavera árabe –Túnez, Egipto, Libia, Siria–. También Internet, en especial las redes sociales virtuales, han sido un poderoso instrumento de oposición política en ámbitos geográficos donde los derechos políticos no existen o están muy limitados. Así, el candidato a la Presidencia de Irán en el año 2009 Hossein Mousavi empleó las redes sociales –*Facebook, Myspace*– y creó una red social –*Green Path of Hope*– para convocar manifestaciones y ofrecer información e imágenes que omitían los canales estatales. Incluso en democracias asen-

lado en otro momento, que el derecho fundamental a la protección de datos personales tiene una dimensión internacional de la que carecen otros derechos fundamentales y que es necesario establecer exigencias homogéneas de privacidad, que superen las discrepancias existentes –por no decir los desequilibrios– entre los distintos niveles de protección de los diferentes países, especialmente entre la Unión Europea, Estados Unidos y el ámbito Asia-Pacífico[39].

---

tadas, como España, Internet –redes sociales como *Twitter*– han favorecido la configuración de grupos de oposición política como el movimiento del 15M o de los indignados y han permitido o canalizado el posicionamiento crítico de los ciudadanos ante la Corona –incidente del Rey en Bostwana; negocios del marido de la Infanta Cristina, Iñaki de Urdangarín, renovación de su contrato con Telefónica, etc–, situaciones que antes se podían haber silenciado con el control de dos o tres medios de comunicación. Además, las nuevas tecnologías favorecen la participación de los ciudadanos en la vida política –un valor procedimental necesario para el principio democrático y para el mantenimiento de una sociedad abierta–. Así, las sociales permiten la posibilidad de asociarse con otros en los procesos de participación, a diferencia de lo que ofrecen los espacios institucionales de participación electrónica o los propios medios de comunicación digitales, donde se puede ejercer la libertad de expresión pero no formar grupos. Igualmente, las redes sociales han descubierto una manera inédita de hacer política, que abre la posibilidad de tener una red de colaboradores y pedirles que hablen por ti, lo que facilita la participación política, especialmente a los jóvenes, como hizo Obama en las elecciones presidenciales americanas de 2008. También Internet es un poderoso instrumento de transparencia administrativa que permite el control social del poder. Además, las nuevas tecnologías responden a las necesidades de comunicación y socialización y pueden evitar situaciones de exclusión social y de desarraigo, aunque también pueden crear otras. Por ello, el acceso a Internet es un derecho fundamental de la persona, lo que no quiere decir que no esté sometido a límites, que requieren una regulación legal y un control judicial, sin perjuicio de la posible intervención en este ámbito de autoridades administrativas independientes.

39. Estados Unidos y la Unión Europea han mantenido históricamente múltiples reuniones para tratar de mejorar la «interoperabilidad» de sus sistemas de protección de datos. Estados Unidos ha defendido hasta ahora que sus políticas de privacidad en el medio electrónico eran, como mínimo, tan estrictas como las impulsadas por la Unión Europea. El Consejero Principal sobre Asuntos Europeos y Aplicación de Leyes Internacionales de la Misión de Estados Unidos ante la UE, Stewart Robinson ha señalado, en referencia a la preocupación global de los usuarios por la seguridad de sus datos cuando utilizan la computación en la nube, que es «falso» que la UE se preocupe más por salvaguardar la privacidad que Estados Unidos, un país que defiende «importantes libertades civiles» y cuya Constitución reconoce el derecho a la privacidad. También quiso descartar la idea de que la UE «protege mejor» esos derechos que Estados Unidos, y señaló que ambos» hacen una labor muy parecida, ambos tienen enfoques muy semejantes». Así, ha destacado que Estados Unidos ha impulsado unas líneas directrices que recogen los derechos fundamentales de los consumidores, de manera que cada industria se comprometa a través de un código de conducta adoptado. Además, señaló que la Casa Blanca iba a presentar de manera inminente un «libro blanco» con la finalidad de proponer a las empresas el desarrollo de códigos de conducta sobre la protección de la información. Como puede comprobarse, el modelo americano ha descansado hasta ahora más en la autorregulación mientras que el modelo europeo ha apostado por las herramientas normativas heterónomas; de ahí la fuerte asimetría.

No obstante, el Presidente de EE.UU. Barak Obama ha presentado el 23 de febrero de 2012 el documento *Consumer Data Privacy in a Networked World. A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, una auténtica

Durante los últimos años se ha hecho si cabe cada vez más patente la necesidad de proteger la privacidad en un mundo sin fronteras –especialmente desde la aparición de Internet– y caracterizado por las transferencias internacionales constantes de datos personales. La protección de la privacidad en un entorno globalizado sólo es posible si se consensuan unas normas de protección de datos personales –asumiendo que existen visiones diferentes en los distintos continentes– y si éstas se extienden a todos los países. Lógicamente, la preocupación por alcanzar unos estándares internacionales de protección de datos personales ha correspondido principalmente a las autoridades de control, en las que recae la responsabilidad de velar por el cumplimiento de la legislación nacional de protección de datos personales y por los derechos de las personas en relación con los tratamientos de sus datos personales. Son estas autoridades las más conscientes de que la actual normativa europea y nacional, si bien es un elemento necesario, sigue siendo todavía insuficiente. No obstante, también los representantes de la sociedad civil y de la industria han apoyado estas iniciativas para el establecimiento de unos estándares internacionales de protección de datos personales: los primeros como defensores de los derechos que no son reales y efectivos con la mera aplicación de las normas nacionales; los segundos movidos por un legítimo interés por comercializar productos y servicios que sólo puede impulsarse a nivel global sobre la base de unos estándares internacionales –y no de una variada y cambiante legislación nacional–, que sean transparentes y que den seguridad jurídica, también para los flujos internacionales

---

Carta de Derechos sobre protección de datos personales, en el marco de un proyecto de Ley sobre Privacidad del Consumidor. El presidente estadounidense ha instado también al Congreso a aprobar las leyes para aplicar la nueva legislación en los sectores comerciales no cubiertos ya por la legislación federal sobre protección de privacidad y para desarrollar un código de conducta, de cumplimiento obligatorio. En la última cumbre bilateral celebrada en noviembre de 2011 en Washington, el presidente estadounidense, Barack Obama, el presidente del Consejo Europeo, Herman Van Rompuy, y el presidente de la Comisión Europea, José Manuel Durao Barroso, se comprometieron a aumentar su cooperación comercial y en términos de regulación. Recientemente EEUU y la UE han firmado un Acuerdo para garantizar la protección de datos personales en los intercambios comerciales, como resultado de la Conferencia destinada a facilitar la interoperabilidad de los regímenes comerciales sobre protección de datos, en la que han participado la Vicepresidenta de la Comisión y responsable de Justicia Viviane Reding y el Secretario de Comercio, John Bryson. Este Acuerdo busca una cooperación transatlántica más fuerte en el ámbito de la protección de datos que refuerce la confianza de los consumidores y promueva un crecimiento continuo de la economía global de Internet y la evolución del mercado digital común transatlántico, algo especialmente importante en el actual contexto de crisis económica y ante la necesidad de apuntalar el crecimiento y el empleo a nivel global. En un momento de cambios legislativos tanto en EEUU como en la Unión Europea, lo que se trata es de crear marcos normativos de reconocimiento mutuos de protección de la privacidad que permitan el flujo de datos y la interoperabilidad en el Atlántico sin discriminación. Si bien el Acuerdo se ha centrado en las relaciones comerciales, se ha puesto sobre la mesa el compromiso de la cumbre de noviembre de 2011 para finalizar las negociaciones que lleven a un acuerdo completo de privacidad, que facilite también el intercambio de datos en otros ámbitos, como la lucha contra el crimen y el terrorismo.

de información, factor esencial en el desarrollo económico[40]. Si bien existía un consenso generalizado sobre la necesidad de unos estándares internacionales, han faltado en los últimos años iniciativas concretas a este respecto. Posiblemente existía un cierto escepticismo –o pesimismo– acerca de las posibilidades reales de alcanzar tan ambicioso objetivo, que olvidaba la importancia de ir dando pasos concretos –aunque fueran pequeños– en esa dirección. Por ese motivo, fue especialmente importante la aprobación por unanimidad de las Autoridades de Control en la 30ª Conferencia Internacional sobre Privacidad y Protección de Datos celebrada en Estrasburgo en 2008 de una Resolución para elaborar una Propuesta Conjunta para el establecimiento de estándares internacionales sobre privacidad y protección de datos[41], siendo la Agencia Española de Protección de Datos la principal promotora de la iniciativa junto con el Comisionado Federal de Protección de Datos de Suiza. Finalmente, la Resolución de Estándares Internacionales fue aprobada por la 31ª Conferencia Internacional sobre Privacidad y Protección de Datos celebrada en Madrid en 2009 –más conocida como Resolución de Madrid–[42]. Esta Resolución de Madrid tiene como objeto «definir un conjunto de principios y derechos que garanticen la efectiva y uniforme protección de la privacidad a nivel internacional, en relación con el tratamiento de datos de carácter personal» –art. 1–. Para ello, recoge unas disposiciones generales, unos principios de protección de datos básicos, unos derechos de protección de datos de los interesados y unas obligaciones de cumplimiento y supervisión. Esta Resolución supone un equilibro entre las diferentes visiones sobre la protección de datos personales existentes a nivel internacional y que se plasman en las distintas legislaciones. Es, por tanto, un documento nacido del diálogo y de la búsqueda del consenso que trata de integrar las sensibilidades de los distintos continentes, recogiendo los principios que son comunes a todos los modelos[43]. De hecho, la Resolución de Estrasburgo

40. Las empresas globales demandan respuestas también globales para la protección de la privacidad. Cfr. la *Declaración de la Industria sobre «la necesidad de marcos internacionales en apoyo a la protección de la privacidad y de los datos personales», de 27 de octubre de 2009*.

41. El Párrafo Operativo 3 de esta Resolución establece que «la Conferencia mandata la creación de un Grupo de Trabajo, bajo coordinación de la Autoridad organizadora de la 31ª Conferencia Internacional y con la participación de las Autoridades de protección de datos interesadas en ello, con el objetivo de elaborar una Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad y de los Datos de Carácter Personal.»

42. Correspondió a la Agencia Española de Protección de Datos el mérito de coordinar el grupo de trabajo que redactó la Propuesta Conjunta sobre Estándares Internacionales. Hay que destacar el papel que en ella jugó el entonces Director de la Agencia Artemi Rallo, que tuvo la inteligencia y el liderazgo necesario que posibilitó la aprobación de la Resolución. Inteligencia –y flexibilidad– porque supo elegir los temas que debían incluirse en el documento final y aquellos que debían constar en la Memoria explicativa, renunciando a otros aspectos que no podían estar en el texto si se quería alcanzar el consenso final. Liderazgo porque fue capaz de vencer reticencias y escepticismos internos y externos para permitir la aprobación de una Resolución y aunar en torno a ella tanto a la sociedad civil como a la industria.

43. Cualquier iniciativa encaminada a tratar de proteger la privacidad de manera global se encuentra con el problema de que hay países mucho más estrictos en sus normas que

señalaba que «el proceso de elaboración de esta Propuesta Conjunta debe desarrollarse fomentando una amplia participación, en los grupos de trabajo, foros o audiencias que se realicen, de entidades y organizaciones tanto públicas como privadas, con el fin de lograr el más amplio consenso institucional y social»[44]. No obstante, este documento de carácter declarativo, siendo importante, no tiene un carácter normativo y no obliga a los Estados que todavía no hayan aprobado leyes adecuadas, lo que perjudica a los intercambios de datos personales[45]. Para disponer de un instrumento normativo internacional es necesario que su aprobación siga las reglas del Derecho Internacional Público, lo que requiere la intervención de representantes de los Estados y un largo proceso de maduración[46]. La propia Resolución de Madrid «expresa la convicción de la Conferencia de que el reconocimiento de estos derechos pasa por la adopción de un instrumento legislativo universal y vinculante, que haga uso, consagre y complemente los principios comunes de protección de datos y de respeto a la privacidad enunciados en los diferentes instrumentos existentes y que refuerce

---

otros. De nada sirve empecinarse en una propuesta nacional o europea muy exigente –de máximos– si en otros ámbitos geográficos se defienden posiciones más flexibles, por lo que se impone una aproximación realista en un proceso negociador de estas características.

44. En los distintos grupos de trabajo participaron no sólo representantes de las autoridades sino también de la sociedad civil, la industria y la Universidad. Como señala Artemi Rallo, «su carácter consensuado aporta dos valores añadidos esencialmente novedosos: de un lado, enfatiza la vocación universal de los principios y garantías; del otro, reafirma la factibilidad de avanzar hacia un documento internacionalmente vinculante, que contribuya a una mayor protección de los derechos y libertades individuales en un mundo globalizado y, por ello, caracterizado por las transferencias internacionales de información». Cfr. RALLO LOMBARTE, A., «Presentación» a *Estándares Internacionales sobre Protección de Datos Personales y Privacidad*, AEPD, 2009. Lógicamente, las Autoridades Nacionales de Protección de Datos deben tratar de impulsar los trabajos necesarios que permitan extraer consecuencias concretas a partir de la aprobación de esta Resolución. Esta es una cuestión que corresponde principalmente en nuestro país a la Agencia Española de Protección de Datos.

45. Como hemos señalado en otro momento –*op. cit.* pp. 1890-1902–, la Conferencia Internacional de Protección de Datos y la Conferencia de Primavera de Autoridades Europeas no están constituidas en virtud de Tratados o Convenios Internacionales y, por tanto, no se trata de la participación en ninguna organización internacional regida por el Derecho internacional general. Estas Conferencias son un foro de debate teórico sobre cuestiones de actualidad que afectan a la protección de datos personales y de intercambio de experiencias entre las distintas Autoridades que tienen que aplicar en el día a día el derecho fundamental. Estas Conferencias también tienen una sesión cerrada sólo para autoridades de control, que sirve para aprobar declaraciones sin valor jurídico como la Resolución de Madrid, que incluso, en algunas ocasiones, han estado en contradicción con la propia opinión de los Estados. En la actualidad, al mismo tiempo que se debate el nuevo marco europeo de protección de datos personales tanto en la Unión Europea como en el Consejo de Europa, se está planteando una reforma de la estructura de la Conferencia Internacional de Autoridades de Protección de Datos, para dotarla de un Comité Ejecutivo y darle una mayor importancia a la sesión cerrada.

46. En parte, las facilidades para aprobar la Resolución de Madrid han sido consecuencia de una estrategia de *wait and see* de muchas autoridades de control y de que ésta no tenga un carácter normativo.

la cooperación internacional entre autoridades de protección de datos»[47]. La Resolución de Madrid es vista como «un nuevo paso hacia la elaboración, en el momento oportuno, de un instrumento internacional vinculante», como una llamada para la aprobación de un convenio universal para la protección de las personas con respeto al tratamiento de datos personales. Por ello, el objetivo más ambicioso de la Resolución –y al que quedan encomendadas las autoridades de protección de datos– es promover esta misma propuesta conjunta «como base para un futuro trabajo para la elaboración de un Convenio universal vinculante, y en particular entre las instituciones» –art. 4.a) de la Resolución–[48]. La Resolución tiene también un objetivo más modesto, que es servir para regular las transferencias internacionales de datos. De hecho, señala que «las disposiciones del presente Documento constituirán base apropiada para permitir las transferencias internacionales de datos de carácter personal –art. 4.2 de la Propuesta Conjunta para la Redacción de los Estándares Internacionales–[49].

En todo caso, hay que recordar que existen en la actualidad instrumentos internacionales de protección de datos personales. No nos referimos en este caso a la Directiva 95/46/CE, que afecta únicamente a la Unión Europea, sino especialmente al Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, que ha desarrollado el art. 8 del CEDH y que ha jugado hasta ahora un papel importante como estandar internacional. Ha sido éste el primer instrumento internacional vinculante en materia de protección de datos personales en los sectores público y privado, que no sólo ha reconocido sino que ha fijado los elementos principales del contenido del derecho fundamental a la protección de datos personales, debiendo destacarse el importante papel jugado por la jurisprudencia del Tribunal Europeo de Derechos Humanos para lograr el reconocimiento y tutela del derecho fundamental a la protección de datos personales[50]. Por ello, el Convenio 108 del Consejo de Europa –y su Protocolo Adicional relativo a autoridades de supervisión y transferencias internacionales– ha sido el documento base para la discusión de una norma internacional para la protección de datos personales. La aprobación de una

47. Cfr. la Nota explicativa de la Resolución de Madrid.
48. Cfr. el apartado 4 de la Resolución.
49. En otro momento la Resolución señala que el documento puede ser utilizado «como base para el desarrollo de la comprensión y la cooperación internacional sobre protección de datos y privacidad, particularmente en el contexto de permitir las transferencias internacionales de datos personales, que tendrán lugar de un modo que proteja los derechos y libertades de los individuos» –art. 4.b) de la Resolución–.
50. El Tribunal Europeo de Derechos Humanos incluyó a partir de 1987 dentro del derecho a la vida privada reconocido en el Convenio, el derecho a la protección de datos personales, desgranando en los últimos veinticinco años una interesante jurisprudencia que ha definido los elementos principales de este derecho fundamental. Cfr. RUIZ MIGUEL, C., *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*, Civitas, Madrid, 1994; QUERALT JIMÉNEZ, A., *El Tribunal de Estrasburgo: una jurisdicción internacional para la protección de los derechos fundamentales*, Tirant lo Blanch, Valencia, 2003, pp. 71-122.

norma internacional no es necesariamente incompatible con promover la ratificación del Convenio 108 del Consejo de Europa por países no europeos que cuenten con una legislación adecuada[51]. Además, la normativa del Consejo de Europa mantiene una importante influencia tanto en la Unión Europea[52] como

51. Este Convenio ha sido suscrito hasta la fecha por 43 países, la mayoría del continente europeo. En el mes de marzo de 2012, la Comisionada presidenta del Instituto Federal de Acceso a la Información y Protección de Datos de Méjico (IFAI) Jacqueline Peschard planteó ante la secretaria general adjunta del Consejo de Europa (CE), Maud de Boer-Buquicchio, el interés de México por adherirse al Convenio 108. Previamente Uruguay ya había solicitado formalmente su adhesión el pasado 6 de julio de 2011. También la Resolución de Madrid expresa el apoyo de la Conferencia Internacional a los esfuerzos del Consejo de Europa para impulsar el derecho a la protección de los datos personales e «invita a los Estados, sean o no miembros de la organización, a ratificar el Convenio». Cfr. la *Nota Explicativa de la Resolución*, donde también se muestra el apoyo de la Conferencia Internacional a las acciones llevadas a cabo por la APEC, la OCDE y otros foros regionales e internacionales con vistas a desarrollar herramientas que fomenten unos mejores estándares internacionales de privacidad y protección de datos personales. Igualmente, *la Declaración de la Sociedad Civil sobre Estándares de Privacidad en un Mundo Global, de 3 de noviembre de 2009*, exhortó «a los países que no hayan ratificado la Convención 108 del Consejo de Europa junto con el Protocolo 2001 para que lo hagan con mayor celeridad». España ha tardado muchos años en ratificar el Protocolo Adicional (Convenio 181) al Convenio 108 a pesar que desde el año 2001 se abrió para su firma. Finalmente lo ha hecho con fecha de 3 de junio de 2010 y ha entrado en vigor el 1 de octubre de 2010. También la Resolución de la Sociedad Civil antes citada menciona las Directrices de Privacidad de la OCDE, de 1980. Hay que señalar que el 28 de enero de 2011, el Consejo de Europa y la Comisión Europea organizaron una conferencia sobre la necesidad de establecer unas normas de protección de datos comunes a escala mundial.
52. Como señaló el comisario Bolkestein en la sesión de clausura de la Conferencia sobre la aplicación de la Directiva, «[c]iertamente no se parte de una hoja en blanco cuando se trata de tomar medidas en el ámbito de la protección de datos (...). Al elaborar su informe, la Comisión [...] deberá tener en cuenta el marco jurídico y político general, en concreto, los principios formulados en el Convenio 108 del Consejo de Europa». Cfr. *Primer informe sobre la aplicación de la Directiva* cit. Como es sabido, el Tribunal de Justicia señaló la imposibilidad de la adhesión de la Comunidad Europea al CEDH señalando que la Comunidad carecía de competencias en esta materia –Dictamen 2/1994, de 28 de marzo de 1996–. Con la entrada en vigor del Tratado de la Unión Europea –antiguo art. F– se estableció que: «1. La Unión se basa en los principios de libertad, democracia, respeto de los derechos humanos y de las libertades fundamentales y el Estado de Derecho, principios que son comunes a los Estados miembros. 2. La Unión respetará los derechos fundamentales tal y como se garantizan en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales firmado en Roma el 4 de noviembre de 1950, y tal y como resultan de las tradiciones constitucionales comunes a los Estados miembros como principios generales del Derecho comunitario». Recientemente el Consejo de Europa ha hecho pública su *Estrategia sobre Internet 2012-15 para la protección y el respeto de los derechos humanos de los usuarios, el Estado de Derecho y la democracia en la red*, que incluye cuarenta líneas de actuación concretas que tratan de hacer de Internet un espacio abierto y centrado en los ciudadanos. Entre estas prioridades destacan la protección de los datos y la privacidad, la protección de los menores, aprovechar el potencial de Internet para promover la democracia, la transparencia y la diversidad cultural, y la cooperación internacional contra el cibercrimen.

en sus Estados miembros[53], y debe ser un punto de referencia, al igual que la jurisprudencia del Tribunal de Estrasburgo, para la elaboración del nuevo marco normativo europeo de protección de datos. Pero, por este mismo hecho hay que reconocer que el Convenio 108 es un documento básicamente europeo –eurocéntrico–, siendo indispensable que la normativa internacional de protección de datos incorpore una visión más amplia que acoja el ámbito geográfico americano y de asia-pacífico.

En la actualidad, en el ámbito del Consejo de Europa se está negociando la redacción de un nuevo Tratado internacional, que reforme y actualice el Convenio 108[54]. No nos corresponde ahora analizar el contenido de la reforma del Convenio 108, que tiene una intensa coincidencia con la propuesta de Reglamento en muchos aspectos –por ejemplo, la transparencia de la información al interesado o el fortalecimiento de las autoridades de control–. Hay dos cuestiones que hay que destacar de los documentos sobre la modernización del Convenio 108. La primera es la preocupación por asegurar la compatibilidad de la normativa del Consejo de Europa con la de la Unión Europea, algo que también está presente en la propuesta de Reglamento general de protección de datos personales. Es interesante comprobar que se están reformando a la vez dos instrumentos de protección de datos y que ambos tienen la vocación de ser compatibles. En segundo lugar, el interés del Consejo de Europa por mantener el carácter abierto del Convenio, lo que permite la adhesión por países no europeos y refuerza su potencial carácter de estándar internacional

B) La autorregulación: privacidad en el diseño y privacidad por defecto

Otro elemento que puede contribuir a alcanzar unos estándares internacionales de protección de datos es la autorregulación[55]. Cualquier régimen normativo puede resultar insuficiente cuando los datos personales se difunden por todo el mundo a través de las redes de TIC y en su tratamiento intervienen varias jurisdicciones, a menudo fuera de la UE. Por ello, la Comisión entiende que es necesaria la utilización de las propias tecnologías como aliadas para

53. Mientras la Carta de Derechos Fundamentales de la Unión Europea y el derecho derivado institucional sólo obligan a los Estados miembros en la ejecución del Derecho de la Unión Europea, el Convenio 108 y el CEDH vincula a los Estados en la actuación de todos sus poderes públicos.

54. En octubre de 2011, el Buró del Comité Consultivo de la Convención 108 (T-PD-BR) se reunión en Estrasburgo para analizar las posibles modificaciones al Convenio 108 y a su Protocolo Adicional. Las propuestas de reforma se discutieron en el Pleno del Consejo del Comité Consultivo Europeo, del 29 de Noviembre al 2 de Diciembre de 2011. Durante el año 2011 se abrió una consulta sobre la modernización del Convenio 108. Hay un documento sobre propuestas de modernización, de 27 de abril de 2012, y un documento final sobre la modernización del Convenio 108, de 17 de septiembre de 2012 –*http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation*–.

55. Así, la propia Resolución de Madrid contiene un conjunto de medidas proactivas entre las que están «la adhesión a acuerdos de autorregulación cuya observancia resulte vinculante, que contengan elementos que permitan medir sus niveles de eficacia en cuanto al cumplimiento y grado de protección de los datos de carácter personal y establezcan medidas efectivas en caso de incumplimiento» –art. 22–.

favorecer el respeto a este derecho, a través de la implantación de las llamadas «tecnologías de protección de la privacidad» –PET–[56]. Con estas iniciativas, se trata de alcanzar sinergias con la industria para que ésta proporcione equipos y software que permita el cumplimiento de la legislación de protección de datos personales. Para la Comisión, si bien «la responsabilidad jurídica del cumplimiento de las normas de protección de datos personales recae en los responsables de su tratamiento, desde el punto de vista social y ético también recae en parte, por ejemplo, en quienes elaboran las especificaciones técnicas y quienes realmente desarrollan o ejecutan programas o sistemas operativos». De igual forma, la Comisión Europea y las autoridades de protección de datos están convencidas de que la mejora del nivel de cumplimiento del derecho fundamental a la protección de datos personales pasa por una labor de promoción que trate de poner este derecho fundamental en positivo. Así, frente a una cierta prevalencia de una imagen negativa de la protección de datos personales –con mensajes como el de que nadie cumple esta legislación–, es necesario lanzar una idea positiva de la protección de datos personales involucrando al propio sector, como por ejemplo, a través de la aprobación de Códigos de Conducta[57] o el establecimiento de un modelo de certificación en privacidad para productos y servicios[58], como los sellos de

56. Las PET son «un sistema coherente de medidas de TIC que protege el derecho a la intimidad suprimiendo o reduciendo los datos personales o evitando el tratamiento innecesario o indeseado de datos personales, sin menoscabo de la funcionalidad del sistema de información». La propia Directiva 2002/58/CE establece que «cuando proceda, se podrán adoptar medidas para garantizar que los equipos terminales estén fabricados de manera compatible con el derecho de los usuarios de proteger y controlar el uso de sus datos personales» –art. 14.3–. Cfr. la *Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET)* –COM (2007) 228 final–, de 2.5.2007, en *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:ES:PDF*. Así, «gracias a dichas tecnologías, las infracciones de las normas de protección de datos y la vulneración de los derechos del ciudadano, además de estar prohibidas y sujetas a sanciones, resultarían más difíciles desde el punto de vista técnico». Esta Comunicación de la Comisión es consecuencia del Primer *informe sobre la aplicación de la Directiva sobre protección de datos*, cit. y enlaza con la Comunicación de la Comisión «Una estrategia para una sociedad de la información segura» [COM (2006) 251, de 31 de mayo de 2006], donde se invitaba al sector privado a «estimular el despliegue de productos, procesos y servicios que favorezcan la seguridad a fin de evitar y combatir la sustracción de la identidad y otros ataques contra la privacidad». Con esta comunicación, la Comisión trata de fomentar la utilización de las PET por parte de los responsables del tratamiento de datos y los consumidores.

57. Estos Códigos Tipo están previstos en la Directiva 95/46/CE –arts. 27-28–, en la LOPD –art. 32– y han tenido un impulso en el RPDP –arts. 71-78–, que ha previsto incluso garantías para su cumplimiento a través de órganos de supervisión independientes y de la imposición de sanciones.

58. Así, hay que señalar que la propia Comisión Europea, en su Comunicación al Parlamento Europeo y al Consejo –*ibídem*–, ha incidido en la necesidad de «un sistema europeo de distintivos de protección de la intimidad, que incluiría asimismo un análisis de las repercusiones económicas y sociales. Gracias a dichos distintivos, los consumidores podrían reconocer fácilmente los productos que cumplen o favorecen el cumplimiento de las normas de protección de datos en el tratamiento de éstos, en concreto mediante la aplicación de PET apropiadas».

privacidad[59]. La defensa de la privacidad se muestra, de esta manera, como una oportunidad de negocio y una ventaja competitiva para las empresas. Además, en relación con el funcionamiento de la economía, un sistema de certificación europeo en privacidad facilita los intercambios comerciales entre los distintos países, creando nuevas oportunidades de mercado. Obviamente, la generalización de un modelo de certificación obliga a resolver cuestiones como la configuración de la autoridad de certificación que valide las evaluaciones realizadas por los expertos o la acreditación de los expertos jurídicos y técnicos que realicen las evaluaciones –haciendo posible la obtención por su parte de un legítimo beneficio pero evitando su captura por parte de empresas–. Es razonable una cierta implicación de las autoridades de protección de datos dentro de un modelo de certificación –en la definición de reglas y procedimientos pertinentes y en la supervisión del funcionamiento del mismo–, siendo importante no confundir los reguladores con los regulados –la autoridad de control son las Agencias de Protección de Datos; la autoridad de certificación y las empresas de auditoría son sectores regulados y sometidos a control–[60].

La propuesta de Reglamento general de protección de datos que presenta la Comisión no sólo ha avanzado aún más en esta apuesta por la autorregulación

59. La *Commission Nationale de l'Informatique et de Libertés* de Francia ha puesto en marcha una certificación en privacidad en su país, algo que exigía su legislación. Hay que destacar el *Proyecto EuroPriSe*, que trataba de poner las bases para el establecimiento de un sello europeo de privacidad para productos y servicios de tecnologías de la información en los sectores público y privado, que fue financiado por la Comisión Europea a través del programa eTEN. El proyecto *EuroPriSe* ha sido impulsado por la Autoridad de Protección de Datos de Schleswig-Holstein y en el participan la *Commission Nationale de l'Informatique et de Libertés* (Francia), la Agencia de Protección de Datos de la Comunidad de Madrid y otros socios como *Independent Centre for Privacy Protection* de Schleswig-Holstein (Alemania), *London Metropolitan University-Londonmet* (Reino Unido), *VaF s.r.o.* (Eslovaquia), *Ernst & Young Sweden* (Suecia),) *TÜV Informationstechnik GmbH* (Alemania), *Austrian Academy of Science, Institute of Technology Assessment* (Austria) y *Borking Consultancy* (Países Bajos). El Supervisor Europeo de Protección de Datos destacó en su Informe Anual de 2008 la importancia del proyecto *EuroPriSe*: Cfr. el *Annual Report 2008*, del Supervisor Europeo de Protección de Datos, p. 85 en *http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2008/AR2008_EN.pdf* Sobre EuroPriSe, cfr. más ampliamente *Privacy Law & Business*, Newsletter núm. 35, febrero, 2008, pp. 12-15. Cfr. también la información que obra en *www.european-privacy-seal.eu/*

60. La Comisión Europea incide en que las autoridades de protección de datos deben formar parte de grupos que se encarguen de analizar la evolución de la tecnología, detectar los peligros que plantea en relación con los derechos fundamentales y la protección de datos personales y definir los requisitos técnicos para hacerles frente. Cfr. la *Comunicación de la Comisión al Parlamento Europeo y al Consejo*, ya citada. Una de las cuestiones a resolver, también dentro del ámbito de la autorregulación, es la definición del parámetro utilizado para evaluar los productos por los expertos acreditados. Este parámetro para la evaluación debía ser hasta ahora, lógicamente, la Directiva 95/46/CE, pero ésta ha sido transpuesta de manera diferente en los distintos países, persistiendo divergencias y faltas de armonización a nivel europeo. Esto nos lleva, de nuevo, a la necesidad de reformar la normativa europea de protección de datos.

sino que ha convertido muchas de estas medidas en obligaciones del responsable del tratamiento. Así, señala claramente que la protección de datos personales debe ser tenida en cuenta en el diseño del sistema de información –la llamada «privacidad en el diseño», *privacy by design*–, fijando para ello obligaciones para el responsable, tanto en el momento de la determinación de los medios de tratamiento como en el del tratamiento propiamente dicho, de implementar medidas y procedimientos técnicos y organizativos apropiados que garanticen la protección de los datos personales –art. 23–. Además señala que la protección de datos debe ser una opción por defecto –la llamada «privacidad por defecto»–, que se materializa en la obligación del responsable del tratamiento de establecer mecanismos que permitan que, por configuración inicial, sólo sean objeto de tratamiento los datos necesarios para cada fin específico, de manera que no se recojan ni se conserven datos más allá del mínimo necesario para los fines, tanto en lo que respecta a la cantidad de los datos como a la duración de su conservación, estableciéndose, asimismo, mecanismos que garanticen que, por defecto, los datos personales no sean accesibles a un número indeterminado de personas[61]. De esta forma, no recae sobre el usuario la selección inicial de las medidas de privacidad, sino que ésta viene ya configurada por defecto, una medida de necesaria aplicación, por ejemplo, tanto en lo relativo a las redes sociales[62] como al uso de coo-

61. La Propuesta Conjunta para la Redacción de Estándares Internacionales apostó también por medidas proactivas en defensa de la privacidad –art. 22–. Pero fue sobre todo la XXXII Conferencia Internacional de Autoridades de Protección de Datos celebrada en Israel en el año 2010 la que adoptó una Resolución en la que se reconoce a la privacidad por diseño –y, dentro de ella, a la privacidad por defecto– como un elemento fundamental, instando a las Autoridades de Control a promover su implantación. Así, se materializa una preocupación porque el software se desarrolle desde el principio teniendo en cuentas las exigencias en materia de privacidad y las principales amenazas y que la privacidad también sea un factor a tener en cuenta en el diseño de los servicios y procesos dentro de las empresas.

62. Las redes sociales deben avanzar en la privacidad por defecto en lo que hace referencia a los niveles de acceso a los datos personales publicados en el perfil –uno de los principales parámetros de confidencialidad–, la cesión de datos de otras personas sin su consentimiento o el establecimiento de canales de denuncia. Así, es necesario que las redes sociales modifiquen sus configuraciones por defecto relativas al nivel de acceso a las páginas personales, evitando que la configuración inicial prevea que toda la información esté en abierto, limitando el nivel de publicidad para que la información sea accesible únicamente para los amigos y no para los amigos de éstos. De esta forma, los usuarios se ven obligados a aceptar expresamente que personas distintas de sus contactos van a acceder al perfil, lo que reduce el riesgo para su privacidad. Sin embargo, en la actualidad la mayoría de las redes sociales establecen por defecto la accesibilidad del perfil no sólo para los amigos sino también para los amigos de los amigos –las personas que forman parte de la lista de contactos de los amigos–. Hay que tener en cuenta que en las redes sociales el consentimiento se ejerce habitualmente aceptando la política de privacidad establecida por defecto. También los códigos de buenas prácticas de las redes sociales tendrían que ir encaminados a que los usuarios no cedieran datos de otras personas –por ejemplo, fotografías o su etiquetado– sin su consentimiento. Asimismo, es necesario que las redes sociales tengan canales de denuncia para hacer desaparecer una intromisión ilegítima en los derechos de las personas, garantizando la respuesta a las solicitudes en un plazo breve de tiempo y eliminando el comentario o la fotografía lesiva con la intimidad de las personas o sobre la que se ha ejercicio un derecho de

kies[63]. La propuesta de Reglamento también defiende los Códigos de conducta –art. 38–, que están destinados a contribuir a la aplicación del Reglamento en sectores de tratamiento específicos y en los que debe implicarse tanto los Estados miembros como las autoridades de control y la propia Comisión, a la que se le faculta para decidir sobre la validez general de los códigos de conducta[64]. Buena muestra de esta apuesta por la autorregulación es que los Códigos de conducta pueden incluir otros procedimientos extrajudiciales y de resolución de conflictos, que permitan resolver las controversias entre los responsables y los interesados, pero todo ello debe ser sin perjuicio de los derechos de los interesados y de su posibilidad de acudir a las autoridades de control. La propuesta de Reglamento también establece que la Comisión y los Estados miembros promoverán la creación de mecanismos de certificación y de sellos en materia de protección de datos que permitan a los interesados evaluar rápida-

---

oposición. Las redes sociales deben también sancionar en el ámbito de su comunidad virtual a aquellas personas que vulneren la intimidad o la protección de datos personales de terceros, publicando fotografías o vídeos de otras personas con su oposición o realizando comentarios que sean poco respetuosos con terceras personas. A nuestro juicio, si bien la responsabilidad civil les correspondería a los autores de la vulneración del derecho a la intimidad y a la protección de datos personales de terceras personas, las redes sociales también tendrían una responsabilidad al ser titulares del medio donde se publica la información, especialmente cuando no son diligentes en la cancelación de la misma si ha sido solicitado previamente por el perjudicado. En general, se echa en falta un adecuado diseño de las plataformas de las redes sociales para reducir los problemas relacionados con la privacidad. Recientemente *Google+* ha lanzado una nueva función para los usuarios de la red social, de forma que todos los usuarios que tengan una cuenta y utilicen el servicio de *Google Contact* para gestionar su libreta de direcciones puedan ver la información de sus contactos desde su perfil de la red social, integrándola dentro de la misma. No obstante, en este caso esta información sólo puede ser vista de forma privada por el usuario y no será un dato al que tengan acceso sus contactos de *Google+*.

63. En la actualidad, la configuración por defecto de tres de los cuatro navegadores más utilizados está predeterminada para aceptar todas las *cookies*, obligando al usuario a modificar la configuración inicial si desea bloquearlas. De esta forma, la mera visita a una página web, si el usuario no hace nada, supone una transmisión de datos de carácter personal al servidor solicitado a través de la comunicación de los navegadores, sin que el usuario tenga siquiera conocimiento. Por ello, es especialmente importante que las tecnologías incorporen medidas que permitan al ciudadano el derecho efectivo a controlar los datos personales que saltan de su terminal, lo que implica el consentimiento para las *cookies*. Hay que mencionar una iniciativa en el ámbito de la autorregulación como son las Plataformas de Preferencias de Privacidad –P3P–, que facilitan que la transmisión de datos entre el usuario y el sitio web sea acorde con sus preferencias en materia de privacidad. Esta plataforma permite la búsqueda y lectura de las políticas de privacidad sin que el usuario la lea cada vez que acceda al sitio web, facilitando a éste la información y la toma de decisiones –en este caso, automatizadas o pseudoautomatizadas– en función de las políticas de privacidad de cada sitio web. Esta Plataforma es complementaria con otras tecnologías de protección del derecho a la intimidad (PET), como son los anuladores de *cookies*.

64. La regulación de estos Códigos de conducta en la propuesta de Reglamento incluye referencias novedosas al tratamiento equitativo y transparente, a la información al público, a la protección de los niños y a los mecanismos de supervisión y garantía –que toma de nuestro RPDP–.

mente el nivel de protección de datos que ofrecen los responsables y los encargados del tratamiento –art. 39–. Estas medidas, junto con otras como la realización de informes de impacto en la protección de datos personales, la implementación de mecanismos de verificación y auditoría de carácter jurídico o la designación de un delegado de protección de datos, que dejan de ser iniciativas de autorregulación para convertirse en la propuesta de Reglamento en obligaciones del responsable, tratan de introducir la protección de datos dentro de la responsabilidad empresarial, convirtiendo a las empresas en un elemento estratégico en el sistema de garantías del derecho a la protección de datos personales, que haga compatible un uso intensivo de las tecnologías y el tratamiento de datos personales necesarios para el funcionamiento global de la economía con el respeto a la privacidad de los usuarios y de los empleados.

Por ello, es imprescindible que las autoridades de control eviten las posiciones frentistas en relación con las empresas y sean capaces de generar entornos de colaboración, lo que no significa ceder ante la industria –que no deja de ser un *stakeholder*– sino de alcanzar un diálogo que permitan la *privacy by design* y la privacidad por defecto. Internet se caracteriza por la desaparición de las fronteras administrativas y por favorecer la interacción de sujetos que se encuentran en diferentes puntos geográficos y sometidos a normas distintas. La autorregulación es, por ello, una respuesta ágil cuando falte una regulación jurídica en el ámbito nacional o internacional, ante situaciones de gran complejidad técnica o ante la imposibilidad de llegar a todos los ámbitos a través de una actividad administrativa de inspección y control, pudiendo contribuir a la protección de los derechos del usuario. Sin embargo, como hemos señalado en otro momento, la autorregulación aporta únicamente una solución complementaria y no puede ser la garantía única sobre la que descanse la privacidad de los usuarios. Los Estados y las entidades internacionales y supranacionales son los últimos garantes del interés público y no deben renunciar a la regulación y a la supervisión. Las normas jurídicas surgen, de hecho, como garantía de la privacidad frente a las malas prácticas movidas por intereses económicas. Las exigencias privadas a través de la autorregulación no llegan a garantizar con plenitud los derechos de los afectados.

IV. LAS DIVERGENCIAS EN LA PROTECCIÓN DE LOS DATOS PERSONALES ENTRE LOS ESTADOS MIEMBROS

La Comisión Europea había afirmado en el pasado que, pese los retrasos y lagunas en su aplicación, la Directiva había cumplido su principal objetivo de eliminar los principales obstáculos a la libre circulación de datos personales entre los Estados miembros derivados de la ausencia de legislación[65]. No obs-

65. La principal dificultad anterior a la adopción de la Directiva era que, mientras la mayoría de los Estados miembros habían adoptado legislación sobre protección de datos, unos pocos no lo habían hecho. En 1995, únicamente Italia y Grecia carecían de ese tipo de legislación, pero, en cambio, ambos Estados miembros fueron de los primeros que transpusieron la Directiva, por lo que se eliminó la principal dificultad. Cfr. *Primer informe sobre la aplicación de la Directiva*, cit. De hecho, en el *Segundo informe de aplica-*

tante, la Comisión también había considerado reiteradamente que las divergencias sobre protección de datos en los Estados miembros eran todavía demasiado grandes[66]. Estas divergencias provienen tanto de la propia legislación de los

ción de la Directiva –cit.–, la Comisión entendía que la Directiva «constituye un marco jurídico general que cumple con sus objetivos originales constituyendo una garantía suficiente para el funcionamiento del mercado interior asegurando al mismo tiempo un alto nivel de protección». Así, «los principios que figuran en la Directiva siguen siendo válidos» y «no tiene previsto presentar ninguna propuesta legislativa para modificar la Directiva».

66. Igualmente, el bajo nivel de armonización en relación a la transposición de la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15.3.2006, sobre conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes de comunicaciones –por la que se modifica la Directiva 2002/58/CE– causa, a juicio de la Comisión, perjuicios a los proveedores de servicios de telecomunicaciones, especialmente a los operadores de menor tamaño. Esta Directiva exige a los Estados miembros que garanticen que los operadores de telecomunicaciones conservan determinadas categorías de datos –números de teléfono, direcciones IP o identificadores de teléfonos móviles– para proporcionar detalles sobre las llamadas telefónicas efectuadas y los correos electrónicos enviados –excluyendo el contenido de tales comunicaciones– con fines de investigación, detección y enjuiciamiento de delitos graves, tal como vengan definidos en cada legislación nacional. Esta Directiva nació como respuesta a los problemas de seguridad vinculados a los atentados terroristas de Madrid en 2004 y de Londres en 2006 y ha servido para mejorar el funcionamiento de la justicia penal y la aplicación de las Leyes, aportando pruebas que han permitido resolver delitos graves como los vinculados a las redes de pederastia. Un reciente informe de la Comisión Europea, de 19 de abril de 2011 –realizado en el marco de la obligación de la Comisión de evaluar la aplicación de la Directiva establecido en su art. 14–, ha señalado que las legislaciones nacionales la han incorporado de manera desigual y que siguen existiendo diferencias entre las legislaciones de los Estados miembros, por ejemplo, en los periodos de conservación –que varían entre seis meses y dos años–, los fines para los que se puede acceder, los procedimientos legales para acceder a los datos o las compensaciones que reciben los operadores por los costes que conlleva conservar los datos y facilitar el acceso. La Comisión asume que la Directiva «únicamente pretende armonizar parcialmente las normas nacionales por lo que no es de extrañar que no exista un planteamiento común en este ámbito». Hay que tener en cuenta que la propia Directiva señala que los datos deberán conservarse por un plazo de tiempo no inferior a seis meses ni superior a dos años, periodo que debe ser decidido por cada Estado miembro al incorporar la Directiva a su legislación nacional. La intención de la Comisión es revisar la Directiva 2006/24/CE para tratar de reducir el número de datos de tráfico objeto de retención y el plazo de conservación, ofreciendo un mayor control sobre los datos que se transfieran a un tercer país.
La falta de precisión de algunos de los preceptos de la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25.11.2009, también ha dificultado su transposición. Muchos países, como es el caso de España, no habían realizado su transposición antes del plazo límite del pasado 25 de mayo de 2011 –sólo la habían transpuesto en plazo Dinamarca y Estonia–. Otros países como Gran Bretaña o Francia habían remitido notificaciones de implantación parcial. La Comisión Europea ha anunciado la apertura de procedimientos sancionadores. Así, por ejemplo, la Directiva no precisa qué debe entenderse por consentimiento. La industria defiende que los navegadores tienen herramientas para bloquear la acción de las cookies y si el internauta no las activa ya está mostrando su consentimiento. En cambio, las Autoridades de protección de datos discrepan de esta postura. Además, hay muy distintos tipo de *cookies* y con diferentes niveles de intrusión.

Estados miembros –de una inadecuada transposición de la Directiva 95/46/CE– como de la deficiente aplicación de la normativa de protección de datos personales en los Estados de la Unión Europea[67], lo que obedece a diversas causas.

A) Desde el margen de maniobra al incumplimiento de las exigencias de la Directiva en su transposición por la legislación de los Estados miembros.

Una de estas causas es la presencia en la Directiva de cláusulas abiertas –*open-ended principles*– que admiten una transposición diferente en la legislación de los distintos Estados[68]. Así, algunos legisladores han aprovechado estas cláusulas abiertas para adoptar una posición más estricta –este es el caso de España[69]–, mientras que otros han mantenido un posicionamiento bastante más

---

Hemos analizado en otro momento la utilización de *cookies* en los servicios de Administración electrónica para dar un servicio más personalizado en una próxima visita al sitio web –enviando un mensaje con las principales novedades desde la última visita, incluso adaptando la información en función de los intereses de cada usuario–, lo que contribuye a mejorar la satisfacción de los ciudadanos. Cfr. *op. cit.* pp. 626-645. Este sistema de seguimiento de la navegación en Internet supone en la mayoría de los casos un tratamiento de datos personales, por lo que requiere con carácter previo el cumplimiento de la información al interesado sobre la existencia del mismo –que la mayoría de las veces desconoce–, de su finalidad, de los destinatarios de la información, de la identidad del responsable y de los derechos que le asisten. A nuestro juicio la personalización de la información administrativa del sitio web es un servicio de valor añadido –una herramienta de marketing administrativo– que no forma parte de la función administrativa ni de la primera relación negocial o administrativa por lo que se requiere el consentimiento del interesado. Las cookies suponen, cuando no existe información ni consentimiento del interesado, una recogida de datos por medios fraudulentos, desleales o ilícitos. Además, debe existir un contrato de encargado de tratamiento cuando lo hacen a través de empresas externas –como es el caso de Nielsen– que no pueden tratar los datos para fines propios sino para prestar un servicio a la Administración.

67. El considerando 7 *in fine* de la Propuesta de Reglamento establece que «la diferencia en los niveles de protección se debe a la existencia de divergencias en la ejecución y aplicación de la Directiva 95/46/CE».

68. Como es sabido dentro del Derecho derivado institucional, hay que distinguir los reglamentos, que agotan la regulación de una materia sin dejar margen de acción a los Estados o dejando a éstos un margen de acción mínimo, de las Directivas como la 95/46/CE, que fijan las grandes líneas de regulación de una materia, así como los objetivos que deben alcanzar los Estados miembros, que pueden completar esa regulación. Es decir, la Directiva, a diferencia de los Reglamentos, permite un margen de actuación a los Estados en su transposición ya que suponen obligaciones «al Estado miembro destinatario en cuanto al resultado que debe conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios» –art. 288– TFUE–.

69. Algunos preceptos de la LOPD, por su carácter restrictivo, se separan de la Directiva. Esto ocurre, por ejemplo, en la regulación de la legitimidad para el tratamiento –por ejemplo, en relación con las excepciones al consentimiento y con la comunicación de datos personales–, de las notificaciones de los tratamientos y de las transferencias internacionales de datos –cuestiones a las que más adelante nos referiremos–. La explicación se encuentra en que la LOPD trató de transponer la Directiva 95/46/CE sin apartarse en exceso de la LORTAD –de hecho lo que aprueba inicialmente el Gobierno es un proyecto de Ley de modificación de la LORTAD–, y ésta última tiene un carácter muy garantista ya que en su elaboración se tuvieron en cuenta los borradores de la Directiva, que fueron mucho más restrictivos que el texto finalmente aprobado –resul-

flexible. Esto se evidencia, por ejemplo, en las diferencias legislativas entre los Estados miembros en lo relativo a los requisitos de notificación, las condiciones para las transferencias internacionales, los números nacionales de identificación o la noción de finalidad específica[70]. Lógicamente, en el análisis de las divergencias en las legislaciones nacionales de los Estados miembros hay que tener en cuenta también que lo que propone la Directiva es la aproximación, no la completa uniformidad, y que, para respetar el principio de subsidiariedad, el proceso de aproximación no debe llegar más lejos de lo necesario[71]. Hay que señalar que el art. 5 de la Directiva, que inicia el Capítulo II titulado «Condiciones generales para la licitud del tratamiento de datos personales», señala que los Estados miembros precisarán, dentro de los límites de ese Capítulo, «las condiciones en que son lícitos los tratamientos de datos personales». Por tanto, los Estados, como señala su Considerando 9, disponen de un cierto «margen de maniobra» del cual podrán servirse, en el contexto de la aplicación de la Directiva, lo que les permite precisar en su derecho nacional las condiciones generales de licitud del tratamiento de datos. Esto hace que dentro de los límites de dicho margen de maniobra y de conformidad con el Derecho de la Unión Europea, puedan surgir algunas «disparidades en la aplicación de la Directiva» que podrán tener «repercusión en la circulación de datos tanto en el interior de un Estado miembro como en la Comunidad». La Directiva 95/46/CE contiene normas que se caracterizan por una cierta flexibilidad y deja en muchos casos en manos de los Estados miembros la tarea de regular los detalles o de elegir entre varias opciones[72]. Como ha señalado la jurisprudencia del Tribunal de Justicia, el respeto del derecho a la vida privada en lo que respecta al tratamiento de los datos de carácter personal, reconocido por los artículos 7 y 8 de la Carta no impide, como señalan los art. 8.2 y 52.1 de la Carta que, bajo ciertas condiciones, puedan introducirse limitaciones a dicho derecho, «correspondiéndole a los Estados miembros, a la hora de adaptar su ordenamiento jurídico a la Directiva 95/46/CE, procurar basarse en una interpretación de ésta que les permita garantizar un justo equilibrio entre los distintos derechos y libertades fundamentales protegidos por el ordenamiento jurídico de la Unión»[73]. De esta forma, el margen de apreciación de que disponen los Estados miembros «únicamente puede utilizarse de conformidad con el objetivo perseguido por la Direc-

---

tado de una difícil negociación con el modelo anglosajón de protección de datos, más flexible que el continental–.

70. Así, la Ley Británica al igual que la española establecen que la finalidad debe ser incluida en la información que se ofrece al interesado y en la notificación a la autoridad de control, lo que no ocurre en otros países.
71. Téngase en cuenta también el diferente estatus de las leyes nacionales que transponen la Directiva en los ordenamientos jurídicos nacionales. Así, en algunos países estas leyes tienen el carácter de normas cuasi-constitucionales –que complementan la Constitución– mientras que en otros el Parlamento puede aprobar leyes que modifiquen las leyes que transponen la Directiva. Esto parece ser, al menos, el caso de Gran Bretaña y Suecia.
72. Cfr. Sentencia *Lindqvist*, cit. apdo. 83.
73. STJUE, de 29.1.2008, as. *Promusicae*, (C-275/06), apdo. 68.

tiva 95/46/CE, que consiste en mantener un equilibrio entre la libre circulación de datos personales y la tutela del derecho a la intimidad»[74].

Otra de las causas de las divergencias en la normativa de protección de datos personales entre los Estados miembros es que éstos se han salido fuera del margen de maniobra que permite la Directiva, incumpliendo sus exigencias y sobrepasando sus límites. El Tribunal de Justicia ha reiterado en la Sentencia de 24 de noviembre de 2011, como ya señaló en la Sentencia *Lindqvist*, «lo que es un dato esencial de la Directiva 95/46. Esta norma no es una directiva de mínimos. Se declara así que la armonización de las legislaciones nacionales no se limita a una armonización mínima, sino que constituye, en principio, una armonización completa. En las directivas de mínimos, el legislador nacional puede elevar el nivel de protección propuesto por el legislador europeo, añadiendo supuestos adicionales a los previstos por éste. Sin embargo, las directivas de armonización completa funcionan como normas de «máximos». Esto es, impiden que el legislador nacional introduzca una protección más rigurosa de los datos personales o bien un ámbito de aplicación mayor que el previsto en las disposiciones de la Directiva». Además, como señala la Sentencia de 24 de noviembre de 2011, citando una reiterada jurisprudencia del Tribunal de Justicia, hay preceptos de la Directiva 95/46/CE que, desde el punto de vista de su contenido, introducen una obligación incondicional y son suficientemente precisos, por lo que tienen efecto directo, de manera que una incorrecta transposición de sus disposiciones por parte del Estado –cuando éste no haya adaptado el Derecho nacional a la Directiva dentro del plazo señalado o cuando haya procedido a una adaptación incorrecta– permite su invocación directa por los particulares frente al Estado y su aplicación por los órganos jurisdiccionales[75].

La Comisión había detectado en el pasado que existía un bajo nivel de cumplimiento de la directiva por los Estados miembros. En muchas disposiciones el margen de acción de los Estados miembros es muy reducido o inexistente y pese a ello se han producido divergencias, lo que significa, a juicio de la Comisión, un incumplimiento de la Directiva comunitaria o una incorrecta transposición[76]. Este sería el caso del art. 2 –las definiciones– y de otras las listas cerradas de la Directiva, como las de los artículos 7 –legitimación del tratamiento–, 8.1 –datos sensibles–, 10 –información al interesado–, 13 –excep-

74. Sentencia *Lindqvist*, cit. apdo. 97.
75. Cfr. STJUE, de 3.3.2011, as. *Nikolovi* (C-203/10), apdo. 61 y jurisprudencia que se cita.
76. La Comisión citaba como ejemplos para justificar esta aseveración el número relativamente reducido de reclamaciones recibidas por la Comisión, así como las escasas autorizaciones por parte de las autoridades nacionales de transferencia a terceros países notificadas a la Comisión en relación con el art. 26.3 de la Directiva 95/46/CE. También señalaba que no todos los Estados miembros han aprovechado las posibilidades que brindaban las excepciones de la Directiva para alcanzar una mayor simplificación –por ejemplo en el caso de las notificaciones–. Igualmente los requisitos de información de las leyes nacionales que se imponen a los responsables del tratamiento de datos son incoherentes con la Directiva, lo que requiere una modificación legislativa –*Primer informe sobre la aplicación de la Directiva*, cit.–

ciones– y 26 –excepciones relativas a las transferencias a terceros países–. Le corresponde a la Comisión velar continuamente por una completa aplicación de la Directiva, llevando a cabo una continua labor de análisis de los textos legislativos de los Estados miembros y, en su caso, denunciar ante el Tribunal de Justicia a aquellos países cuyas legislaciones incumplían la Directiva. Así, la Comisión decidió en diciembre de 1999 denunciar a Francia, Alemania, Irlanda, Luxemburgo y los Países Bajos ante el Tribunal de Justicia de las Comunidades Europeas por no haber notificado todas las medidas necesarias para aplicar la Directiva 95/46/CE[77].

B) La satisfacción del interés legítimo del responsable del tratamiento y la necesaria ponderación con los derechos del interesado. La Sentencia del Tribunal de Justicia, de 24 de noviembre de 2011.

Un buen ejemplo de lo que estamos diciendo es la transposición del art. 7.f de la Directiva, que establece como un principio legitimador del tratamiento que sea 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». Esta previsión legal relativa a la satisfacción de un interés legítimo del responsable y a la necesidad de llevar a cabo una ponderación –*balance test*- se ha recogido en algunas legislaciones nacionales. Según un informe encargado por la Comisión, los elementos que han de tenerse en cuenta por los Estados son la naturaleza de los datos y del tratamiento, las medidas adoptadas por el responsable para garantizar los derechos del interesado y si el tratamiento es efectuado por la Administración Pública o por una entidad privada. Llama la atención que los Estados mantengan un mayor control si es un responsable de un fichero público el que utiliza como criterio de legitimación esta previsión de la Directiva. No obstante, en general esta previsión es aplicada por los Estados de manera más restrictiva de cómo aparece expresada en la Directiva y sometida a otros requerimientos. De esta forma, el balance de intereses se inclina hacia el titular de los datos o se limita su aplicación a pocos datos o a supuestos específicos autorizados por la Autoridad de control. Así, en esta materia existe una divergencia sustancial entre las legislaciones de los Estados miembros[78].

---

77. En 2001, los Países Bajos y Alemania notificaron sus medidas y la Comisión archivó las causas instruidas contra dichos Estados. Francia notificó su ley de protección de datos de 1978, por lo que se abandonaron los procedimientos contra dicho Estado. Francia anunció al mismo tiempo su intención de aprobar una nueva ley. Respecto a Luxemburgo, la acción de la Comisión dio lugar a la condena de dicho Estado miembro por el Tribunal de Justicia por no cumplir sus obligaciones. Posteriormente se aplicó la Directiva a través de una nueva ley, que entró en vigor en 2002. Irlanda notificó una aplicación parcial en 2001; sin embargo, con posterioridad se aprobó una ley completa. Cfr. *Primer informe sobre la aplicación de la Directiva*, cit.–.
78. Así, por ejemplo, en Alemana se llevan a cabo diferentes test para el sector privado y para el sector público. En Finlandia, la Ley establece un número limitado de supuestos en los que puede llevarse a cabo el tratamiento y en los que puede producirse una aplicación de esta previsión de la Directiva. En otros casos se exige al responsable del fichero que considere que puede aplicar esta previsión que obtenga la autorización de la autoridad de control.

Recientemente el Tribunal de Justicia de la Unión Europea, a instancias del Tribunal Supremo de España, ha puesto en evidencia el incumplimiento de nuestro país en la transposición del art. 7.f de la Directiva. Así, la LOPD no ha transpuesto esta previsión de la Directiva sino que ha concretado previamente aquellos supuestos en los que el *balance test* justifica que los responsables de ficheros lleven a cabo el tratamiento de datos personales sin consentimiento del interesado. Así, los tratamientos que encontrarían justificación dentro de este equilibrio de intereses previsto en la Directiva serían para el legislador español aquellos necesarios para notificar riesgos crediticios, información aseguradora para evitar el fraude y especialmente aquellas tratamientos de datos necesarios para desarrollar la actividad de publicidad o de prospección comercial a través de fuentes accesibles al público –directorios telefónicos, boletines oficiales, censo promocional–. En todo caso, no podemos olvidar que el Considerando 30 de la Directiva señala como motivos del art. 7.f) asegurar el equilibrio de los intereses en juego, para lo cual los Estados pueden precisar las condiciones en las que se podrán utilizar y comunicar a terceros datos de carácter personal, en el desempeño de actividades legítimas de gestión ordinaria de empresas y con fines de prospección comercial. La regulación tasada de las fuentes accesibles al público, entre las que están, exclusivamente, el censo promocional –que todavía no existe–, los repertorios telefónicos en los términos previstos por su normativa específica, las listas de personas pertenecientes a grupos profesionales que contengan un limitado número de datos, los diarios y boletines oficiales y los medios de comunicación –art. 3.j) LOPD– que permiten la consulta, tratamiento y cesión a cualquier persona –art. 6.2 in fine y art. 11.2.b) LOPD– sin más exigencia que, en su caso, el abono de una contraprestación[79], es la concreción que lleva a cabo el Legislador de la exigencia de un interés legítimo. En general, la Ley Española sigue siendo restrictiva en este punto a juicio de la Comisión. Así, como señala el informe encargado por la Comisión, «el hecho de que la Ley Española atribuya un tratamiento especial a los procesos que consisten en la revelación de información a terceras personas –cesión de datos– hace que los tratamientos de datos personales sin el consentimiento del interesado sean considerablemente más difíciles en España que en otros países»[80].

---

79. El art. 6.2.b) LOPD establece en todo caso que no será preciso el consentimiento para el tratamiento de datos personales que figuren en fuentes accesibles al público siempre que el tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

80. «This peculiarity together with the fact that the Spanish law confers a special treatment to processing that consists of disclosure of information to a third party («cesión de datos») makes the processing of personal data without consent of individuals considerably more difficult in Spain than in other countries». Cfr. *Analysis and impact study on the implementation of Directive EC 95/46 in Member States*, *http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm* Cfr. el análisis de esta cuestión en nuestro comentario al art. 11 de la LOPD «La comunicación de datos personales», en TRONCOSO REIGADA, A. (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas-Thomson Reuters, Cizur Menor, 2010, pp. 950-1005.

El Tribunal Supremo en la Sentencia de la Sala de lo Contencioso-Administrativo –Sección Sexta–, de 15 de julio de 2010, planteó una cuestión prejudicial al TJEU relativa al art. 7.f) de la Directiva 95/46/CE, que surgió al enjuiciar el art. 10.2 del RPDP, que recoge las excepciones al consentimiento del interesado para el tratamiento y para la cesión de datos personales previstas en la LOPD. El Tribunal Supremo entendía que la excepción establecida en el art. 10.2.b) del RPDP no considera suficiente que el responsable o el tercero a quien se comuniquen los datos tengan un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado –que es la previsión que se encuentra en el art. 7.f) de la Directiva–, sino que exige que los datos objeto de tratamiento y de cesión figuren en fuentes accesibles al público, lo que puede suponer una restricción indebida de los tratamientos y las cesiones de datos sin consentimiento y no transpone debidamente el art. 7.f) de la Directiva 95/46/CE, infringiendo, por tanto, el Derecho Comunitario[81].

El Tribunal Supremo «considera que el Derecho español añade al interés legítimo como presupuesto del tratamiento de los datos sin consentimiento del titular un requisito que no está presente en la mencionada Directiva: que los datos consten en fuentes accesibles al público». Para el Tribunal Supremo, el art. 7.f) está pensando «en coyunturas singulares, atendibles y susceptibles de análisis en función de las características del caso concreto y no acudiendo a categorizaciones genéricas y abstractas» por lo que no puede establecerse por el legislador «una lista cerrada y exhaustiva»[82]. Por ello, el Tribunal Supremo plantea la cuestión prejudicial al Tribunal de Justicia de la Unión Europea en los siguientes términos: «¿Debe interpretarse el artículo 7, letra f), en el sentido de que se opone a una normativa nacional que, no mediando consentimiento del afectado y para permitir el tratamiento de sus datos de carácter personal que resulte necesario para satisfacer un interés legítimo del responsable o de los terceros a los que se vayan a comunicar, exige además de que no se lesionen los derechos y libertades fundamentales de aquel que los datos consten en fuentes accesibles al público?; y, ¿concurren en el mencionado artículo 7, letra f), las condiciones que exige la jurisprudencia del Tribunal de Justicia de la Unión Europea para atribuirle efecto directo?»[83].

---

81. Para el Tribunal Supremo, «si concurre un interés legítimo del responsable o de los destinatarios de los datos, el tratamiento resulta posible salvo que, en atención a la naturaleza de los datos y del soporte, a las condiciones subjetivas del afectado, a la finalidad perseguida, etc., deba darse prevalencia a los derechos fundamentales, en particular, al derecho a la intimidad del titular de los datos».
82. En consecuencia, «los Estados miembros no pueden establecer otras excepciones y limitaciones que las que se contemplan en el artículo 13 de la repetida Directiva».
83. Lógicamente la respuesta depende para el Tribunal Supremo de la interpretación que el Tribunal de Justicia dé al artículo 7, f) de la Directiva 95/46/CE, pues «si concluye que nada impide que los Estados miembros exijan, además de la concurrencia del repetido interés, la presencia de los datos en fuentes accesibles al público, habrá que concluir que la Ley española y el Reglamento que la desarrolla se ajustan en este punto al ordenamiento jurídico de la Unión. Si, por el contrario, es criterio del Tribunal de Justicia que no les cabe a los Estados miembros añadir requisitos adicionales a aquella

Pues bien, el Tribunal de Justicia de la Unión Europea, en la Sentencia de 24 de noviembre de 2011 que resuelve estas cuestiones prejudiciales, señala, en relación con el art. 7 de la Directiva, que sólo son legítimas las medidas nacionales que *precisen* alguno de los principios –disponiendo en este punto los Estados miembros de un margen de apreciación con arreglo al art. 5 de la Directiva–, estando prohibidas aquellas medidas nacionales que establezcan *exigencias adicionales* que modifican el alcance del art. 7 de la Directiva. Por tanto, los Estados miembros no pueden introducir, en virtud del art. 5 de la Directiva, nuevos principios de legitimación de los tratamientos de datos personales distintos a los enunciados en el artículo 7 de esa Directiva, ni tampoco pueden modificar, mediante exigencias adicionales, el alcance de los seis principios establecidos en dicho artículo 7. El Tribunal de Justicia señala que el art. 7.f) contiene dos requisitos acumulativos para que un tratamiento de datos personales sin que medie el consentimiento del interesado se considerado lícito: que sea 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, y que no prevalezcan los derechos y libertades fundamentales del interesado[84]. Por tanto, este precepto de la Directiva se opone a toda normativa nacional que imponga exigencias adicionales que se sumen a los dos requisitos acumulativos antes señalados. Además, el segundo de esos requisitos exige una ponderación de los derechos e intereses en conflicto, que dependerá, en principio, de las circunstancias concretas del caso particular de que se trate y en cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta el derecho a la vida privada y a la protección de los datos personales reconocidos en los arts. 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea. A la hora de realizar esta ponderación, la mayor o menor gravedad en la lesión de los derechos de la persona afectada por el tratamiento puede variar en función de que los datos figuren ya o no en fuentes accesibles al público. Lógicamente, si no figuran en estas fuentes, la lesión en los derechos del interesado es potencialmente más grave y debe ser apreciada en su justo valor, contrapesándola con el interés legítimo perseguido por el responsable del tratamiento o por el tercero a los que se comuniquen sus datos. Sí es legítimo que, en virtud de la previsión del art. 5 de la Directiva, los Estados miembros establezcan los principios que deben regir esa ponderación. Lo que no es legítimo es que «la normativa nacional excluya de forma categórica y generalizada la posibilidad de tratar determinadas categorías de datos personales, sin permitir ponderar los derechos e intereses en conflicto en cada caso en concreto», estableciendo con carácter definitivo el resultado final de la ponderación de los derechos e intereses en conflicto «sin permitir un resultado diferente en atención a las circunstancias

---

exigencia, debería inaplicarse, para el caso de que se pueda reconocer al art. 7,f) efecto directo.

84. Esta interpretación se encuentra también corroborada, a juicio del Tribunal, en que el art. 7 de la Directiva emplea los términos «sólo pueda efectuarse si» y la conjunción «o», que pone de manifiesto el carácter exhaustivo y taxativo de la lista que figura en dicho artículo.

particulares de cada caso concreto» –dejando lógicamente al margen la referencia que la propia Directiva en el art. 8 hace a los datos especialmente protegidos–[85].

La segunda cuestión prejudicial planteada por el Tribunal Supremo se refiere a si es atribuible al art. 7.f) de la Directiva 95/46/CE el efecto directo. Este es uno de los principios que permite la articulación entre el ordenamiento jurídico europeo y los ordenamientos nacionales de los países miembros cuando existan conflictos entre sus normas, como claramente se produce en este caso entre la Directiva 95/46/CE y la legislación española de protección de datos personales[86]. La resolución de esta cuestión prejudicial obliga a analizar si estamos o no dentro del margen de divergencia legítima en la transposición de la Directiva que tiene cada Estado para alcanzar los objetivos comunitarios y si

85. Por ello, la Sentencia del Tribunal de Justicia responde a la primera cuestión prejudicial señalando que el art. 7.f de la Directiva «debe interpretarse en el sentido de que se opone a una normativa nacional que, para permitir el tratamiento de datos personales 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, exige, en el caso de que no exista consentimiento del interesado, no sólo que se respeten los derechos y libertades fundamentales de éste, sino además que dichos datos figuren en fuentes accesibles al público, excluyendo así de forma categórica y generalizada todo tratamiento de datos que no figuren en tales fuentes».

86. Ese principio implica que el Derecho europeo está integrado por normas jurídicas generadoras de derechos y obligaciones, que deben ser aplicadas por las autoridades nacionales. El Derecho europeo, como ha señalado el TJCE en la Sentencia, de 9.03.1978, –as. *Simmentha*– «debe desplegar la plenitud de sus efectos de manera uniforme en todos los Estados miembros, a partir de su entrada en vigor y a lo largo de toda la duración de su validez; de este modo, estas disposiciones constituyen una fuente inmediata de derechos y de obligaciones para todos los afectados por ellas, bien se trate de Estados miembros o de particulares que sean parte en relaciones jurídicas que incumben al derecho comunitario». Lógicamente, esta eficacia directa es especialmente predicable de los Reglamentos ya que, como señala el art. 288 del TFUE, «el reglamento tendrá un alcance general. Será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro». El efecto directo del Derecho de la Unión no se predica sólo de los reglamentos porque la jurisprudencia del Tribunal de Justicia, especialmente a partir de la Sentencia *Van Gend & Loos* –STJCE, de 5.02.1963– lo ha extendido al Derecho originario y a las Directivas. Le corresponde al Tribunal de Justicia de la Unión Europea determinar si una Directiva, como la 95/46/CE, dispone de efecto directo. Los órganos jurisdiccionales nacionales –especialmente cuando hayan agotado los recursos judiciales internos– deben plantear la cuestión prejudicial en virtud de la previsión establecida en el art. 267 TFUE, como así ha hecho acertadamente el Tribunal Supremo, cuando duden si una Directiva, como es el caso, dispone de eficacia directa. Son muchas las referencias bibliográficas sobre esta cuestión. Nos limitamos a citar un trabajo clásico de MENGOZZI, P., que ha actuado como Abogado General en este procedimiento, *Il Diritto della Comunità Europea*, Cedam, Padua, 1990, pp. 88-132 y 140-146. Lógicamente, el ordenamiento jurídico europeo debe ser aplicado por las autoridades nacionales de los Estados miembros –Administración y Tribunales nacionales–, lógicamente cuando se trate del ejercicio de competencias que se hayan atribuido a la Unión Europea y sometidas a integración –por tanto, dentro del ámbito del art. 93 CE–, ya que estamos hablando de dos ordenamientos jurídicos distintos con campos de actuación propios.

concurren en el art. 7,f), las condiciones que exige la jurisprudencia del Tribunal de Justicia de la Unión Europea para atribuirle efecto directo. Así, si bien, como hemos señalado antes, la Directiva 95/46/CE confiere a los Estados miembros un margen de apreciación más o menos grande para la aplicación de algunas de sus disposiciones, la Sentencia del Tribunal de Justicia, de 24 de noviembre de 2011, que resuelve estas cuestiones prejudiciales, señala que el art. 7.f) contiene los dos requisitos acumulativos que permite la posibilidad de tratar los datos personales sin consentimiento del interesado[87], por lo que es una disposición suficientemente precisa y establece una obligación incondicional, que son los dos elementos exigidos por la jurisprudencia para reconocer el efecto directo. Por ello, una incorrecta transposición de este precepto permite que pueda ser invocado directamente por un particular y aplicado por los órganos jurisdiccionales nacionales. Hay que recordar también el principio de primacía del Derecho comunitario[88], que no es sólo sobre el Reglamento sino sobre cualquier norma estatal cualquiera que sea su rango, también sobre la LOPD, por lo que cuando existan una incompatibilidad entre el Derecho Comunitario y la Ley nacional, la autoridad nacional –administrativa o judicial– debe optar por inaplicarla sin necesidad de *«pedir o esperar la remoción previa por vía legislativa o mediante cualquier otro procedimiento constitucional»* (STJCE *Simmenthal*, 1978)[89].

C) La necesaria inaplicación y derogación de preceptos de la LOPD en virtud de esta Sentencia y la necesidad de que el Legislador establezca procedimientos ante la autoridad de control que permitan justificar el interés legítimo del responsable, faciliten la ponderación con los derechos de los interesados y garanticen la publicidad y la seguridad jurídica.

Recientemente, la Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo, de 8 de febrero de 2012, teniendo en cuenta la Sentencia del Tribunal de Justicia, de 24 de noviembre de 2011, que resolvía la cuestión prejudicial, ha anulado el art. 10.2.b) del RPDP. La realidad es que este art. 10.2.b) del RPDP es reproducción del art. 6 LOPD y, en menor medida, del art. 11 LOPD. Así, el art. 10.2.b) del RPDP exige para el tratamiento y para la cesión la concurrencia de los dos requisitos: que los datos figuren en fuentes accesibles al público y que el responsable del fichero o el tercero a quien se comuniquen los datos tenga un interés legítimo para su tratamiento y conocimiento –siempre

87. La Sentencia menciona la sentencia *Österreichischer Rundfunk*, ya cit..
88. El principio de primacía del Derecho Comunitario sobre el Derecho interno está, de nuevo, referido a un ámbito competencial sometido a integración europea donde se ha cedido el ejercicio de competencias a la Unión Europea. Este principio de primacía fue afirmado por el Tribunal de Justicia de la Unión Europea a partir de la Sentencia *Costa/ ENEL* (1964). Hay que recordar que tanto el principio de efecto directo como el de primacía han sido asumidos por el Tribunal Constitucional en las Sentencias 28/91 y 64/91 y DTC 1/2004, y por el Tribunal Supremo en la Sentencia de 28 de abril de 1987. Cfr. PÉREZ TREMPS, P., *op. cit.* pp. 128-170.
89. El Tribunal Supremo podía haber planteado la cuestión prejudicial en relación con la LOPD, teniendo en cuenta que el RPDP es desarrollo de ésta.

que no se vulneren los derechos y libertades del interesado–. Igualmente, el art. 6.2 LOPD establece que no será preciso el consentimiento para el tratamiento «cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado»; es decir, requiere para el tratamiento sin consentimiento la concurrencia de ambos requisitos, aunque en la práctica se han reputado como legítimos todos los tratamientos de datos que procedían de fuentes accesibles al público, sin que ninguna Resolución de la Agencia Española de Protección de Datos hasta ahora haya requerido el interés legítimo del responsable o haya realizado una labor de ponderación con los derechos del interesado. Se entendía que el hecho de que los datos figurasen en fuentes accesibles al público –las propias características de estos datos– hacía que estos tratamientos no afectaran a los derechos y libertades de los interesados, algo que podía estar más o menos claro en relación con los repertorios telefónicos o los listados de personas pertenecientes a grupos profesionales pero que no lo estaba tanto en relación con la información que aparece publicada en diarios oficiales. En cambio, el art. 11.2.b) LOPD se limita a no exigir el consentimiento para la cesión cuando los datos se recojan de fuentes accesibles al público, sin demandar ningún interés legítimo del responsable o del cesionario y sin hacer ninguna referencia a la necesidad de ponderar que no se vulneren los derechos del interesado. Por tanto, es la propia LOPD quien no ha transpuesto bien la Directiva Comunitaria –exigiendo el requisito adicional de que los datos figuren en fuentes accesibles al público y no recogiendo claramente la exigencia de un interés legítimo del responsable y del cesionario y la necesidad de llevar a cabo la ponderación con los derechos del interesado–, siendo el Reglamento *secundum legem*. Como hemos señalado en otro momento, no le corresponde a la norma reglamentaria corregir las deficiencias en las que ha incurrido el Legislador en la transposición de una Directiva[90]. Es necesario que el Legislador modifique estos preceptos legales en aquello que sea incompatible con el art. 7.f) de la Directiva, sin esperar a que se plantee una nueva cuestión prejudicial acerca de éstos y evitando, de esta forma, las incertidumbres que genera la inaplicación o desplazamiento de preceptos de leyes internas por parte de los jueces[91].

No es suficiente para la transposición adecuada de la Directiva 95/46/CE que el Legislador suprima de la LOPD el requisito adicional de la procedencia de

90. Esta mala transposición que la LOPD ha efectuado de la Directiva Comunitaria, restringiendo el tratamiento y la cesión no sólo cuando sea necesario para la satisfacción del interés legítimo sino también cuando es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio al poder público –exigiendo también al presencia de una habilitación legal para las cesiones de datos entre Administraciones Públicas– la hemos criticado tempranamente en «La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional», *Cuadernos de Derecho Público* núms. 19-20, 2003, pp. 305-312 y ahora en *La protección de datos personales. En busca del equilibrio*, cit. pp. 95-105, 140-168, 499-548.

91. Cfr. *supra* apdo. I.

los datos de fuentes accesibles al público. Además, le corresponde al Legislador encontrar fórmulas que permitan al responsable justificar la necesidad del tratamiento o de la cesión para la satisfacción de un interés legítimo del responsable o del tercero al que se comuniquen los datos y que faciliten llevar a cabo una ponderación con los derechos y libertades fundamentales del interesado que se encuentran en conflicto y que pueden prevalecer. Esto conlleva, a nuestro juicio, el establecimiento de un procedimiento ante las autoridades de control, como ocurre con el procedimiento de exención del deber de información al interesado o el procedimiento para la autorización de la conservación de datos para fines históricos, estadísticos o científicos –arts. 153-158 RPDP–. Este procedimiento se iniciaría a instancia de los responsables o eventuales cesionarios, que tendrían que justificar el interés legítimo del tratamiento –aportando un plus de razonabilidad y asumiendo la carga de la prueba– y debería dar participación a los interesados o a las asociaciones que defiendan derechos y libertades de los interesados. Así, si bien la ponderación exige tener en cuenta las circunstancias del caso concreto, estos casos concretos son siempre clasificables en tipologías y permiten el establecimiento de algunos criterios generales y neutrales que den garantías tanto a responsables como a interesados. Así, hay que hacer compatible la necesidad de llevar a cabo una ponderación, que es siempre un juicio en el caso concreto, con la necesaria previsibilidad del comportamiento de la autoridad de control y la seguridad jurídica de los sujetos obligados[92]. La ponderación no se debe llevar a cabo únicamente en el procedimiento sancionador iniciado contra el responsable del tratamiento sino previamente, con un procedimiento de autorización o de control previo, que permita al responsable conocer *ex ante* el resultado de la ponderación para llevar a cabo o no el tratamiento, una exigencia también de la proyección amplia del principio de legalidad en la potestad sancionadora de la Administración –art. 25 CE–. Tampoco parece que la consulta previa del responsable a la autoridad de control sea el procedimiento más adecuado, si no permite la participación de los interesados[93]. Además, es necesario dar publicidad al resultado de esta ponderación para que otros responsables puedan tener en cuenta el criterio favorable a la legitimación del tratamiento en el desempeño de sus actividades económicas y comerciales ya que lo contrario originaría una desigualdad para los competidores. De esta forma, un interés legítimo de un responsable que permite una legitimación del tratamiento de datos personales sin consentimiento y que prevalece sobre otros derechos o intereses legítimos de los afectados debe ser igual-

92. La previsibilidad de las autoridades de control y la necesidad de establecer principios generales y neutrales es una cuestión sobre la que hemos reflexionado en la «Introducción» a *Principios y Derechos de Protección de Datos Personales. Doctrina de la Agencia de Protección de Datos de la Comunidad de Madrid 2002-2009*, Civitas-APDCM, Madrid, 2010, p. 37 –esta idea se encuentra recogida también en *La protección de datos personales. En busca del equilibrio*, cit. p. 30–. Cfr. Wechsler, T., «Toward neutral principles of Constitutional Law», *Harvard Law Review*, núm. 73, 1950, pp. 1-19.

93. La consulta previa a la autoridad de control, que dé lugar a un dictamen público para otros responsables del tratamiento, puede ser un procedimiento razonable mientras que no haya otro habilitado al efecto.

mente válido y aplicable a la misma tipología de tratamientos de datos personales que hagan otros responsables que ostenten el mismo interés legítimo. Es esencial, por tanto, que la necesidad de prever la ponderación entre derechos dentro de un supuesto de legitimación del tratamiento de datos personales sin consentimiento no suponga una merma del principio de seguridad jurídica –art. 9.3 CE– tanto de responsables de tratamiento como de interesados[94]. Por último, hay que señalar que la Agencia Española de Protección de Datos podría llevar a cabo una interpretación y aplicación restrictiva del art. 7.f) de la Directiva 95/46/CE, que, como ya hemos señalado tiene efecto directo, en lo que hace referencia al resultado de la ponderación lo que, lógicamente, podría también ser recurrido y analizado por la Audiencia Nacional. Como el criterio de legitimación del tratamiento sin consentimiento del interesado previsto en el art. 7.f) de la Directiva 95/46/CE se encuentra igualmente recogido en el art. 6.1.f) de la propuesta de Reglamento, esta situación de incertidumbre sólo desaparecería con el establecimiento a nivel europeo de criterios o parámetros abstractos, que sin negar la ponderación en el caso concreto –derivado del momento aplicativo–, disminuya al menos el margen de maniobra en este punto de las autoridades de control.

D) La deficiente aplicación de la normativa de protección de datos personales en los Estados de la Unión Europea.

Así, otras divergencias entre los Estados miembros en la protección de los datos personales no provienen tanto de la legislación sino de la diferente interpretación y aplicación que llevan a cabo las autoridades de control y los órganos jurisdiccionales de los mismos principios y derechos recogidos en la Directiva[95]. Los Tribunales nacionales han establecido una jurisprudencia relativa a la protección de datos personales, sin plantear cuando era necesaria la conveniente cuestión prejudicial[96]. El carácter de cláusula abierta –de valor– de

94. Así, hay que reconocer que la concreción –la materialización– por parte de Legislador de la existencia de un interés legítimo en las cesiones de datos que obren en fuentes accesibles al público facilitaba la seguridad jurídica tanto del afectado como del responsable del tratamiento –art. 11.2.b) LOPD–.

95. Buena muestra las discrepancias en la aplicación de las normas de protección de datos personales en los diferentes Estados miembros ante el mismo supuesto de hecho y la necesidad de actuar de manera coordinada ha sido el caso de *Google Street View*, que ha sido sometido a exigencias de privacidad más duras en Alemania que en otros Estados miembros. Como es sabido, entre mayo de 2007 y mayo de 2010 Google recopiló los datos de redes *Wifi* en muchos países como parte de su proyecto *Street View*, que ofrece a los usuarios de *Google Maps* y *Google Earth* la posibilidad de ver a nivel de calle las imágenes de las estructuras y los terrenos adyacentes a las carreteras y autopistas. Sin embargo, Google también recogió las contraseñas, historial de uso de Internet y otros datos personales sensibles, que no eran necesarios para su proyecto, según advirtió la Comisión Federal de Comunicaciones de los Estados Unidos de América. *Google* reconoció públicamente en mayo de 2010 que los coches que utilizaban para tomar las fotos para *Street View* habían recogido datos privados, la mayoría de ellos fragmentados. Ello dio lugar a una investigación de la FCC acerca de si se había violado la Ley de Comunicaciones.

96. La primera cuestión prejudicial, como acabamos de ver, sobre la transposición de la Directiva 9546/CE en nuestro país la planteó la Sala de lo Contencioso-Administrativo

las normas de la Directiva que recogen los principios y derechos ha permitido una variabilidad en la definición de los criterios de aplicación por parte de las distintas autoridades de control de protección de datos ante los mismos supuestos de hecho. Esto es lo que ha ocurrido con el principio de calidad y de finalidad compatible, que, dada su flexibilidad, se ha prestado a una aplicación divergente[97]. Posiblemente, una aproximación de los criterios de interpretación hubiera podido atenuar mucho las diferencias legislativas entre los Estados miembros. El Grupo de Trabajo regulado en el Artículo 29 de la Directiva 95/46/CE, en el que participan las autoridades de protección de datos de los Estados miembros, ha jugado un papel fundamental, facilitando una cooperación más estrecha entre todas ellas que permita una aplicación homogénea de la Directiva[98]. Este Grupo de Trabajo es, como se ha dicho, «a key element in ensuring better and more coherent implementation», lo que permite reducir la repercusión negativa de las divergencias legislativas de los Estados miembros, constituyéndose hasta ahora en una auténtica alternativa a otras soluciones más complejas como la modificación de las leyes de los Estados miembros o la aprobación de un nuevo marco normativo europeo, como se plantea en la actualidad. No obstante, la Comisión Europea ha considerado que el Grupo de Trabajo debía mejorar su contribución a la armonización entre los Estados miembros[99]. En todo caso, hay que señalar que existe una cierta contradicción entre la voluntad de la Comisión de alcanzar una interpretación más flexible de la Directiva –dando juego al régimen de excepciones previsto en la misma– y la posición tradicionalmente más restrictiva del Grupo de Trabajo del Artículo 29[100]. Tam-

---

del Tribunal Supremo, a través de la Resolución de 15 de julio de 2010 –por tanto, quince años después de la aprobación de la Directiva–. Recientemente, la Sala de lo Contencioso-Administrativo de la Audiencia Nacional ha planteado, a través del Auto de 27 de febrero de 2012, una cuestión prejudicial en relación con la aplicación de la Directiva a los buscadores, que más adelante analizaremos –*infra* apdo. V.E)–.

97. Cfr. *Analysis and impact study on the implementation of Directive*, cit..

98. Este Grupo ha desarrollado un trabajo útil en ámbitos como las transferencias internacionales, los tratamientos de datos biométricos o el concepto de dato personal. De hecho, este grupo tiene la función de «estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea» –art. 30.1.a) de la Directiva–.

99. Cfr. *Segundo Informe sobre la aplicación de la Directiva*, cit.. Era importante que el Grupo de Trabajo hubiera sido capaz de encontrar una respuesta armonizada a cuestiones de interés público como la información al interesado, la seguridad o la simplificación de los requisitos de notificación, lo que hubiera facilitado el cumplimiento de sus obligaciones a las empresas multinacionales. No olvidemos que el Grupo de Trabajo debe informar a la Comisión de la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieran afectar a la equivalencia de la protección de datos personales –art. 30.2 de la Directiva–. La Comisión llegó a afirmar que «está dispuesta a formular propuestas si el Grupo de Trabajo no puede hacerlo en un plazo razonable (12 meses)». Muchos problemas de armonización en la protección de los datos personales a nivel europeo residen en que el grupo de trabajo del artículo 29, especialmente a partir de su ampliación a veinticinco miembros, tiene un procedimiento lento de toma de decisiones. Esto se ha notado, por ejemplo, en el retraso en emitir el dictamen sobre computación en nube.

100. La Comisión ha abogado, como hemos señalado antes, por la necesidad de una mayor

bién las autoridades nacionales de protección de datos –si bien son independientes en la aplicación de la normativa– podían haber hecho un mayor esfuerzo en tratar de adaptar sus posiciones a las líneas comunes establecidas en este Grupo de Trabajo.

Otra de las causas del bajo cumplimiento de la Directiva, que genera también divergencias entre los Estados miembros en protección de datos personales, es la distinta capacidad coercitiva de las autoridades de control, algo que, como profundizaremos más adelante, afronta y resuelve la propuesta de Reglamento. Esto ha hecho que la situación jurídica de los agentes económicos en los distintos Estados miembros no haya sido la misma hasta ahora, lo que entorpecía el funcionamiento del mercado interior. Hay que mencionar también la falta de medios de muchas autoridades de control que impide una intensa actividad de control sobre el cumplimiento de la legislación[101]. Como señala el Parlamento Europeo, las autoridades «are currently 'under-resourced for their wide range of tasks». Esto obliga a la Comisión a reclamar a los Estados miembros recursos adicionales para las autoridades de protección de datos con la finalidad de asegurar una mayor efectividad en el funcionamiento del sistema. Para la Comisión existe una fuerte interrelación entre la ausencia de una intensa actividad coercitiva por parte de las autoridades de control y la irregular conformidad de los responsables de tratamiento para «introducir cambios en sus prácticas actuales para ajustarse a unas normas que pueden parecer complejas y pesadas, mientras el riesgo de que se detecte esta actuación parece reducido»; lo que conlleva «un escaso conocimiento por parte de los interesados acerca de sus derechos, que puede ser el origen del fenómeno anterior». A juicio de la Comisión, «dada la interrelación de los tres aspectos, la resolución de uno de ellos puede repercutir positivamente en los otros dos. Una acción coercitiva más enérgica y eficaz mejorará la conformidad con la legislación. Una mayor conformidad permitirá que los responsables del tratamiento de datos suministren más información y de mejor calidad a los interesados acerca de la existencia del tratamiento y de sus derechos según la legislación, con lo que mejorará el grado de sensibilización sobre la protección de datos de los ciudadanos en general»[102].

V. UN NUEVO MARCO JURÍDICO COHERENTE Y HOMOGÉNEO DE PROTECCIÓN DE DATOS: LA PROPUESTA DE REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Todas estas incongruencias en la protección de los datos personales en los

---

clarificación de la cláusula del equilibrio de intereses –art. 7.f)–. Igualmente ha defendido «una interpretación razonable y flexible» de determinadas disposiciones de la Directiva como la relativa a los datos sensibles. Así, en este punto si bien la Comisión desea una adecuada protección de este tipo de datos, plantea una posición más flexible teniendo en cuenta la realidad de la actividad diaria, las operaciones habituales de tratamiento y los riesgos efectivos que determinadas operaciones suponen para la protección de los derechos y libertades fundamentales de la persona –*ibidem*–.

101. Cualquier autoridad de protección de datos personales es pequeña en medios materiales y humanos en relación con la función de velar por el cumplimiento de esta legislación, lo que obliga a analizar qué función debe ser prevalente. Una reflexión acerca del *selective to be efective* la hemos hecho en *La protección de datos* personales, cit. pp. 1822-1827.

102. Cfr. *Primer informe sobre la aplicación de la Directiva* cit..

distintos Estados de la Unión justifican para la Comisión la necesidad de disponer de un nuevo marco jurídico coherente y homogéneo de protección de datos en toda el territorio de la Unión que reduzca o suprima el margen de elección que disponen tanto los legisladores nacionales como las autoridades de control y los Tribunales. La Comisión entendía inicialmente –hace nueve años– que «no puede considerarse que una gran parte de las divergencias detectadas por los servicios de la Comisión constituyan infracciones de la legislación comunitaria ni que tengan repercusiones negativas significativas en el mercado interior, pero, en caso contrario, la Comisión hará todo lo necesario para resolver la situación»[103]. Sin embargo, la Comisión ha sido cada vez más consciente del problema que supone la fragmentación de la normativa de protección de datos en la Unión Europea, tanto en relación a la división entre pilares como a las diferencias legislativas y de aplicación de la normativa entre los Estados miembros. El Tribunal de Justicia había manifestado que el margen de apreciación de que disponen los Estados miembros en virtud del art. 5 de la Directiva únicamente puede utilizarse de conformidad con el objetivo perseguido por la Directiva 95/46/CE, que consiste en mantener un equilibrio entre la libre circulación de datos personales y la tutela del derecho a la intimidad[104]. Ninguno de los dos objetivos que señalaba la Directiva 95/46/CE se garantizaba plenamente[105]. Así, en primer lugar, el derecho a la protección de datos de carácter personal, consagrado en el art. 8 de la Carta, requiere el mismo nivel de protección de datos personales, lo que no ocurría en la actualidad. Al mismo tiempo, las nuevas tecnologías, como hemos señalado anteriormente, facilitan la comunicación de manera prácticamente inmediata de datos personales más allá de las fronteras nacionales y de la Unión Europea. La ejecución de la normativa de protección de datos personales, que materializa el derecho del ciudadano al control de su información personal, exige un mayor nivel de cooperación entre las autoridades de protección de datos de los diferentes Estados miembros. También la Unión Europea se encuentra en mejores condiciones para garantizar una tutela efectiva de los ciudadanos europeos frente a tratamientos de sus datos que se realizan fuera de las fronteras de la UE y que afectan a varios Estados miembros, que las iniciativas adoptadas a nivel de cada uno de los Estados. En segundo lugar, la diversidad de enfoques nacionales relativos a la protección de datos personales constituye todavía un obstáculo para la realización del mercado interior[106]. Como señala el Considerando 7 de la Propuesta de Reglamento

103. Cfr. *Primer informe sobre la aplicación de la Directiva*, cit.
104. Cfr. la Sentencia *Lindqvist*, antes citada, apartado 97.
105. Así, la Ficha financiera Legislativa de la propuesta de Reglamento señala en el apartado de «Principales conclusiones extraídas de experiencias similares anteriores» –apdo. 1.5.3– que «la presente propuesta se basa en la experiencia adquirida con la Directiva 95/46/CE y responde a los problemas derivados de la transposición y aplicación fragmentadas de dicha Directiva, *que impidieron lograr el doble objetivo de alcanzar un elevado nivel de protección de datos y establecer un mercado único para la protección de datos*».
106. Como señala la STJUE, de 24 de noviembre de 2011, citando de nuevo la Sentencia *Lindqvist* –apdo. 79–, «las diferencias entre los regímenes nacionales aplicables al tratamiento de datos personales pueden afectar seriamente al establecimiento y al funcio-

–siguiendo el Considerando 7 de la Directiva–, las diferencias en el nivel de protección de datos personales entre los Estados miembros pueden impedir la libre circulación de los datos de carácter personal en la Unión, constituyendo un obstáculo al ejercicio de las actividades económicas y falseando las competencia. Es necesario una regulación más transparente y una unidad de aplicación del Derecho europeo que imponga a los responsables y encargados de tratamiento el mismo nivel de obligaciones, una supervisión coherente y unas sanciones equivalentes en el territorio de la Unión. Esta misma idea había sido planteada reiteradamente por los representantes de intereses empresariales que se habían quejado ante la Comisión de que las disparidades actuales impiden a las organizaciones multinacionales desarrollar políticas paneuropeas sobre protección de datos. Los operadores económicos requieren de una mayor seguridad jurídica que permita las transferencias de datos personales a través de las fronteras interiores de la UE, algo incompatible con la actual fragmentación de las legislaciones nacionales. También el desarrollo de la economía digital en la Unión Europea requiere de un «marco sólido y coherente, armonizado para la protección de datos personales en la Unión». Hay que tener en cuenta, además, que la integración económica y social resultante del funcionamiento del mercado interior ha llevado a un aumento sustancial de los flujos transfronterizos y del consiguiente intercambio de datos entre los operadores económicos y sociales, públicos y privados. También el Derecho de la Unión exige a las autoridades nacionales de los Estados miembros que cooperen e intercambien datos personales a fin de poder desempeñar sus funciones o llevar a cabo tareas en nombre de una autoridad de otro Estado miembro –Considerando 4 de la Propuesta de Reglamento–.

Así, la Comisión en el Plan de acción por el que se aplica el Programa de Estocolmo subrayó la necesidad de garantizar que el derecho fundamental a la protección de datos de carácter personal se aplique de forma homogénea en el contexto de todas las políticas de la UE. La Comisión ha concluido que la UE necesita *«una política más integradora y coherente en materia del derecho fundamental a la protección de los datos de carácter personal»*[107]. Por estos motivos

namiento del mercado interior». Los dos objetivos se introducen dentro de los «Indicadores de resultados e incidencia» –apdo. 1.4.4– de la Ficha Financiera Legislativa que elabora la Comisión. Esta señala que, por una parte, los responsables del tratamiento de datos se beneficiarán de una mayor seguridad jurídica gracias a la armonización y clarificación de las normas y procedimientos de protección de datos de la UE, lo que permitirá garantizar las mismas condiciones y una aplicación coherente; por otra parte, se indica que las personas tendrán un mejor control de sus datos personales, lo que aumentará su confianza en el entorno digital, y seguirán estando protegidas incluso cuando sus datos personales se traten en el extranjero. Así la Ficha Financiera Legislativa, en relación a la satisfacción de necesidades a corto plazo, señala que las personas físicas en la actualidad disfrutan de derechos de protección de datos diferentes debido a la fragmentación y a la incongruente aplicación y ejecución de la legislación en los distintos Estados miembros. Además, las personas físicas a menudo no saben lo que pasa con sus datos personales y no tienen ningún tipo de control sobre ellos y por lo tanto no llegan a ejercer sus derechos de forma efectiva.

107. Cfr. la Comunicación de la Comisión titulada «Un enfoque global de la protección de los datos personales en la Unión Europea» –COM (2010) 609 final– y el Plan de

también la Comisión ha elegido como norma general de protección de datos el Reglamento al ser una norma de derecho derivado institucional, que a diferencia de la Directiva, no obliga al Estado miembro destinatario en cuento al resultado que debe conseguirse –dejando a las autoridades nacionales la elección de la forma y de los medios– sino que tiene un alcance general, siendo obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro –art. 288 TFUE–. El Reglamento es, pues, el instrumento jurídico adecuado para lograr una mayor armonización y seguridad jurídica, estableciendo un modelo uniforme que sirva para superar las actuales diferencias y la fragmentación jurídica que se derivan de las distintas aplicaciones nacionales de la Directiva, estableciendo un auténtico sistema europeo de protección de datos[108]. La aproba-

acción de la Comisión por el que se aplica el Programa de Estocolmo –COM (2010) 171 final–. Previamente, en el año 2010, el Consejo Europeo, en el Programa de Estocolmo –«Una Europa abierta y segura que sirva y proteja al ciudadano»–, había invitado a la Comisión a evaluar el funcionamiento de los instrumentos de la UE en materia de protección de datos y a presentar, en caso necesario, nuevas iniciativas legislativas y no legislativas. El Parlamento Europeo se pronunció por un régimen general de protección de datos en la UE –Resolución del Parlamento Europeo sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada «Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos – Programa de Estocolmo», adoptada el 25 de noviembre de 2009–. La Comisión señala que [s]i *bien el marco jurídico actual sigue siendo adecuado por lo que respecta a sus objetivos y principios, no ha evitado, sin embargo, la fragmentación en 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. Ha llegado por ello el momento de establecer un marco más sólido y coherente en materia de protección de datos en la UE, con una aplicación estricta que permita el desarrollo de la economía digital en el mercado interior, otorgue a los ciudadanos el control de sus propios datos y refuerce la seguridad jurídica y práctica de los operadores económicos y las autoridades públicas*» –«Contexto» de la Propuesta de Reglamento–. La Resolución del Parlamento Europeo, de 6 de julio de 2011, aprobó un informe sobre la protección de los datos personales en la Unión Europea que respaldaba el enfoque adoptado por la Comisión para establecer un nuevo marco de protección de datos personales. También el Consejo de la Unión, en sus conclusiones adoptadas el 24 de febrero de 2011, manifestó su apoyo a la intención de la Comisión de reformar el marco de protección de datos y mostró su acuerdo con muchos elementos de la posición de la Comisión. Igualmente, el Comité Económico y Social Europeo se mostró a favor del objetivo de la Comisión de garantizar una aplicación más coherente de las normas de la UE en materia de protección de datos en todos los Estados miembros y de llevar a cabo una revisión adecuada de la Directiva.

108. En este sentido hay que entender que la propuesta del Reglamento –por tanto, el legislador– delegue en la Comisión el poder de adoptar actos no legislativos de alcance general que completen o modifiquen determinados elementos no esenciales del Reglamento (actos cuasi legislativos), de conformidad con el artículo 290 del TFUE, en muchas materias como la licitud del tratamiento; las condiciones de licitud para tratamientos específicos; la especificación de los criterios y condiciones en relación con el consentimiento de los niños; el tratamiento de categorías especiales de datos; la especificación de las medidas de seguridad técnicas y organizativas; los criterios y requisitos relativos a la información al interesado y en relación con el derecho de acceso; el derecho al olvido y a la supresión; la actualización del importe de las multas administrativas; etc. El art. 86 señala las condiciones a los que están sujetas los poderes de la Comisión para adoptar actos delegados Igualmente, la propuesta de Regla-

ción de esta nueva normativa europea de protección de datos personales está destinada a garantizar mejor tanto el derecho a la protección de los datos personales como el funcionamiento del mercado interior y la libre circulación de información personal. Como había señalado la Comisión en el pasado, esta nueva regulación debe promover la igualdad de condiciones de los agentes económicos, contribuyendo, a través de la simplificación del entorno normativo, a que se fomente la actividad transfronteriza y la competitividad.

A) El objeto y el ámbito de aplicación material y territorial. El problema de las corporaciones que tienen su sede fuera de la Unión Europea.

La propuesta de Reglamento tiene como objeto las normas relativas a la protección de las personas *físicas* en lo que respecta al *tratamiento* de sus datos personales y las normas relativas a la libre circulación de tales datos –art. 1.1–, por lo que existe una continuidad esencial con la Directiva 95/46/CE en dos aspectos esenciales. El primero de ellos es que la propuesta de Reglamento no protege los datos personales sino sólo los datos personales sometidos a tratamiento[109]. Así, mantiene como ámbito de aplicación material los tratamientos automatizados así como los tratamientos no automatizados o manuales de datos personales contenidos o destinados ser incluidos en un fichero –art. 2.1-[110]. El segundo aspecto es que la protección de la propuesta de Reglamento se extiende a las personas físicas, no a las personas jurídicas, una cuestión que sin embargo había sido motivo de divergencia ya que algunos países habían considerado como dato de carácter personal también aquellos referidos a las personas jurídicas[111]. La propuesta de Reglamento es clara en este punto ya que limita su

---

mento confiere a la Comisión competencias de ejecución con la finalidad de garantizar unas condiciones uniformes para la aplicación del Reglamento. El artículo 87 recoge la disposición relativa al procedimiento del comité necesario para la atribución de competencias de ejecución a la Comisión.

109. Esta es una cuestión sobre la que hemos hecho incidencia reiteradamente –*La protección de datos personales*. cit. pp. 731-741–.

110. La propuesta de Reglamento reitera en este punto las previsiones existentes en la Directiva 95/46/CE. Así, basta que exista tratamiento automatizado de datos personales para que sea aplicable la normativa de protección de datos, con independencia de que exista o no fichero. En cambio, es necesario que exista un fichero para que pueda hablarse de tratamiento manual. La definición de fichero manual era mucho más precisa en la Directiva al referirse a «archivo estructurado según criterios específicos relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trate» –Considerando 16 de la Directiva 95/46/CE, que ha servido entre nosotros para resolver la problemática sobre la apostasía y los expedientes de bautismo –SSTS, de 19.9.2008 y de 14.10.2008–. En cambio, la propuesta de Reglamento se limita a hablar de ficheros y carpetas estructuradas con arreglo a criterios específicos –Considerando 13–, sin hacer referencia a que esta estructuración se realice en virtud de criterios relativos a personas ni a la accesibilidad de esta información.

111. Es el caso de Austria, Italia y Luxemburgo. Dinamarca y Alemania también lo incluyen en algunos supuestos. Cfr. el apdo. «The substantive scope of the national laws (Article 3)» en el *Primer informe sobre la aplicación de la Directiva*, cit.. La LOPD incluye dentro su ámbito de aplicación los tratamientos de datos de carácter personal, entendiendo por estos «cualquier información concerniente a personas físicas identificadas o identificables» –art. 3.a)–, excluyendo las personas jurídicas. Además, posteriormente, el RPDP también excluye los datos de las personas físicas de contacto que

objeto en el art. 1.2 a la protección de «los derechos y libertades de las personas *físicas*» y su ámbito material en el art. 2.1 al tratamiento de sus datos personales, excluyendo claramente de su ámbito de protección los datos de las personas jurídicas[112].

---

presten sus servicios en personas jurídicas así como los datos relativos a empresarios individuales –los autónomos que no tienen forma jurídica societaria– cuando hagan referencia a ellos en su calidad de industriales, comerciantes o navieros –art. 2.2 y 2.3–. A nuestro juicio, estos dos preceptos del Reglamento podían ser incompatibles con la Directiva 95/46/CE y con la LOPD, que tienen como ámbito de aplicación los datos de personas físicas identificadas o identificables sometidos a tratamiento, no excluyendo de su ámbito de aplicación los datos personales cuando se utilizan para una finalidad comercial. La finalidad del tratamiento no delimita el ámbito de aplicación del derecho fundamental a la protección de datos personales, que es existencia de datos personales sometidos a tratamiento. No tendría sentido que este derecho fundamental protegiera los datos identificativos y de domicilio de una persona física y no protegiera al mismo tiempo los datos relativos al puesto profesional o a una actividad comercial o industrial, ya que esa información, sometida a tratamiento, puede ocasionar una vulneración de nuestros derechos fundamentales, permitiendo establecer perfiles o clasificaciones que impidan el ejercicio de los derechos y el libre desarrollo de la personalidad. Otra cosa distinta es que los tratamientos de datos identificativos y profesionales, a pesar de estar incluidos dentro del ámbito de aplicación del derecho fundamental a la protección de datos personales, se encuentren sometidos a límites legítimos, como sería su tratamiento y su cesión en el marco de una relación negocial o administrativa (arts. 6.2 y 11.2 LOPD). Esta cuestión la hemos analizado *La protección de datos personales*, cit. pp. 942-953.

112. El Considerando 12 de la propuesta de Reglamento señala que por lo que respecta al tratamiento de datos relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto, *nadie puede invocar la protección del presente Reglamento*. Ello también es de aplicación cuando el nombre de la persona jurídica incluya los nombres de una o más personas físicas. Sin embargo, la propuesta de Reglamento no resuelve la cuestión relativa a los ficheros con datos de personas físicas de contacto que presten sus servicios en personas jurídicas así como los datos de personas físicas que son empresarios individuales y actúan en su calidad de industriales, comerciantes o navieros. Hay que señalar que MARTÍN Y PÉREZ DE NANCLARES, J., *–loc. cit.* pp. 231-233–, considera, que en determinados supuestos también las personas jurídicas podrían llegar a hacerse acreedoras por analogía de una protección de sus intereses legítimos por derivación del art. 8 de la Carta, que debe interpretarse también dentro del especial contexto de la Unión Europea en el que las empresas son en buen número de ocasiones las destinatarias principales de las acciones y normas comunitarias. Hay que tener en cuenta que el derecho de toda persona a la protección de los datos de carácter personal que le conciernan se halla íntimamente vinculado al derecho al respeto a la vida privada del art. 7 de la Carta. Recuerda que el TJ –Sentencia de 21 de septiembre de 1989, *Hoechst*, Rec. 46/87 y 227/88– ha reconocido a las empresas el disfrute de determinadas manifestaciones del derecho a la inviolabilidad del domicilio, señalando que las intervenciones de los poderes públicos en la esfera de la actividad privada de cualquier persona jurídica han de tener fundamento legal y deben respetar el principio de proporcionalidad. Igualmente señala que la Directiva 2002/58/CE, que desarrolla la protección de datos a las comunicaciones electrónicas, sí protege los intereses legítimos de los abonados que sean personas jurídicas –art. 1.2–.

Más complicado ha sido qué se entiende por datos personales. Hasta ahora ha habido diferencias entre los Estados Miembros en relación con el concepto de dato personal, que era definido por el art. 2.a) de la Directiva como toda información sobre una persona física identificada o identificable, siendo identificable toda persona cuya identidad pueda determinarse mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, económica, cultural o social. Por una parte, las divergencias están en si hay que emplear o no una aproximación relativa al concepto de dato personal en el sentido de que los datos deben ser considerados personales solo para alguien que pueda relacionar el dato con una persona o con un individuo identificado. Así, distintas Leyes consideran que *encoded or pseudonymised data* son datos personales para aquellos que tienen acceso al mismo tiempo al dato y a la clave, pero no lo son para aquellas otras personas que, al no disponer de la clave, no pueden establecer tal relación[113], un aspecto que tiene consecuencias en relación con la investigación sanitaria que se realiza frecuentemente en redes internacionales mediante datos codificados o reversiblemente disociados[114]. Otro problema es la consideración o no como datos de carácter personal de la información sobre fallecidos. La mayoría de las leyes se aplican a las personas naturales o físicas, excluyendo a los fallecidos. Algunas leyes lo manifiestan de manera clara refiriéndose a *natural living persons* or *living individuals*; en cambio, otras se aplican a personas fallecidas[115]. Sin embargo, la propuesta de Regla-

113. La Ley Austriaca considera estos datos como «indirectly identificable data»; la Ley Alemana los considera «pseudonymised data». La Ley Británica considera solamente como datos personales «*data relating to a living individual who can be identified from those data or... from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller*».

114. El art. 3.k) de la Ley 14/2007, de 3 de julio, de Investigación biomédica define el dato codificado o reversiblemente disociado como aquel dato no asociado a una persona identificada o identificable por haberse sustituido o desligado la información que identifica a esa persona utilizando un código que permita la operación inversa. Cfr. NICOLÁS JIMÉNEZ, P., *La protección jurídica de los datos genéticos de carácter personal*, Cátedra de Derecho y Genoma Humano, Comares, Granada, 2006, pp. 327-329 y 351-353, Así, en el proyecto «Genetic databases for international biomedical research. The ICGC» hemos defendido la conveniencia de que la cesión a centros de investigación internacionales se haga de datos disociados o codificados, teniendo en cuenta también la Opinión 4/2007, del Grupo de Trabajo del Art. 29. Cfr. *infra* nota 237 sobre la investigación biomédica.

115. Este es el caso de Portugal dónde la legislación de aquel país se aplica a los fallecidos en virtud de una interpretación de la autoridad de protección de datos de la legislación de protección de datos y del Código Civil. Luxemburgo autoriza a los familiares cercanos de los fallecidos el acceso a la última información de salud de éste. Francia establece la posibilidad de los familiares de requerir al responsable del fichero que rectifique la información que no contemplaba el fallecimiento. La LOPD no dice nada al respecto. En cambio, el RPDP establece que no será de aplicación a los datos referidos a personas fallecidas, sin perjuicio de que las personas vinculadas a éste puedan dirigirse a los responsables de los ficheros que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo y solicitar en su

mento no resuelve todas estas cuestiones, aunque aclara algunas. Así, precisa, con mala técnica normativa, el concepto de dato personal, señalando que es toda información relativa a un interesado, y definiendo interesado como toda persona física identificada, directa o indirecta, por medios que puedan ser utilizados razonablemente por el responsable o por cualquier otra persona física o jurídica[116], añadiendo elementos que no estaban en la Directiva pero

caso, la cancelación de los datos –art. 2.4–. Lógicamente, los fallecidos no pueden disponer de la protección de datos como derecho autónomo –no pueden ser informados, ni consentir ni pueden ejercitar los derechos de acceso, rectificación, cancelación y oposición–. Sin embargo, la legislación –la Ley 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, la Ley 41/2002, de 14 de noviembre, de Autonomía del paciente, la Ley 14/2007, de 3 de julio de Investigación biomédica, la Ley 16/1985, de 25 de junio, de Patrimonio histórico español, etc. reconocen el derecho a la intimidad de las personas fallecidas y la obligación de respetar la confidencialidad de su información y de sus muestras genéticas. No es posible que un fallecido se encuentra protegido por el derecho a la intimidad y no disponga al mismo tiempo de la protección de datos personales que es su garantía institucional. De esta forma, el dato personal de un fallecido no es *res nullius* sino que es un bien jurídico que requiere protección; subsiste el deber de secreto médico –no se puede dar información sobre la enfermedad que lleva al fallecimiento de una persona–; es necesario implantar medidas técnicas y organizativas que garanticen la seguridad de los datos; hay que respetar el principio de calidad que implica que no puede tratarse información excesiva y que persiste la obligación de conservar la historia clínica de los fallecidos y de cancelarla cuando haya dejado de ser necesaria; no se puede abandonar historias clínicas de fallecidos en la calle; no se puede comunicar ni publicarse en Internet la información relativa a fallecidos, ni puede ser vendida ni objeto de reutilización pública. Por tanto, hay que respetar la protección de los datos personales de los fallecidos, de la misma manera que no se puede atentar contra su honor ni utilizar su imagen porque existen bienes jurídicos vinculados a la dignidad de una persona que no se extinguen con la muerte. Es un error grave afirmar que es innecesario aplicar la normativa de protección de datos personales a los fallecidos porque estos se encuentran ya protegidos por el derecho a la intimidad. Además de que no es posible jurídicamente disponer de intimidad y carecer al mismo tiempo de su garantía de instituto, tampoco es posible en la práctica tutelar la intimidad de los fallecidos si no se implementan los principios que garanticen ésta «en lo que concierne al tratamiento de los datos personales». Esta es una cuestión que hemos analizado extensamente en *La protección de datos personales*, cit. pp. 1119-1130.

116. El Grupo de Trabajo del Art. 29 precisa que la potencial identificación indirecta tiene que ser por «medios que puedan ser utilizados razonablemente por el responsable o por cualquier otra persona física o jurídica», es decir, que no le supongan un esfuerzo desproporcionado. Cfr. el Dictamen 4/2007 del Grupo de Trabajo del Artículo 29 sobre el concepto de datos personales. *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf* El considerando 26 de la Directiva –no el texto articulado de ésta– como el Considerando 23 y el art. 4.1) de la propuesta de Reglamento señalan que para determinar si una persona es identificable deben tenerse en cuenta todos los medios que razonablemente pudiera utilizar el responsable del tratamiento o cualquier otro individuo para identificar a dicha persona. Llama atención que esta precisión de la propuesta de Reglamento se hace no en la definición de dato personal, que es la que ayuda a concretar el ámbito de aplicación material, sino en la definición de interesado –art. 4.1–.

que ya habían sido expresamente admitidos por el Grupo de trabajo del Artículo 29 como la dirección «ip», los datos de localización, el identificador en línea[117] o uno o varios elementos específicos de identidad genética[118].

La propuesta de Reglamento establece un conjunto de exclusiones de su ámbito de aplicación material, entre las que están las actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión como es la seguridad nacional, las actividades incluidas en la política exterior y de seguridad común y las actividades relativas a la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales[119]. La propuesta de Reglamento también excluye de su ámbito de aplicación material, como hacía el art. 3.2 de la Directiva 95/46/CE, los tratamientos de datos personales que lleve a cabo una persona física en el ejercicio de sus actividades

117. En relación con los identificadores en línea, el Considerando 24 de la propuesta de Reglamento señala que «cuando utilizan servicios en línea, las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como las direcciones de los protocolos de internet o los identificadores de sesión almacenados en *cookies*. Ello puede dejar huellas que, combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas e identificarlas. De ello se deduce que los números de identificación, los datos de localización, los identificadores en línea u otros factores específicos *no necesariamente tienen que ser considerados datos de carácter personal en toda circunstancia*. A nuestro juicio, como hemos señalado anteriormente, las *cookies*, con independencia de la información almacenada en las mismas, pueden vincularse con el usuario de un determinado dispositivo conectado a Internet y permite obtener el perfil del mismo. Si bien la dirección IP no siempre es estática sino que puede ser dinámica, además de que no identifica a un usuario sino un equipo _que puede ser de utilización compartida, por ejemplo en puntos de acceso público a Internet o en un cibercafé–, en muchas ocasiones es una «información concerniente a personas físicas identificadas o identificables». El TJUE ha señalado que el derecho a la protección de los datos personales y el derecho a la vida privada –arts. 7 y 8 de la Carta– se aplican a toda información sobre una persona física identificada o identificable –Sentencia, de 9.11.2010, as. *Volker und Markus Schecke y Eifert*, apdo. 52.

118. La propuesta de Reglamento introduce en las Disposiciones Generales –art. 4– un conjunto de definiciones nuevas –que no estaban en la Directiva ni tampoco todas en la normativa española, aunque sí algunas de ellas en distintos documentos del Grupo del Artículo 29–, que aportan una mayor seguridad jurídica, como la de violación de datos personales, datos genéticos, datos biométricos, datos relativos a la salud, establecimiento principal –que afecta al ámbito de aplicación territorial–, representante, empresa, grupo de empresas, normas corporativas vinculantes, niño, autoridad de control. Sin embargo, no parece adecuado utilizar el apartado de definiciones para llevar a cabo una regulación sustancial, afirmando, por ejemplo que «niño» es toda persona menor de 18 años o que los responsables del tratamiento o los criterios específicos para su nombramiento pueden ser fijados por el Derecho de la Unión o por la legislación de los Estados miembros.

119. Esta materia es objeto de una Propuesta de Directiva del Parlamento Europeo y del Consejo y que no podemos analizar en este trabajo por razones de espacio. Lógicamente, el Reglamento no regula los tratamientos de datos de carácter personal por las instituciones, órganos y organismos de la Unión, que está sujetos al Reglamento nº 45/2001, ya citado. No obstante, este último Reglamento deberá ser armonizado con el texto que se apruebe de Reglamento general de protección de datos personales.

exclusivamente personales o domésticas, precisando con acierto «siempre que no tengan un interés lucrativo» –art. 2.2.d)–[120]. Esta cuestión tiene particular interés en el ámbito de las redes sociales, donde, si bien la mayoría de los tratamientos que llevan a cabo los usuarios afectan a la esfera familiar y de amistad –y se encuentran excluidos, por tanto, del ámbito de aplicación material de la normativa[121]–, hay otros tratamientos desarrollados por los usuarios en los servicios de redes sociales que no pueden ser considerados de carácter «personal o doméstico» y que, por tanto, no se encuentran excluidos de la normativa de protección de datos[122]. Esto ocurriría, por ejemplo, cuando los usuarios utilizan el servicio de red social como una plataforma de colaboración con una empresa para una finalidad comercial[123] o con medio para una finalidad de carácter político o social, que no son finalidades personales o domésticas[124]. Además, la propuesta de Reglamento no tiene en cuenta la Sentencia *Lindqvist* que establecía que los tratamientos que consistan en la publicación de datos personales de manera que éstos sean accesibles para una pluralidad de personas,

120. El Considerando 15 de la Propuesta pone como ejemplo de tratamientos personales o domésticos la correspondencia y la llevanza de un repertorio de direcciones, sin ningún interés lucrativo y, por tanto, sin conexión alguna con una actividad profesional o comercial. Sin embargo precisa que esta exención no debe aplicarse a los responsables o encargados del tratamiento que proporcionen los medios para tratar los datos personales relacionados con tales actividades personales o domésticas.

121. La Audiencia Nacional, en su Sentencia de 15 de junio de 2006, ha establecido que se consideran ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas los datos que «afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en estos ámbitos».

122. El Dictamen 5/2009 del Grupo de Trabajo del Artículo 29 precisa en qué circunstancias las actividades de un usuario de servicios de redes sociales no están cubiertas por la «exención doméstica». Una preocupación de este Grupo de Trabajo es la difusión y utilización de la información disponible en los servicios de redes sociales con fines secundarios, no buscados. Así, el Dictamen 5/2009 señala que una tendencia creciente que se evidencia en los servicios de redes sociales es el paso de la *Web 2.O* para el ocio a la *Web 2.0* para la productividad y los servicios.

123. Así, muchas redes sociales especializadas son básicamente redes de profesionales, como *Linkedlnn* –que quieren favorecer las relaciones entre profesionales– o *Ryze.com* –que hace conexiones de empresas para resolver sus necesidades–. En general, la información de relaciones profesionales no forma parte nuclear de la privacidad de las personas. En ese sentido, las redes generalistas tienen un mayor nivel de riesgo ya que no sólo ofrecen información profesional sino también, vivencias o aficiones. No obstante, no están excluidos de la LOPD los tratamientos de datos personales de potenciales clientes. *MySpace*, si bien es una red generalista, dispone de un grupo formado por artistas que la aprovechan para dar a conocer sus trabajos ante el público en general.

124. El hecho de que no se aplique al usuario la excepción de los tratamientos con fines personales o domésticos no significa que no sean de aplicación otras excepciones, como son las destinadas a aquellos tratamientos que suponen el ejercicio de otros derechos fundamentales, como la libertad de información y de expresión, que en todo caso se encuentran limitados por el derecho a la intimidad, como ha establecido el art. 80 de la propuesta de Reglamento y el art. 9 de la Directiva 95/46/CE, y analizaremos más adelante –*infra* apdo. V.E)–.

aunque sean personales o domésticos y no tengan un interés lucrativo, estarían dentro del ámbito de aplicación material de la normativa[125]. De esta forma, un número muy elevado de contactos por parte de un usuario en una red social implica que no conoce a muchos de ellos –consecuencia de una aceptación indiscriminada de peticiones de amistad sin que exista una relación personal-[126], por lo que no puede hablarse de datos que afecten a la esfera familiar y de amistad o de tratamientos personales o domésticos. Tampoco puede hablarse de un tratamiento «personal o doméstico» cuando el perfil y los contactos personales se encuentran abiertos para todos los usuarios de la red social o cuando la información personal puede ser indexada a través de motores de búsqueda fuera de la propia red. En estos supuestos, el usuario debe ser considerado responsable de un tratamiento, aplicándole el mismo régimen que en la publicación de datos personales en otras plataformas tecnológicas de manera abierta en Internet[127]. De hecho, la interpretación limitada del concepto de tratamiento personal o doméstico es una consecuencia del principio *pro libertate*, que obliga a una interpretación restrictiva de los límites a un derecho fundamental, especialmente cuando afecta al contenido esencial del derecho y a los interés jurídicos que le dan vida. Así, excluir estos tratamientos del derecho fundamental a la protección de datos personales afectaría a los intereses jurídicos que dan vida a este derecho –especialmente de terceras personas–, dejándolos sin protección –STC 11/1981, de 8 de abril–. Este planteamiento es una exigencia del respeto a los derechos de las personas en las redes sociales. Así, no tendría sentido que

125. La STJCE, de 6.11.2003, as. *Lindqvist*, analiza el caso de la catequista sueca que publicó datos personales en Internet. Cfr. sobre la cuestión GUERRERO PICÓ, M.C., *op. cit*. pp. 356-361.

126. Muchas decisiones en Internet, como la aceptación de una petición de amistad o la determinación de un perfil abierto en las redes sociales, a lo que se puede añadir también la inserción de comentarios en *Twitter* o las respuestas con automatismos a algunos correos electrónicos, se toman, a nuestro juicio, en lo que Kahneman ha definido el sistema 1, el pensamiento más intuitivo y emocional, que requiere un menor esfuerzo mental y que concluye rápidamente sin esperar la conciencia racional, utilizando la memoria –y especialmente las emociones más intensas grabadas en la misma–, como patrón para la toma de decisiones. Este comportamiento generalmente incrementa la posibilidad de error y crea problemas a los usuarios. Lo razonable sería que estas decisiones en Internet, vistas las consecuencias –por ejemplo, las continuas disculpas por comentarios insertados en *Twitter*–, se tomaran en el sistema 2, que es deliberativo y lógico, conlleva un proceso de análisis y examen crítico de la evidencia disponible y permite juicios más consistentes, pero que es también más lento. Cfr. KAHNEMAN, D., *Thinking, Fast and Slow*, Farrar, Straus and Giroux, New York, 2011, esp. pp. 19-107 y 408-419.

127. Hemos señalado en otro momento que la realización de fotografías de grupos de menores en centros educativos por parte de los padres puede considerarse un tratamiento personal o doméstico pero su publicación en Internet en abierto supone un tratamiento que sale de la esfera personal y se constituye en una cesión indiscriminada de datos personales. 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, señala que la protección de estos derechos «quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia» –art. 2.1–.

no pueda aplicarse la normativa de protección de datos personales –y, por tanto, no esté vigente el derecho fundamental a la protección de la información personal– a tratamientos que suponen una cesión indiscriminada de datos –incluso sensibles– de terceras personas a un número muy amplio de usuarios de una red social, a todos los usuarios de la misma sin restricciones de acceso o al público en general –a través de motores de búsqueda–. Esta publicación de datos personales debe suponer que el usuario de la red social asume la responsabilidad del tratamiento –en relación con las personas cuyos datos y fotografías aparecen publicadas en el perfil–, lo que le obliga, en especial, al cumplimiento de los principios de información y consentimiento y al respeto a los derechos de los afectados, respondiendo también no sólo ante las Agencias de Protección de Datos, sino también en el orden jurisdiccional civil como en el penal por las vulneraciones de los derechos de las personas que se deriven de la información incorporada a la red social.

Especial mención merece el ámbito de aplicación territorial de la propuesta de Reglamento –art. 3– ya que trata de resolver la problemática de jurisdicción y de ley aplicable que plantean las corporaciones internacionales que ofrecen servicios de tratamiento de datos –redes sociales virtuales, motores de búsqueda, servicios de computación en nube– y que no tienen su sede en la Unión Europea. Hasta ahora, la Directiva 95/46/CE se aplicaba al responsable del tratamiento cuando éste fuera efectuado en el marco de las actividades de un establecimiento del responsable en el territorio de un Estado miembro o cuando el responsable que no estuviera establecido en el territorio de la Comunidad recurra a medios, automatizados o no, situados en el territorio de un Estado miembro, salvo en el caso de que dichos medios de utilicen sólo con fines de tránsito –art. 4.1.de la Directiva y art. 2.1.c) LOPD-[128], supuestos que han dado lugar

128. Así, por ejemplo, las redes sociales utilizan medios ubicados dentro de la Unión Europea, no sólo por la utilización de *cookies* o *barners*, sino porque la recogida de datos se produce en parte dentro de la Unión Europea. Cfr. el «Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecido fuera de la UE», del Grupo de Trabajo del Artículo 29, aprobado el 30 de mayo de 2002 –*http://ec.europa. eu/justice_home/fsj/privacy*–. El Grupo de Trabajo del Artículo 29, en el Dictamen 5/2009, señala que las disposiciones de la Directiva relativas a la protección de datos se aplican en la mayoría de los casos a los proveedores de servicios de redes sociales, aunque su sede se encuentre fuera de la Unión Europea. El Grupo de Trabajo del artículo 29 se remite a su dictamen previo sobre los motores de búsqueda, con el fin de obtener información complementaria sobre las cuestiones del establecimiento y la utilización de equipo como determinantes para la aplicabilidad de la Directiva relativa a la protección de datos y de las normas derivadas del tratamiento de las direcciones IP y la utilización de «cookies. El Dictamen 8/2010, de 16 de diciembre, sobre Derecho Aplicable, elaborado por el Grupo de Trabajo del Artículo 29 trata de clarificar la aplicación del art. 4 de la Directiva «en un contexto internacional más amplio». Así, en relación con el recurso a «medios», que pueden suponer la aplicación de la Directiva a responsables del tratamiento no establecidos en el territorio de la UE, el dictamen aclara que debería aplicarse cuando no haya ningún establecimiento en la UE *que desencadene la aplicación del artículo 4* o cuando el tratamiento *no se realice en el marco* de dicho establecimiento. Igualmente explica el sentido de que se utilicen medios en los Estados de la Unión para la recogida de datos aunque el responsable

recientemente a una cuestión prejudicial planteada por la Audiencia Nacional[129]. Sin embargo, la propuesta de Reglamento no esgrime para el ámbito de aplicación territorial el criterio –presente en el art. 4.1.c) de la Directiva 95/46/CE– relativo al empleo de medios técnicos en los Estados de la Unión –que el responsable que tiene su sede fuera de la Unión Europea recurra para el tratamiento de datos personales a medios, automatizados o no, situados en los Estados de la Unión– sino que emplea «un factor de conexión más específico» que tiene en cuenta la necesaria «orientación hacia las personas». Para ello, se establece que el Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable no establecido en la misma cuando las actividades de tratamiento estén relacionadas con la oferta

---

esté fuera de la misma, poniendo como ejemplo el uso de vehículos para la recogida de información sobre punto de acceso *wifi* o la propia computación en nube usando la instalación de *cookies* o *javascripts*. Cfr. Dictamen 8/2010 sobre Derecho Aplicable elaborado por el Grupo de Trabajo de la Unión Europea del Artículo 29, que está accesible en *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_es.pdf*

129. El Auto de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 27 de febrero de 2012, planteó una cuestión prejudicial –que después analizaremos en lo que hace referencia al derecho al olvido en Internet, *infra* apdo. V.D)–, en el marco de las Resoluciones de tutela de derechos que la AEPD ha dictado frente a *Google*. Así, se pregunta si debe interpretarse que existe un establecimiento cuando la empresa proveedora del motor de búsqueda crea en un Estado Miembro una oficina o filial destinada a la promoción y venta de los espacios publicitarios del buscador, que dirige su actividad a los habitantes de ese Estado, o cuando la empresa matriz designa a una filial ubicada en ese Estado miembro como su representante y responsable del tratamiento de dos ficheros concretos que guardan relación con los datos de los clientes que contrataron publicidad con dicha empresa o cuando la oficina o filial establecida en un Estado miembro traslada a la empresa matriz, radicada fuera de la Unión Europea, las solicitudes y requerimientos que le dirigen tanto los afectados como las autoridades competentes en relación con el respeto al derecho de protección de datos, aun cuando dicha colaboración se realice de forma voluntaria [aquí debería producirse una respuesta afirmativa a la luz del art. 3.2 de la propuesta de Reglamento que analizamos]. También se pregunta si debe interpretarse el art. 4.1.c de la Directiva 95/46/CE en el sentido de que existe un «recurso a medios situados en el territorio de dicho Estado miembro» cuando un buscador utilice arañas o robots para localizar e indexar la información contenida en páginas web ubicadas en servidores de ese Estado miembro o cuando utilice un nombre de dominio propio de un Estado miembro y dirija las búsquedas y los resultados en función del idioma de ese Estado miembro [ambas respuestas serían afirmativas a la luz de los Dictámenes 5/2009 y 8/2010, del Grupo del Art. 29]. También se pregunta si puede considerarse como un recurso a medios, en los términos del art. 4.1.c de la Directiva 95/46/CE, el almacenamiento temporal de la información indexada por los buscadores en internet [existe una responsabilidad del buscador sobre sus propios tratamientos, como señalaremos más adelante] y si puede entenderse que este criterio de conexión concurre cuando la empresa se niega a revelar el lugar donde almacena estos índices alegando razones competitivas. Por último, en el caso de que el TJUE señale que no concurren los criterios de conexión previstos en el art. 4 de la Directiva, se pregunta si debe aplicarse la Directiva 95/46/CE en materia de protección de datos, a la luz del art. 8 de la Carta Europea de Derechos Fundamentales, en el país miembro donde se localice el centro de gravedad del conflicto y sea posible una tutela más eficaz de los derechos de los ciudadanos de la Unión Europea.

de bienes o servicios a dichos interesados en la Unión y con el control de su conducta –art. 3.2–, siguiendo en este punto el Dictamen 8/2010, del Grupo de Trabajo del Artículo 29[130]. Esta ampliación del ámbito de aplicación territorial se complementa con la obligación de los responsables del tratamiento no establecidos en la Unión de designar un representante en la misma, que actúe en lugar del responsable, al que puede dirigirse cualquier autoridad de control en lo que respecta al cumplimiento de sus obligaciones, y que debe estar establecido en uno de los Estados miembros en que residan los interesados cuyos datos personales son objeto de tratamiento en el contexto de una oferta de bienes o servicios o cuyo comportamiento esté siendo controlado –arts. 4.14 y 25–[131].

La propuesta de Reglamento mejora la posición jurídica y las garantías de los ciudadanos europeos, teniendo en cuenta la naturaleza global de Internet, basado en plataformas digitales que no se circunscriben a un solo territorio. De esta forma, se trata de poner fin a una práctica frecuente de las Corporaciones internacionales, que alegan reiteradamente que no les es de aplicación el derecho europeo, negando con ello a sus usuarios europeos algunos derechos que la normativa les garantiza y, además, obligando a los ciudadanos europeos a solicitar la tutela de sus derechos ante Cortes internacionales, principalmente la estadounidense, lo que genera una indudable indefensión. La propuesta de Reglamento –al igual que anteriormente lo hacia la Directiva y los Dictámenes del Grupo de Trabajo del Art. 29– obliga a los proveedores de servicios en Internet –buscadores, redes sociales– a someterse a la legislación europea de protección de datos personales, de forma que se pueda garantizar de manera efectiva los derechos de los ciudadanos europeos frente a las prácticas de estas empresas, sometiéndolas, además, a las competencias de control de las autoridades administrativas de protección de datos de los Estados de la Unión y de sus órganos jurisdiccionales –y no, por ejemplo, a los de EEUU–[132].

---

130. Cfr. Dictamen 8/2010 sobre Derecho Aplicable elaborado por el Grupo de Trabajo de la Unión Europea del Artículo 29 había destacado algunos campos que podían ser objeto de mejora. Así, este dictamen abre la puerta a que el criterio de los medios se complemente con «la orientación a los destinatarios, que dé lugar a la aplicación de la legislación de la UE sobre protección de datos cuando la actividad de tratamiento de datos personales se destine a ciudadanos que se encuentren en la UE».

131. No es aplicable la obligación de designar representante cuando el responsable esté establecido en un país con nivel adecuado de protección, cuando sea una empresa con menos de doscientos cincuenta trabajadores o un organismo público, o cuando el responsable ofrezca sólo ocasionalmente bienes o servicios a interesados residentes de la Unión. El carácter ocasional se desprende de analizar las actividades generales del responsable para determinar si la oferta de bienes y servicios a los interesados es accesoria a las actividades principales –Considerando 64–. En todo caso, hay que recordar que la Directiva 95/46/CE ya preveía que cuando el responsable no estuviera establecido en el territorio de la Unión Europea y utilice en el tratamiento medios situados en un país de la Unión Europea, deberá designar un representante en ese país –art. 4.2–, lo que no siempre se cumplía.

132. Recientemente *Google* ha presentado una nueva política de privacidad, en la que prevé crear un perfil de datos del usuario utilizando todas las aplicaciones derivadas del buscador como redes sociales o programas de localización geográfica. La Comisaria Europea de Justicia, Viviane Reding, ha pedido a Google que deje en suspenso las

B) Las obligaciones del responsable: la evaluación de impacto, el *Data Protection Officer* y la conservación de la documentación.

La Directiva 95/46/CE no regulaba en ningún artículo específico las obligaciones del responsable y del encargado del tratamiento, encontrándose éstas desgranadas en todo el texto. En cambio, la propuesta de Reglamento dedica específicamente el Capítulo IV al «Responsable del tratamiento y encargado del tratamiento». En este Capítulo se incluyen un conjunto de obligaciones generales del responsable del tratamiento –art. 22–, entre las que destacan la adaptación de políticas y la implementación de medidas apropiadas no sólo para asegurar sino también para «poder demostrar» que el tratamiento de datos personales se lleva a cabo de conformidad con el Reglamento, como serían la realización de evaluaciones de impacto en relación con la protección de datos, el cumplimiento de los requisitos en materia de autorización o consultas previas con la autoridad de control, la designación de un delegado de la protección de datos, la conservación de la documentación y la implementación de los requisitos en materia de seguridad. Además, le corresponde al responsable implementar mecanismos para verificar la eficacia de estas medidas, comprobación que podrá incluir –siempre que no sea desproporcionado– una auditoría independiente interna o externa, que no estará limitada, como hasta ahora, a la confirmación del cumplimiento de las medidas de seguridad –la conocida auditoría bienal prevista en el art. 96 del RPDP para los ficheros y tratamientos a los que le corresponde implantar medidas de seguridad de nivel medio y alto– sino que va a revisar el cumplimiento de la legislación –el respeto de los principios y de los derechos, esto es, la llamada parte jurídica de los tratamientos–. En todo caso, hay que señalar que la propuesta de Reglamento contiene distintas excepciones a las obligaciones del responsable –también a los principios y derechos y a la imposición de sanciones económicas– cuando el responsable del tratamiento sea una microempresa o una empresa de menos de doscientos cincuenta trabajadores. No era razonable que el nivel de exigencia fuera idéntico al de las grandes corporaciones, teniendo en cuenta que tampoco es semejante el nivel de riesgo. Además, la protección de la libertad de empresa, especialmente para favorecer la iniciativa empresarial en un contexto de crisis económica, es una finalidad legítima que puede justificar excepciones al derecho a la protección de datos personales[133].

---

nuevas normas de privacidad anunciadas porque no cumplen la legislación europea de protección de datos, recordando, en línea con la propuesta de Reglamento, que las Compañías internacionales que ofrecen sus servicios a los consumidores de la UE deben respetar las normas europeas de protección de datos. También las autoridades de control de privacidad de Asia-Pacífico –en concreto su Grupo de Trabajo Tecnológico TWG–, han remitido un escrito a *Google* en el que manifiestan su preocupación por sus cambios en la política de privacidad y, en concreto, si se podrá combinar información suministrada por usuarios registrados en un servicio (como Gmail, YouTube o el motor de búsqueda de Google) con información de otros servicios, señalando también la falta de plazos para la eliminación de la información cuando ha sido solicitada por el interesado.

133. La propuesta de Reglamento también faculta a la Comisión para adoptar actos delegados relativos a las condiciones para los mecanismos de verificación y auditoría y el

La propuesta de Reglamento introduce como obligación del responsable y del encargado realizar con carácter previo una evaluación de impacto relativa a la protección de datos –los *Privacy Impact Assessment* (PIA) –arts. 33–[134], cuando los tratamientos entrañen riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance o fines[135]. Incluso se

criterio de proporcionalidad, considerando incluso la adopción de mecanismos específicos para las microempresas y las pequeñas y medianas empresas, una previsión acertada ya que muchas infracciones a la normativa de protección de datos se han producido tradicionalmente por las dificultades que tienen las pymes para su pleno cumplimiento. Así, por ejemplo, el Considerando 102 incide en la importancia de que las autoridades de control desarrollen actividades de sensibilización con microempresas. En todo caso, la preocupación porque la protección de datos personales no suponga una dificultad añadida para las pequeñas y medianas empresas sigue siendo una preocupación en el sector y es un reto que tiene ante sí la Comisión. El concepto de microempresas, pequeñas y medianas empresas se encuentra en la Recomendación 2003/361/CE, de 6.5.2003.

134. Este informe de evaluación debe contener la descripción general del tratamiento, los riesgos para los derechos y libertades de los interesados y las medidas contempladas para hacer frente a los riesgos y para garantizar el cumplimiento de la normativa y el respeto de los derechos e intereses legítimos de las personas afectadas. Se prevé que el responsable tenga en cuenta la opinión de los interesados o de sus representantes, sin perjuicio de la protección de los intereses públicos o comerciales o de la seguridad de las operaciones del tratamiento. La Exposición de Motivos contiene una interesante simplificación, permitiendo que la evaluación de impacto abarque a más de un único proyecto, por ejemplo, en caso de que las autoridades u organismos públicos tengan la intención de crear una aplicación o plataforma común de tratamiento o de que varios responsables se planteen introducir una aplicación o un entorno de tratamiento común en un sector o segmento de la industria o para una actividad horizontal de uso generalizado –Considerando 72–.

135. Se entienden que entrañan riesgos: la evaluación sistemática y exhaustiva de los aspectos personales propios de una persona física o destinada a analizar o a predecir su situación económica, localización, estado de salud, preferencias personales, fiabilidad o comportamiento y sobre la cual se tomen medidas que produzcan efectos jurídicos que afecten significativamente a dicha persona; los tratamientos a gran escala de datos de salud, raza, vida sexual o destinados a la prestación de la atención sanitaria, investigación epidemiológica, estudios de enfermedades mentales o infeccionas, cuando estos datos sean tratados con el fin de tomar medidas o decisiones sobre personas concretas; el seguimiento de zonas de acceso público, en particular la video-vigilancia a gran escala, los tratamientos a gran escala de datos de niños, de datos genéticos o de datos biométricos. Por tanto, la protección específica a través de esta evaluación de impacto no se realiza únicamente sobre datos especialmente protegidos –como los datos de salud o los datos genéticos– sino también sobre datos identificativos –como los derivados de la video-vigilancia o los datos biométricos– cuando son tratamientos a gran escala. Hay que señalar que en nuestro país, los tratamientos de datos personales derivados de la video-vigilancia en lugares públicos sólo pueden realizarse por las Fuerzas y Cuerpos de Seguridad, con autorización previa de la Comisión de Videovigilancia. La Agencia de Protección de Datos de la Comunidad de Madrid obliga, con anterioridad al tratamiento, a que el responsable presente un informe de proporcionalidad, que justifique la racionalidad, la necesidad y la proporcionalidad en sentido estricto de la medida. Esta exigencia se aplicaba, entre otros, a los tratamientos de datos en el ámbito de la video-vigilancia –en virtud de la Instrucción 1/2007– y a los tratamientos de datos biométricos–. Los datos biométricos son empleados para el control de acceso y de presencia de empleados públicos o de trabajadores, para la identifi-

establece la necesidad de que el responsable o el encargado obtenga con carácter previo al tratamiento de estos datos –art. 34– una autorización de la autoridad de control –o lleve a cabo una consulta– cuando el tratamiento pueda suponer riesgos para los interesados–[136], una previsión que se contenía en el art. 20 de la Directiva 95/46/CE. Como es sabido, en nuestro país sólo estaba previsto el procedimiento de autorización para algunas transferencias internacionales de datos, para la conservación de datos para fines históricos, estadísticos o científicos o para exención del deber de información al interesado –arts. 70 y 155-158 RPDP–.

La propuesta de Reglamento incluye dentro de las obligaciones del Responsable y del encargado la designación de un delegado de protección de datos –art. 35-37–[137]. Hay que señalar que la Directiva 95/46/CE ya contemplaba la figura del *Data Protection Officer*[138], un encargado de protección de datos –no

cación personal en pasaportes y documentos de identidad, e, incluso, se ha planteado su uso para el control de asistencia a cursos de formación en el ámbito público. Los datos biométricos son datos identificativos, no de salud, si bien, en todo caso, deben respetar el principio de calidad y de proporcionalidad. No obstante, en los países de la antigua Europa del Este los datos biométricos –como la huella dactilar– son considerados especialmente protegidos por su uso policial en el pasado. Esta cuestión la hemos analizado en *La protección de datos personales*, cit. pp. 216-244. Cfr. el Documento de Trabajo sobre biometría HTTP://EC.EUROPA.EU/JUSTICE/POLICIES/PRIVACY/DOCS/WPDOCS/2003/WP80_ES.PDF

136. El art. 34.2.b) permite a las autoridades de control la determinación de los tratamientos que son objeto de consulta previa, lo que introduce, de nuevo, un ámbito importante de divergencia en el régimen jurídico de protección de datos personales en los diferentes Estados miembros, afectando a la seguridad jurídica de los responsables y de los interesados y al funcionamiento del mercado interior, y que no se resuelve con la comunicación por parte de las autoridades de control al Consejo Europeo de Protección de Datos, de las listas de operaciones de tratamiento que requieren consulta previa –art. 34.4–.

137. La Confederación de Organizaciones Europeas de Protección de Datos (CEDPO), cuyo objetivo principal es promover el papel del delegado de protección de datos (DPO), ha elaborado un interesante informe sobre la propuesta de Reglamento –principalmente centrado en la importancia de esta figura–, en cuya elaboración ha participado la Asociación Profesional Española de Privacidad, teniendo una intervención destacada su Presidente Ricard Martínez –cfr. el documento original en *http://bit.ly/HeeUpi*–. De hecho. R. Martínez participó en la elaboración de la Resolución de Madrid de Estándares Internacionales, de 2009, donde ya se reconoce el importante papel de los DPO. Es interesante resaltar que las previsiones que se incluyen en la propuesta de Reglamento sobre la posición del delegado de protección de datos «cumple con las expectativas de CEDPO» –el documento llega a decir que «el reconocimiento del DPO en el artículo 35 a 37 de la propuesta es «muy bienvenida»–. El documento cita la experiencia positiva de Alemania con el DPO en los últimos 30 años, siendo cada vez más aceptados por Estados miembros como Francia y los Países Bajos. También refiere un estudio independiente encargado por el Ministerio de Justicia holandés que señaló que las organizaciones que han nombrado un DPO tienen un mayor grado de concienciación en la observancia de la legislación.

138. Un buen estudio sobre esta figura en la Directiva se encuentra en SANTAMARÍA RAMOS, F. J., *El encargado independiente. Figura clave para un nuevo derecho de protección de datos*, La Ley, Madrid, 2011, pp. 377-441. La LOPD no regula la figura del delegado de protección de datos. Únicamente el RPDP establece la necesidad de designar un

confundir con el encargado del tratamiento– que tenia la función de aplicar de manera independiente la normativa en el ámbito interno del responsable. Sin embargo, la creación de esta figura era en la Directiva una opción del responsable –no una obligación– y su regulación se encontraba en el precepto dedicado a la notificación de los tratamientos a la autoridad de control –art. 8.2–. De hecho, su función era llevar a cabo un registro de los tratamientos efectuados por el responsable, exceptuando así la obligación de notificación a la autoridad de control. La propuesta de Reglamento considera una obligación del responsable y del encargado la designación de un delegado de protección de datos cuando el tratamiento sea llevado a cabo por una autoridad u organismo público[139], o se realice en empresas de doscientos cincuenta trabajadores o más[140],

responsable de seguridad para los ficheros y tratamientos que tengan que implantar medidas de seguridad de niveles medio y alto –art. 95–. Sin embargo, tanto el *Primer Informe sobre la aplicación de la Directiva*, cit. como el Informe del Grupo de Trabajo del Artículo 29, sobre la obligación de notificación a la autoridad de control, de 18 de enero de 2005 (WP 106), ya recomendaron la designación de DPOs dentro de un mayor recurso a las excepciones previstas en la Directiva para alcanzar una mayor simplificación.

139. El delegado de protección de datos no tiene que ser necesariamente distinto para cada tratamiento sino que es una designación por el responsable o el encargado que puede ser también para todos sus tratamientos. Así, la propuesta de Reglamento señala que el delegado en el caso de los organismos públicos podrá ser designado para varias de sus entidades, teniendo en cuenta su estructura organizativa. Hay que valorar que las Administraciones Públicas no tienen un único responsable de tratamientos sino que frecuentemente disponen de un gran número de responsables, algo que depende de las competencias administrativas y que suele estar descentralizado, existiendo en este punto un amplio margen de discrecionalidad para tomar decisiones de oportunidad organizativa. Los criterios significativos para la identificación de los ficheros y tratamientos son habitualmente los que se refieren a la finalidad y a los usos previstos –valorando también los colectivos de los que se pretende obtener los datos y la tipología de datos– y la noción del responsable. En todo caso, la delimitación de los tratamientos –también necesaria para las obligaciones de documentación que sustituye a la obligación de notificación– tiene que ser configurada como algo que sirva para facilitar el control de la información personal. Hemos analizado en otro momento la conveniencia de un modelo centralizado o descentralizado en la declaración de los ficheros por las Administraciones Públicas –cfr. *La protección de datos personales*, cit. pp. 292-315–. Así, podrá existir un solo delegado de protección de datos por cada Comunidad Autónoma o por cada Ayuntamiento –sin perjuicio de que estos tengan interlocutores en los distintos organismos o centros– o establecer delegados de protección de datos por Ministerios, Consejerías o por Concejalías –o incluso por centros en el caso sanitario o de servicios sociales–. En todo caso, parece que la intención de la propuesta de Reglamento es ir hacia un delegado único de protección de datos por cada entidad. Así, se explica la previsión de un delegado de protección de datos único para grupos de empresas. No obstante, una conclusión distinta se obtiene de la posibilidad de que el delegado ejerza otras funciones profesionales dentro de la entidad. A nuestro juicio, el hecho de que el delegado de protección de datos pueda dedicarse a otras funciones o incluso pueda ser externo trata de evitar que esta figura suponga una nueva carga económica dentro de la empresa

140. Llama la atención que la propuesta de Reglamento establezca la obligatoriedad de un delegado de protección de datos en función del tamaño de la empresa –del número de empleados– y no directamente de la tipología del tratamiento, de la clase de datos –menores, datos de salud, biométricos, genéticos– o del nivel de riesgo. Pensemos en

o cuando la actividad principal del responsable o del encargado consista en operaciones de tratamiento que, en razón de su naturaleza, alcance o fines, requieran un seguimiento periódico y sistemático de los interesados, lo que incluiría, por ejemplo, a los centros sanitarios –o sociales– privados con menos de doscientos cincuenta trabajadores que disponen de las historias clínicas o de historias sociales de múltiples usuarios. Merece la pena mencionar expresamente que la propuesta de Reglamento trata de reforzar la independencia del delegado de protección de datos, convirtiéndolo en una suerte de autoridad independiente dentro de la Administración Pública y de la empresa, al que se le exige una capacidad profesional[141] y se le rodea de unas garantías de incompatibilidad –que no tenga que cumplir otras funciones profesionales que sean incompatibles con sus tareas de delegado y que puedan ocasionarle un conflicto de intereses– y de inamovilidad –dispone de un mandato mínimo de dos años, renovable sin límite, y sólo podrá ser cesado por incumplimiento de sus funciones–[142]. Así, se establece expresamente que el delegado de protección

---

una empresa –por ejemplo, del sector de la construcción– que tenga este número de trabajadores y cuyo único fichero sea el de gestión de personal y que debería designar en virtud de la propuesta de Reglamento un delegado de protección de datos. El documento de CEDPO también defiende que se tenga en cuenta otros criterios para determinar la obligación de establecer un DPO, como la finalidad de las operaciones de tratamiento, la naturaleza de los datos, la sensibilidad de los datos o del tratamiento o la cantidad de los datos objeto de tratamiento. Además, CEDPO señala la conveniencia de que la propuesta de Reglamento introduzca incentivos a favor de la designación de DPO cuando no sea obligatorio, haciendo hincapié en las ventajas de la designación de un DPO y subrayando su papel central para el cumplimiento de las nuevas obligaciones que la propuesta de Reglamento introduce para responsables y encargados, como las evaluaciones de impacto de protección de datos, la notificación de quiebras de seguridad, la privacidad por defecto, y la formación del personal. Así, señala que las organizaciones más pequeñas también pueden beneficiarse del nombramiento de DPO, como una ventaja competitiva y como una forma de reducción de sus riesgos.

141. La propuesta de Reglamento hace referencia a las «cualidades profesionales» y «conocimientos especializados» del delegado de protección de datos, pero no prevé un sistema de acreditación de los expertos –algo que tampoco se exigía hasta ahora en España para la realización de la auditoría externa o interna de seguridad del art. 96 RPDP– y que es una de las demandas tradicionales de las asociaciones de profesionales de la privacidad. El documento de CEDPO incide también en la importancia de la cualificación del DPO, que se centra en el buen conocimiento de la ley de protección de datos y de los estándares de tecnologías de la información, incluyendo la conveniencia de establecer un programa de certificación de DPO.

142. El documento de CEDPO critica el establecimiento de un período mínimo de designación del DPO porque podría poner en riesgo su independencia, algo que no se entiende porque la inamovilidad es tradicionalmente una garantía de independencia. Sin embargo, el documento de CEPDO sugiere la introducción de una interesante garantía adicional: que los DPOs internos dispongan de protección contra el despido injusto para garantizar su independencia. Además, destaca la importancia de que el DPO disponga de visibilidad dentro de la organización. El dictamen del Comité Económico y Social sobre la propuesta de Reglamento –DOUE, 31.0.2012– señala también la necesidad de precisar mejor la protección contra el despido, que debe definirse con claridad y extenderse más allá del periodo durante el cual la persona afectada desempeñe esta función y la liberación del DPO de toda responsabilidad cuando haya notificado las irregularidades al empleador o a la autoridad de control –apdo. 4.11– .

de datos debe desempeñar sus actividades con independencia y no recibirá ninguna instrucción, teniendo la capacidad de informar directamente a la dirección. En todo caso, si bien la propuesta del Reglamento es bienintencionada –esta figura era una de las demandas del sector, especialmente de las asociaciones de profesionales de la privacidad y de los sindicatos[143]–, no va a ser fácil que el delegado de protección de datos cumpla sus funciones con independencia cuando la propuesta de Reglamento prevé que éste sea un *empleado* del responsable o una persona con un contrato de servicios y teniendo en cuenta que los principales conflictos a los que tendrá que enfrentarse diariamente son entre los intereses de la propia empresa y los derechos de los interesados que debe proteger[144]. Por último, si bien el delegado de protección de datos tiene una función muy amplia de supervisar el cumplimiento de la normativa de protección de datos en el ámbito del responsable o del encargado –lo que incluye la información a los interesados, las obligaciones de documentación, las solicitudes de ejercicio de los derechos, los requisitos relativos a la protección de datos en el diseño, las auditorías correspondientes, la formación del personal, la evaluación de impacto, las comunicaciones y notificaciones de violaciones de datos personales, etc–, funciones todas ellas mencionadas en el art. 37–, no hay que olvidar que el delegado no es una autoridad de control sino que pertenece a la empresa o a la Administración Pública y está sometido al control de la Agencia de Protección de Datos, sin perjuicio de que ésta tenga en él un punto de contacto a los efectos de las autorizaciones, solicitudes o consultas previas[145].

143. Las organizaciones sindicales han defendido tradicionalmente la figura del DPO, pensando que sus miembros en la empresa iban a ocupar esta responsabilidad. De hecho, el dictamen del Comité Económico y Social –donde participan las organizaciones sindicales– sobre la propuesta de Reglamento defiende expresamente «el derecho de participación directa de los representantes del personal en la designación del DPO» –apdo. 4.11–. Los sindicatos son independientes –aunque no siempre– de la dirección de la empresa pero tienen, en cambio, otras dependencias. Además, la función de los sindicatos es la defensa de los derechos de los trabajadores pero los tratamientos de datos personales de las empresas exceden de los de su personal y afectan sobre todo a los derechos de los ciudadanos-clientes, en relación con los cuales las organizaciones sindicales pueden defender posiciones distintas e incluso contrapuestas.

144. La verdad es que si ya cuesta que los órganos rectores de las Administraciones independientes sean auténticamente independientes –o que los funcionarios sean independientes en la aplicación de la Ley– más difícil lo van a tener personas incardinados en la propia empresa o que presten servicio a la empresa, cobrando en ambos casos de la misma, algo que también ocurre en las funciones de auditoría. Además, hay que añadir los riesgos de captura de los DPOs por parte de sectores privados vinculados a las tecnologías de la información. La realidad es que no hay figuras auténticamente independientes en la empresa –en algunas ocasiones, se es independiente hasta que llama la dirección de la empresa–. Quiero que se me entienda bien: defiendo la figura de los delegados de protección de datos, creo que se va a implantar y que va a suponer un cierto paso adelante en la protección de datos personales; pero tampoco es bueno tener mucha confianza, esperar mucho de ellos para luego desanimarse al observar su funcionamiento práctico.

145. El documento de CEDPO recomienda la introducción de una función general del DPO: «Asesorar al responsable de datos o al encargado sobre la estrategia de protección de datos en general». Además, destaca la conveniencia de emplear la figura del DPO como un medio para la reducción de las cargas administrativas. Sin embargo, no

Otra de las obligaciones generales del responsable del tratamiento que introduce la propuesta de Reglamento es la conservación de la documentación, que viene a sustituir a la obligación de notificación prevista en los arts. 18 y 19 de la Directiva, un elemento donde existen importantes divergencias entre los Estados miembros. Como es sabido, estos preceptos flexibilizan esta obligación, ofreciendo a los Estados miembros la posibilidad de establecer excepciones a la notificación cuando el riesgo sea reducido o se designe por parte del responsable un encargado de protección de datos. La Comisión se ha lamentado de que algunos Estados –uno es el caso de España– no hayan aprovechado esta posibilidad, manteniendo la obligación de notificación de todos los ficheros. La Comisión Europea ha estado siempre comprometida con la necesidad de simplificar aún más esta obligación, recomendando la utilización más frecuente de las excepciones y, en especial, de la posibilidad prevista en el art. 18.2 de la Directiva, de designar un encargado de la protección de datos personales. La Comisión ha insistido en la necesidad de ir aproximando las exigencias de los Estados miembros respecto a la notificación de las operaciones de tratamiento por parte de los responsables ya que existen todavía muchas divergencias. La Comisión también ha incidido en las diferencias existentes en la manera en que los distintos Estados miembros han aprovechado las excepciones a las obligaciones de notificación[146]. Llama la atención que el número de inscripciones sea enormemente bajo –*astonishingly low*– en relación con el número de entidades que debían haber notificado los ficheros[147].

---

parece razonable su propuesta de que cuando hubiera designado un DPO sea conveniente reemplazar la obligación de consulta previa a la autoridad de control para operaciones de tratamiento que entrañen riesgos específicos, por una obligación de mera información por parte del DPO ya que la independencia y las funciones de DPO y de una autoridad de control no son comparables. No hay que olvidar la importancia de las herramientas de control y supervisión fuera de la empresa y el hecho de que las empresas –y los propios DPOs– están sometidos a control. No compartimos, pues, las reflexiones de SANTAMARÍA RAMOS que considera al encargado independiente como «el juez imparcial que garantiza el correcto funcionamiento del sistema», «la persona que vela de manera independiente por los derechos».

146. Cfr. *Primer informe sobre la aplicación de la Directiva*, cit.-. El documento de *Analysis and impact study on the implementation of Directive*cit.–ha hecho una descripción de la obligación de notificación y del principio de publicidad recogido en los arts. 18-21 de la Directiva. Así señala que algunos Estados miembros prevén la obligación de notificación de todos los tratamientos, incluidos aquellos mantenidos en ficheros manuales –Dinamarca, Grecia, Italia y Luxemburgo– mientras que otros lo extienden únicamente a los ficheros manuales –Finlandia y Portugal–. En relación con el contenido de las notificaciones, las leyes nacionales incluyen las materias señaladas en el art. 19. Distintos Estados miembros han hecho uso mayor o menor de la posibilidad de establecer excepciones a la obligación de notificación –este sería el caso de Austria, Bélgica, Dinamarca, Francia, Holanda, Italia, Suecia, Finlandia y Gran Bretaña–. En cambio España no ha establecido la posibilidad de establecer excepciones, ni siquiera para los tratamientos de datos personales menos intrusivos. Portugal ha exceptuado únicamente la notificación de aquellos ficheros que constituyen fuentes accesibles al público.

147. A fecha de elaboración del informe antes citado, el número más alto de notificaciones se encontraba en Francia –700.000 ficheros–. La Comisión destacaba que era semejante la cifra de ficheros declarados –250.000– en países como España o Gran Bretaña,

Pues bien, la propuesta de Reglamento ahonda más en esa línea de la simplificación de cargas administrativas ya que hace desaparecer la obligación de notificación de los responsables, sustituyéndola por una obligación de documentación de los tratamientos que asegure que estos respetan la normativa, estando la documentación a disposición de la autoridad de control[148]. Así, el responsable y el encargado –y el representante del responsable– tienen ahora la obligación de documentar y de conservar la documentación de todas las operaciones de tratamiento efectuadas bajo su responsabilidad –art. 28–, entre los que están el nombre y los datos de contacto del responsable, los fines del tratamiento –en particular los intereses legítimos perseguidos por el responsable–, una descripción de las categorías de datos, los destinatarios o categorías de destinatarios de los datos personales –lo que incluye los responsables del tratamiento a quienes se comuniquen los datos–, la información sobre las transferencias internacionales, los plazos establecidos para la supresión de los datos y los mecanismos para verificar las medidas. Como se puede observar, la mayoría de las obligaciones de documentación del responsable que se incluyen ahora formaban parte antes de los elementos necesarios para la notificación de los tratamientos a la autoridad de control, a lo que se añade otra información que trata de justificar mejor el tratamiento como la relativa a los intereses legítimos perseguidos por el responsable y al plazo de supresión de los datos. Lo que se pretende con esta nueva obligación de documentación es mantener los elementos positivos de la notificación de los tratamientos, eliminando los aspectos que algunos consideraban a primera vista como burocráticos[149], aunque lógica-

---

a pesar de que hayan tenido un diferente posicionamiento en relación con la obligación de notificación: la legislación española no admite excepciones a la obligación de notificación establecida en la Directiva, mientras que la legislación británica prevé estas excepciones. En todo caso hay que señalar el nivel muy elevado de cumplimiento de la obligación de declaración de ficheros públicos en el ámbito de responsabilidad de la Agencia de Protección de Datos de la Comunidad de Madrid, además de otros datos comparativos que justificaban su existencia y actividad –cfr. *La protección de datos personales*, cit. pp. 1800-1808.

148. Ha sido un lugar común entre nosotros calificar como burocrática la obligación de notificación de tratamientos a la autoridad de control. Sin embargo, difícilmente puede calificarse como tal un trámite que puede hacerse cumplimentando un impreso muy breve de manera electrónica, una exigencia mucho más sencilla que la que imponen otras Administraciones Públicas como la Seguridad Social o la Agencia Tributaria y que están menos vinculadas a la tutela de un derecho fundamental. La supresión de la obligación de notificación es resultado de la opción estratégica de la Comisión de reducir o simplificar las cargas administrativas para lograr los objetivos de la Agenda Digital para Europa, el Plan de Acción de Estocolmo y la Estrategia Europa 2020. Así, la evaluación del impacto que realizó la Comisión sobre la propuesta de Reglamento revisó todos los cálculos y estimaciones relativas a la carga administrativa y los costes de las notificaciones.

149. Además, la propuesta de Reglamento excluye de esta obligación de documentación a las personas físicas que traten datos sin interés comercial –sería un tratamiento excluido si fuera personal o doméstico– o a las empresas u organizaciones que emplean a menos de doscientas cincuentas personas y que traten datos personales sólo como actividad accesoria a sus actividades principales –art. 28.4–. Se trata, de nuevo, de eliminar obligaciones en aquellas empresas que cuyos tratamientos impliquen menos riesgos.

mente, esta medida afecte o suprima el principio de publicidad de los tratamientos y el derecho de consulta al registro general –art. 21 de la Directiva y art. 14 LOPD, en conexión con los arts. 20 y 25 LOPD–. Además, hay que reconocer que la notificación de los tratamientos ha sido hasta ahora para los responsables en nuestro país, el primer paso para el cumplimiento de la legislación ya que les obligaba a identificar los tratamientos y a plantearse su finalidad, que datos recaban, las medidas de seguridad a implantar, etc. De hecho, a nuestro juicio, en España hay un mayor nivel de cumplimiento de la legislación, no sólo por la actividad inspectora y sancionadora de la autoridad de control, sino por el establecimiento de un sistema de notificación de los tratamientos, sin perjuicio de que hubiera sido conveniente la acogida de algunas excepciones a esta obligación previstas en la Directiva –por ejemplo, para las pymes–. En todo caso, aunque la desaparición de la obligación de notificación es aplicable también a los tratamientos de datos personales que lleven a cabo las Administraciones Públicas, hay que recordar que estos tratamientos –que, además, se hacen sin el consentimiento del interesado– tienen que estar previstos en una norma –en una disposición de carácter general–, una exigencia del principio de legalidad administrativa, que obliga a todos los poderes públicos a actuar siempre *positive bindung*, vinculados positivamente al derecho[150].

Otra de las obligaciones del responsable es la implementación de los requisitos en materia de seguridad. Existían también discrepancias en lo relativo a la plasmación práctica de la seguridad de los tratamientos de datos personales. La mayoría de los Estados habían optado por una formulación similar a la prevista en el art. 17 de la Directiva, que impone a los responsables la obligación de aplicar medidas técnicas y organizativas adecuadas para la protección de los datos de carácter personal, garantizando un nivel de seguridad adecuado en relación a los riesgos que presente el tratamiento y la naturaleza de los datos –teniendo en cuenta los conocimientos técnicos existentes y el coste de su aplicación–, pero sin establecer unas concretas medidas de seguridad. En cambio, como destacaba la Comisión, España aprobó una regulación que con gran nivel de detalle establece las medidas de seguridad técnicas y organizativas que deben ser implantadas dependiendo del nivel de riesgo[151]. La propuesta de Reglamento, siguiendo en este punto la regulación española –y a diferencia de la Directiva 95/46/CE– opta por supeditar el respeto al principio de seguridad por

150. No será necesario aprobar una disposición de carácter general cuando el tratamiento de datos está previsto en una norma –por ejemplo, el padrón municipal que se encuentra regulado en el art. 16 LBRL–. En cambio, cuando no existe norma que habilite el tratamiento de datos personales, la aprobación de la norma siempre es preceptiva aunque se exceptúe la obligación de notificación.

151. Nos referimos al RD 994/1999, de 11 de junio, que aprobó el Reglamento de Medidas de Seguridad de los Ficheros automatizados que contengan Datos de Carácter Personal, ya derogado por el RPDP que establece medidas de seguridad tanto para los tratamientos automatizados como para los ficheros y tratamientos no automatizados –Título VIII, arts. 79-114–. Holanda también ha aprobado unas medidas de seguridad que no son vinculantes para los responsables de ficheros aunque es usado como un importante elemento de autorregulación.

parte del responsable con la implantación de medidas concretas. El principio de seguridad no puede considerarse una obligación de resultado porque la seguridad absoluta no existe. Por ello, la vulneración del principio de seguridad por parte del responsable tiene que vincularse al incumplimiento de unas concretas medidas de seguridad aprobadas previamente, lo que permite la declaración de infracción, facilitando y objetivando la actividad de la autoridad de control[152]. Hay que señalar que la propuesta de Reglamento no regula la seguridad de los datos entre los principios de protección de datos sino entre las obligaciones del responsable y también del encargado del tratamiento, con independencia del contrato suscrito con el responsable del tratamiento –art. 30–. Una de las novedades es la necesidad de realizar una evaluación de riegos, que permita adoptar medidas para proteger los datos contra su destrucción accidental o ilícita, pérdida accidental o cualquier tratamiento ilícito como la comunicación, difusión, el acceso no autorizado o la alteración de los datos personales. Existe una preocupación específica no sólo por impedir cualquier acceso no autorizado sino también por evitar cualquier forma no autorizada de comunicación, lectura o copia. La propuesta de Reglamento no incluye una referencia a niveles de seguridad ni tampoco un conjunto de medidas de seguridad a implementar sino que, al igual que el art. 9 LOPD que prevé su desarrollo reglamentario, y a diferencia de la Directiva, faculta a la Comisión para realizar los actos normativos necesarios para especificar las medidas técnicas y organizativas, lo que incluye la referencia a sectores específicos y situaciones de tratamiento de datos específicas, teniendo en cuenta no sólo la evolución de la tecnología, sino también las soluciones de privacidad desde el diseño y la protección de datos por defecto. Entre las novedades que se presentan en la regulación de la seguridad de los datos se encuentra la notificación de la violación de los datos personales a la autoridad de control[153] y su comunicación al interesado[154] –arts. 31-32–.

152. La Resolución de infracción que la APDCM declaró a la Consejería de Sanidad de la Comunidad de Madrid por vulneración del principio de seguridad, ocasionado por la filtración de las historias clínicas del Hospital Severo Ochoa de Leganés a medios de comunicación y a asociaciones de pacientes, se fundamentó en que no estaba en funcionamiento el registro de accesos, una medida de seguridad establecida en la normativa que facilita la trazabilidad de las personas que acceden a las historias clínicas.

153. La violación de datos personales debe notificarse a la autoridad de control sin demora injustificada y, de ser posible, a más tardar veinticuatro horas después de que se haya tenido constancia de ella. Esta notificación deberá describir la naturaleza de la violación de los datos personales –las categorías y el número de interesados–, las consecuencias de la violación, las medidas adoptadas para atenuar sus efectos negativos y para poner remedio a la violación de datos personales. El responsable está, además, obligado a documentar estas brechas de seguridad.

154. La propuesta de Reglamento regula también la obligación de comunicación de la violación de datos personales al interesado cuando sea probable que ésta afecte negativamente a la protección de sus datos personales o a la privacidad del interesado, salvo que el responsable demuestre, a satisfacción de la autoridad de control, que ha implementado medidas de protección tecnológica que hagan ininteligibles los datos para cualquier persona no autorizada. Si el responsable no hubiera comunicado la violación al interesado, la autoridad de control, una vez considerados los efectos negativos probables de la violación, podrá exigirle que lo haga. Esta comunicación inmediata de la

De hecho, entre las definiciones novedosas que incluye la propuesta del Reglamento –y que no estaban ni en la Directiva, ni en la LOPD ni en el RPDP– está la de violación de datos personales, más conocida por brechas de seguridad –las llamadas *«BCRs»*[155]. Hay que señalar que la Directiva de 2009/136/CE, por la que se modifica la Directiva 2002/58/CE relativa al tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas, incorpora a ésta un art. 2.h) sobre el concepto de violación de datos personales y añade un apartado 4.3, estableciendo la obligación del proveedor de servicios de comunicaciones electrónicas de notificar la violación de datos personales sin dilaciones indebidas tanto a la autoridad de control como a los abonados o particulares, una cuestión que la Comisión Europea había pretendido extender a otras áreas como los servicios financieros.

La propuesta de Reglamento también regula expresamente la figura del encargado del tratamiento –art. 26–, que no estaba bien resuelta en la Directiva –que únicamente definía al encargado en el art. 2.e) y lo regulaba en el art. 17 en relación con la seguridad de los tratamientos–, pero sí en la LOPD –art. 12– y especialmente, en el RPDP, que establece un auténtico estatuto del encargado del tratamiento –arts. 20-22–, por lo que la regulación prevista en la propuesta de Reglamento supone un avance a nivel europeo pero no aporta grandes novedades en nuestro país[156]. Destaca que hay que elegir un encargado que ofrezca garantías suficientes para implementar las medidas apropiadas –existe una responsabilidad *in eligendo*, a la que ya hacía mención la Directiva en relación con la seguridad-, que el encargado empleará únicamente a personal que se haya comprometido a respetar la confidencialidad o esté sujeto a una obligación legal de confidencialidad, que el encargado tiene la posibilidad de ayudar al responsable a garantizar el cumplimiento de sus obligaciones y que la relación entre el responsable y el encargado se documentará por escrito, debiendo constar las instrucciones del responsable y las obligaciones del encargado[157].

---

violación de datos personales tanto al interesado como a la autoridad de control están justificadas en que esta puede causar, si no adoptan medidas rápidas y adecuadas, pérdidas económicas sustanciales y perjuicios sociales al interesado, incluida la usurpación de su identidad, por lo que los interesados deben ser informados par adoptar las cautelas necesarias. El Considerando 67 señala que la violación afecta negativamente a los datos personales o la intimidad de los interesados cuando conlleva, por ejemplo, fraude o usurpación de identidad, daños físicos, humillación grave o perjuicio para su reputación. La notificación debe describir la naturaleza de la violación de los datos personales y las recomendaciones para que la persona afectada mitigue sus potenciales efectos adversos.

155. Así, se define violación de datos personales como toda violación de la seguridad que ocasione la destrucción accidental o ilícita, la pérdida, alteración, comunicación no autorizada o el acceso a datos personales transmitidos, conservados o tratados de otra forma –art. 4.9–.

156. Así, la previsión de que todo encargado que trate los datos más allá de las instrucciones del responsable del tratamiento ha de ser considerando corresponsable se encontraba ya en el art. 12.4 LOPD.

157. Se echa en falta en la propuesta de Reglamento una regulación más precisa de la computación en nube, una relación jurídica que podría encuadrarse como encargo del tratamiento y donde hay cuestiones a tener en cuenta como los sucesivos encargos

C) Los principios: la licitud de los tratamientos y las categorías especiales de datos.

La regulación que la propuesta de Reglamento hace de los principios relativos al tratamiento de datos personales y que se desarrolla en el Capítulo II –arts. 5-10– no aporta una especial novedad. El Considerando 7 de la Propuesta de Reglamento, recogiendo el parecer de las consultas previas a las partes interesadas, señala que los principios generales de la Directiva 95/46/CE «siguen siendo válidos y actuales», algo que también se puede extender a sus objetivos –como señalamos anteriormente– y a su neutralidad tecnológica; lo que se trata ahora es de alcanzar una correcta implementación de los principios que asegure un nivel de protección de datos personales equivalente en todos los Estados miembros. Así, la mayoría de los Estados miembros han transpuesto de manera similar y con pocas variaciones el art. 6 de la Directiva relativo al principio de finalidad[158] y al principio de calidad[159]. La propuesta de Reglamento únicamente introduce el principio de transparencia –que los datos serán tratados de manera transparente en relación con el interesado del art. 5.a)–, lo que tiene consecuencias, como señalaremos más adelante, en relación con la información y el derecho de acceso–; precisa el principio de prohibición de exceso materializándolo en un principio de minimización de datos –en términos de la Comisión–, que obliga en el art. 5.c) a que «los datos sean limitados al mínimo necesario en relación a los fines para los que se traten» y «sólo se tratarán si y siempre que estos fines no pudieran alcanzarse mediante el tratamiento de información que no implique datos personales»[160]; y establece que el responsable del tratamiento de datos, «para cada operación de tratamiento, garantizará

---

de tratamiento que difícilmente son autorizados previamente por el responsable del tratamiento –una exigencia que se mantiene en el art. 26.2.d) de la Propuesta de Reglamento–, además de las implicaciones que tiene el *cloud computing* en relación a la Ley aplicable –que es la Ley nacional del responsable del tratamiento o del cliente– o a las transferencias internacionales de datos. La computación en nube ha supuesto una revolución pero no ha cambiado los conceptos básicos; el fundamental es que los datos siempre están almacenados en algún sitio físico –aunque no se aplique la ley del lugar de almacenamiento de la información–. Cfr. sobre la cuestión el Dictamen 196, de 1 de julio de 2012, del Grupo de Trabajo del Art. 29 sobre la computación en nube.

158. La Carta de los Derechos Fundamentales de la Unión Europea señala que «los datos se tratarán de modelo leal y *para fines concretos*» –art. 8.2–, algo que siempre ha supuesto problemas en el ámbito del antiguo tercer pilar.

159. Las principales diferencias se producían entre la Directiva y la anterior Ley Francesa que solamente prohibía la recogida de datos desleal o ilícita y preveía que la información se mantendrá personalizada –sin disociar– sólo el tiempo necesario para cumplir la finalidad para la cual los datos han sido recabados. Además, el art. 6.1.b) de la Directiva permite el tratamiento posterior con fines históricos, estadísticos o científicos, siempre y cuando se establezcan las garantías oportunas. Sin embargo, los Estados, si bien han autorizado este tratamiento, no han establecido las garantías adecuadas, algo que finalmente se incorporó al RPDP –arts. 157-158–. Cfr. el documento de trabajo encargado por la Comisión *Analysis and impact study on the implementation of Directive*, cit..

160. Cfr. nuestro trabajo «El principio de calidad de los datos», *loc. cit.* pp. 340-394.

y demostrará el cumplimiento de las disposiciones del presente Reglamento» –art. 5.f)–, es decir, transforma las obligaciones del responsable del Capítulo IV en un principio general de responsabilidad –uno de los conceptos que más se reiteran en el texto es el de la *accountability*– que le obliga, entre otras cosas, a documentar el cumplimiento de los principios y derechos en los tratamientos de datos personales[161]. Se mantienen en el art. 6 de la propuesta de Reglamento las condiciones de licitud de los tratamientos del art. 7 de la Directiva[162], que, a diferencia del Convenio 108, ya contenía una lista exhaustiva y taxativa de supuestos de legitimidad para el tratamiento de datos personales distintos del consentimiento del interesado[163]. Así, los tratamientos de datos personales se reputan legítimos si existe consentimiento, relación contractual, obligación jurídica del Derecho de la Unión o de la legislación del Estado, cumplimiento de una misión de interés público o inherente al ejercicio de poder público o satisfacción del interés legítimo perseguido por el responsable, siempre que no prevalezca el interés o los derechos y libertades del interesado. Un aspecto importante de la propuesta de Reglamento es que trata de clarificar la regla del consentimiento como criterio de licitud de los tratamientos. No se encontraba claramente diferenciado en la Directiva 95/46/CE el concepto de «consentimiento inequívoco» –art. 7.a)– o el concepto de «consentimiento explícito» –art. 8.2.a)–. A juicio de la Comisión, era necesaria una interpretación clara y uniforme del consentimiento válido en toda la Unión Europea que dé seguridad jurídica a los agentes económicos. Por ello, se establecen ahora algunos rasgos nuevos en relación con el consentimiento, que ya estaban señalados por la doctrina y la jurisprudencia: que la carga de la prueba del consentimiento la tiene el responsable del tratamiento, que el consentimiento para el tratamiento debe ser distinguido de cualquier otra dación de consentimiento para otro asunto y que el consentimiento no es una base jurídica válida cuando existe un desequilibrio entre el interesado y el responsable del tratamiento[164]. Sin embargo, el

161. Dentro de los principios se establece como novedad que el responsable del tratamiento no está obligado a obtener información adicional para identificar al interesado con la única finalidad de cumplir las disposiciones del Reglamento –art. 10–.

162. La Exposición de Motivos de la propuesta de Reglamento señala que los criterios del art. 6 de la Directiva se especifican más en profundidad, por lo que respecta al criterio del interés legítimo del responsable y la observancia de las obligaciones jurídicas y del interés público. Esta cuestión la analizamos *supra* apdo. IV.B) y C).

163. La Comisión entendía que algunos Estados miembros habían ido demasiado lejos o se han quedado cortos respecto a la lista de motivos de tratamiento legítimo que figura en el artículo 7 de la Directiva 95/46/CE.

164. Este es un concepto jurídico indeterminado que puede tener importantes consecuencias prácticas. Se trata, como señala la Exposición de Motivos, de aclarar las condiciones para que el consentimiento sea válido como fundamento jurídico del tratamiento lícito. Como hemos dicho en otro momento, el consentimiento no lo es todo –por eso no es plenamente adecuada la expresión derecho a la autodeterminación informativa– sino que se debe respetar el resto de los principios de protección de datos personales, en especial el principio de calidad, en supuestos donde hay una excepción del consentimiento –por ejemplo, en los tratamientos que llevan a cabo las Administraciones Públicas–, o donde, como en este caso, existe una relación negocial donde prevalece la posición de una de las partes –relación laboral o contratos de adhesión–. Hay que señalar que el art. 82 de la propuesta de Reglamento habilita a los Estados miembros

cambio más relevante en la licitud de los tratamientos no se encuentra en el Capítulo II –Principios– sino en el Capítulo I –Disposiciones Generales–, y más concretamente en las definiciones, donde desaparece la legitimidad del consentimiento tácito. La Comisaria Viviane Reding ha manifestado recientemente que «permanecer en silencio no es consentimiento». El consentimiento es para la propuesta de Reglamento toda manifestación de voluntad no sólo libre, específica, informada sino también *explícita*[165], «mediante la que el interesado acepta, ya sea mediante una declaración, ya sea mediante una clara acción afirmativa, el tratamiento de datos personales que le conciernen»[166]. Lo que exige la propuesta de Reglamento es que exista una acción afirmativa del interesado, que puede darse de muchas maneras[167]. Posiblemente, la mejora de las tecnologías de la comunicación ha facilitado la posibilidad de exigir el consentimiento explícito, algo que en el pasado podía ralentizar la relación jurídica en Internet[168].

---

a adoptar por Ley normas específicas que rijan el tratamiento de datos personales de los trabajadores en el ámbito laboral, en cuestiones como la contratación de personal, la ejecución del contrato laboral y el cumplimiento de las obligaciones.

165. Como señala la Exposición de Motivos de la propuesta de Reglamento, el consentimiento se debe dar «de forma explícita por cualquier medio apropiado que permita la manifestación libre, específica e informada de la voluntad del interesado, ya sea mediante una declaración o una clara acción afirmativa del interesado, que garantice que la persona es consciente de que está dando su consentimiento al tratamiento de datos personales, incluso mediante la selección de una casilla de un sitio web en internet o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo fin o fines. Si el consentimiento del interesado se ha de dar a raíz de una solicitud electrónica, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta» –Considerando 25–.

166. Se trata, como señala la Exposición de Motivos, de «dotarse de una definición única y coherente que garantice que el interesado es consciente de que da su consentimiento y a qué lo da». De esta forma, la propuesta de Reglamento es más garantista que la Carta de los Derechos fundamentales de la Unión Europea que sólo señala que los datos se tratarán «sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por ley» –art. 8.2–. Se entendía que este consentimiento debía de prestarse de forma inequívoca. –cfr. MARTÍN Y PÉREZ DE NANCLARES, J., *loc. cit*. p. 235–. Esto estaba en línea con la Directiva que consideraba únicamente como rasgos esenciales del consentimiento que fuera libre, específico, informado –art. 2.h)– e inequívoco –art. 7.a)–, En cambio, el consentimiento expreso o explicito se requería únicamente para el tratamiento de categorías especiales de datos –art. 8.2.a) de la Directiva y art. 7 LOPD–. En todo caso, la expresión «inequícovo» –*unambiguous*– era en el fondo algo bastante parecido a explícito. La validez del consentimiento tácito fue admitida tempranamente por la AEPD. *http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2000-0000_Caracteres-del-consentimiento-definido-por-la-LOPD.pdf*

167. Por ejemplo, si la página web utiliza *cookies*, bastaría que se advirtiera en el comienzo de la navegación, de forma que si el usuario sigue navegando en la web, estaría llevando a cabo la acción afirmativa.

168. Llama la atención que la última propuesta de la Industria, en concreto de *Microsoft* –evento de *Seattle*, de septiembre de 2012–, insiste en que la protección de datos no debe pivotar sobre el principio de consentimiento sino sobre el principio de finalidad.

La existencia de este consentimiento explicito no supone un problema para la generalidad de los tratamientos de la industria –si no existiera, en ocasiones, una voluntad de manipularlo–. Además, el consentimiento no es la única base jurídica que justifica la licitud de los tratamientos. Persisten otros supuestos de legitimación de los tratamientos –la satisfacción de un interés legítimo perseguido por el responsable, la ejecución de un contrato–. De lo que se trata es que cuando se pretenda que la base jurídica de la licitud del tratamiento sea el consentimiento, este se esté prestando realmente y que no genere dudas.

La propuesta de Reglamento también contiene una regulación específica de las categorías especiales de datos, tanto en lo que hace referencia al principio general de prohibición de tratamiento como a los supuestos donde existe un interés legítimo del responsable que justifica su tratamiento sin consentimiento del interesado[169]. Mención específica merece la referencia al ámbito de la salud. La propuesta de Reglamento es bastante sucinta en el art. 9.2.h) ya que se limita considerar que no están prohibidos los tratamientos de datos de salud cuando sean necesarios a efectos sanitarios, llevando la regulación sustancial al art. 81 –«Tratamiento de datos personales relativos a la salud»– dentro de las Disposiciones relativas a situaciones de tratamiento de datos específicas[170]. La pro-

---

Sin embargo, existe una preocupación de las autoridades de control porque la recogida y el tratamiento de datos personales para finalidad de *marketing* se hagan con el consentimiento del interesado. La Comisión quiere que los clientes estén informados de cómo se está controlando su uso de Internet para dirigirles publicidad. Así, los usuarios deben saber cuándo los comercios on-line' usan las páginas web consultadas con anterioridad como base para hacer sugerencias de productos. La importancia del consentimiento para la finalidad de *marketing* es una cuestión sobre la que ya se ha pronunciado el Grupo de Trabajo del Artículo 29, en sus Dictámenes 5/2004, sobre comunicaciones de venta directa no solicitada y 15/2011, sobre la definición del consentimiento. Cfr. estos documentos en *http://ec.europa.eu/justice/policies/privacy/docs* Además, hay que señalar, como veremos después, que la propuesta de Reglamento ha reconocido un derecho de oposición al tratamiento de datos destinados a mercadotecnia directa –art. 19.2–.

169. También señala la propuesta de Reglamento en otros apartados que los tratamientos de categorías especiales de datos requieren una evaluación de impacto relativa a la protección de datos –art. 33– y que estos datos no pueden servir para evaluar determinados aspectos de la personalidad –art. 20–. El Ministerio de Justicia de España quiere introducir una enmienda para permitir la cesión de datos a terceros sin consentimiento para averiguar la filiación natural, tras la polémica por el caso de los bebes robados. En todo caso, la propuesta de Reglamento ya prevé el tratamiento si es necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, si bien, habrá que hacerlo a través del órgano judicial –como en la actualidad prevé el art. 11.2.d) de la LOPD–.

170. Este precepto es esencialmente coincidente con el art. 8.3 de la Directiva, al igual que con el art. 7.6 LOPD, al referirse a los tratamientos de categorías especiales de datos cuando sean necesarios para la prevención –la propuesta de Reglamento añade la medicina del trabajo, una precisión posiblemente innecesaria ya que se encuentra subsumida en las demás– o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. La propuesta de Reglamento extiende la previsión a los tratamientos de datos relativos a

puesta de Reglamento contiene al principio una definición más vaga de datos relativos a la salud, que incluye no sólo cualquier información que se refiera a la salud física o mental de una persona, sino también la asistencia prestada por los servicios de salud a una persona[171]. En cambio, separa los datos genéticos

la salud por razones de interés público en el ámbito de la salud pública, como la protección contra riesgos sanitarios transfronterizos graves, o para garantizar altos niveles de calidad y seguridad de los medicamentos o del material sanitario –una precisión interesante, aunque estos tratamientos estuvieran encuadrados en la prevención del art. 8.3 de la Directiva y en la transferencia internacional para la salvaguarda de un interés vital del art. 26,1,e) de la Directiva–. También se incluyen los tratamientos por otras razones de interés público en ámbitos como la protección social, especialmente a fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad –cfr. también el Considerando 42 de la propuesta de Reglamento, que también estaba en el Considerando 34 de la Directiva–. Esta actividad se ha encuadrado hasta ahora en la referencia a la gestión de los servicios sanitarios –si se trata del pago del coste de la asistencia– o en habilitaciones legales específicas, como los arts. 18 y 103-105 de la Ley 15/1980, de 8 de octubre, de Contrato de Seguro, el Real Decreto Legislativo 1/1994, de 20 de junio, por el que se aprueba el Texto Refundido de la Ley General de la Seguridad Social o los arts. 139 y ss de la LRJAP y PAC, para la responsabilidad patrimonial de las Administraciones Públicas. Cfr. también el Considerando 122, en relación con el tratamiento de datos para la asistencia sanitaria, la necesidad de unas condiciones armonizadas que protejan los derechos de las personas físicas, también el derecho de acceso a la historia clínica, y el Considerando 123 en relación con los tratamientos de datos sin consentimiento para la salud pública y para garantizar la sostenibilidad de la asistencia sanitaria universal. En todo caso, la propuesta de Reglamento no autoriza la aplicación de la excepción sanitaria a todas las categorías especiales de datos, como, por razones –aparentemente– de mala técnica legislativa, sí se encontraba tanto en el art. 8.3 de la Directiva como en el art. 7.6 LOPD. Además, hay que señalar que el art. 81 exige para el tratamiento de datos de salud a efectos sanitarios, no sólo que sea para el cumplimiento de los fines antes descritos sino que este tratamiento se realice sobre la base del Derecho de la Unión o de los Estados miembros, que deberá establecer las disposiciones específicas adecuadas para salvaguardar los legítimos intereses del interesado. Es decir, es necesario, además, una habilitación legal específica, algo no previsto en el art. 8 de la Directiva ni en el art. 7.6 LOPD. Existen en nuestro país distintas habilitaciones legales a estos efectos –la Ley 41/2002, de 14 de noviembre, de autonomía del paciente o la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud, aunque es razonable que esta previsión de la propuesta de Reglamento apoye la tesis de quienes defienden una ley de protección de datos en el ámbito sanitario. Por último, hay que señalar que el art. 81 de la propuesta de Reglamento separa los tratamientos de datos de salud para la investigación sanitaria –como el establecimiento de registros de pacientes con el fin de mejorar el diagnóstico, distinguir entre tipos de enfermedades similares y preparar estudios para terapias– de aquellos tratamientos para la prevención, la asistencia y la gestión de servicios sanitarios, situando los tratamientos para la investigación sanitaria dentro de los tratamientos para fines de investigación histórica, estadística y científica regulados en el art. 83 y sometiéndolos a los mismos criterios –cfr. *supra* nota 237–.

171. De esta forma sería dato relativo a la salud la información referida al pago de una prestación sanitaria aunque ésta no contenga referencia a ninguna enfermedad, algo claro en el ámbito de la atención especializada –aunque el diagnóstico sea finalmente negativo–, pero mucho más dudoso en el ámbito de la atención primaria –salvo que exista una acumulación de prestaciones–. En este punto es más preciso el RPDP que

y los datos de salud, a diferencia de la normativa española, que tradicionalmente considera los primeros parte de los segundos. Los datos genéticos son considerados en la propuesta de Reglamento categorías especiales de datos a efectos de su tratamiento, pero no datos de salud[172].

Fuera ya del ámbito sanitario, es interesante señalar que la propuesta de Reglamento permite a las fundaciones, asociaciones u organismos sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical el tratamiento de datos no sólo de sus miembros sino también de antiguos miembros o de personas con las que mantengan contactos regulares en relación con sus fines, siempre que no se comuniquen fuera del organismo, sin el consentimiento de los interesados –art. 9.2.d)–[173]. Otra excepción a la prohibición de tratamiento

---

define como dato de salud la información concerniente a la salud pasada, presente y futura, física o mental, de un individuo, considerándose en particular como datos relacionados con la salud de las personas, los referidos a su porcentaje de discapacidad y a su información genética –art. 5.1.g)–. La definición de dato de salud que se encuentra en el articulado de la propuesta de Reglamento puede calificarse como poco precisa. De hecho, ni siquiera incorpora la definición de dato de salud que se contiene en la Memoria explicativa del Convenio 108 –apdo. 45– y en la Recomendación Nº R. (97) 5, del Consejo de Europa –apdo. 38–, que sí se contienen en el RPDP. La RPDP sólo omite como dato de salud las referencias al abuso del alcohol y de la nicotina, al consumo de drogas y al número de días de baja en el fichero de nóminas, que se encontraban en los textos del Consejo de Europa. También la STJCE, de 6.11.2003, –As. *Lidnquist*– había mantenido un concepto amplio de dato de salud. No obstante, el Considerando 26 de la propuesta de Reglamento trata de complementar la definición de dato de salud, añadiendo, entre otras, la referencia a un número, símbolo u otro dato signado a una persona que la identifique de manera unívoca a efectos sanitarios; las muestras biológicas; la identificación de una persona como prestador de asistencia sanitaria a la persona; la información sobre discapacidad o riesgo de enfermedades, el estado fisiológico o biomédico real del interesado, etc.

172. La propuesta de Reglamento define los datos genéticos como los datos, con independencia de su tipo, relativos a las características de una persona que sean hereditarias o adquiridas durante el desarrollo prenatal temprano. Cfr. sobre la cuestión el Documento de Trabajo sobre datos genéticos, del Grupo del Artículo 29, de 17 de marzo de 2004 en *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp91_es.pdf*

173. Hay que recordar que el art. 7 LOPD, en aplicación del art. 8 de la Directiva, excluye del consentimiento expreso y por escrito a los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas cuya finalidad sea política, filosófica, religiosa o sindical «en cuento a los datos relativos a sus asociados y miembros». Es necesario establecer límites al derecho a la cancelación de datos personales cuando afecta a la libertad religiosa. A nuestro juicio, la Iglesia Católica y las distintas comunidades y órdenes religiosas no tienen que cancelar toda su información sobre antiguos miembros, teniendo derecho a guardar constancia de quiénes han pertenecido a esa institución, todo ello en virtud del derecho fundamental a la libertad religiosa, que es un bien constitucional de titularidad individual y colectiva y que tiene dentro de su contenido la facultad de disponer de un mínimo de información necesaria para salvaguardar los fines de la institución, información que es necesaria para preservar los intereses jurídicos que dan vida a este derecho y que en caso contrario quedarían desprotegidos. Los datos de las personas que han pertenecido a instituciones de la Iglesia Católica –ex-sacerdotes o ex-religiosos– siguen siendo necesarios para éstas ya que los Estatutos de estas instituciones y comunidades religiosas no permiten que personas que hayan abandonado una institución puedan volver a perte-

de categorías especiales de datos es que el interesado los haya hecho manifies-

necer a ella –o al menos, hasta que transcurra un plazo de tiempo–. Así, por ejemplo, un sacerdote que se ha secularizado no puede volver a ordenarse; un religioso que ha abandonado la orden no puede volver a tomar los votos. Por ello, el mantenimiento de una mínima información es consecuencia del ejercicio de la libertad religiosa en sentido colectivo. Es claro, por tanto, que algunos datos siguen siendo necesarios y pertinentes para la finalidad para la que se recogieron: dejar constancia de que el interesado perteneció a la institución y causó baja en la misma, circunstancia que debe tenerse en cuenta en el caso de que la persona interesada quisiera al cabo del tiempo volver a solicitar la admisión por lo que la institución tiene un interés legítimo en tener constancia de qué fieles han formado parte de la misma. La obligación de cancelación existe cuando los datos han dejado de ser necesarios o pertinentes para la finalidad para la cual han sido recabados o registrados, pero no cuando se mantiene la finalidad –art. 4.5 LOPD–, en virtud de los Estatutos de una comunidad. Hay que recordar, además, que el art. 23 de la LOPD, siguiendo en este punto el art. 13.1.g) de la Directiva 95/46/CE –lo que se mantiene en el art. 21.1.f) de la propuesta de Reglamento–, establece la facultad del responsable de fichero para denegar el acceso, la rectificación y la cancelación de los datos personales en función de la protección de otros derechos y libertades, en este caso de la libertad religiosa de los individuos y de las comunidades, que se encuentra expresamente recogido en el art. 16 CE. Lógicamente, el derecho a la protección de datos, especialmente el principio de calidad, implica importantes límites a la libertad religiosa: obliga a cancelar el dato de pertenencia a la institución –lo que manifiesta la libertad religiosa en sentido negativo–; la institución sólo puede mantener de las personas que la han abandonado una información adecuada y pertinente –no parece excesiva la información sobre fecha de ingreso y fecha de baja de la institución–; los interesados tienen derecho a la exactitud de los datos –no pueden constar como miembros sino como ex miembros–. Además, esta información no puede comunicarse al exterior. Hay que analizar también si el establecimiento de obligaciones de cancelación, con amenaza de sanción administrativa si no se hace, puede afectar al Acuerdo, de 3 de enero de 1979, entre el Estado Español y la Santa Sede, que tiene rango de Tratado internacional y que en su apartado II.6, establece que «el Estado respeta y protege la inviolabilidad de los archivos, registros y demás documentos pertenecientes a la Conferencia Episcopal Española, a las Curias Episcopales, a las Curias de los Superiores Mayores de las Órdenes y Congregaciones Religiosas, a las Parroquias y a otras Instituciones y Entidades Eclesiásticas». Sin embargo, distinta ha sido la postura del Tribunal Supremo en la Sentencia 7583/2011, de 1 de noviembre, que reconoce el derecho a los ex-miembros de una comunidad religiosa a cancelar todos sus datos obrantes en la institución. La Sentencia contiene dos argumentos acertados y un tercero claramente desacertado. Como primer argumento, la Sentencia señala que una hoja con el nombre, fecha de ingreso y fecha de baja, constituye un fichero de datos y por tanto le es de aplicación la Ley de Protección de Datos. La sentencia afirma que los datos de la institución están organizados y clasificados hasta el punto de que son fácilmente localizables, a diferencia de los libros bautismales, que son "una pura acumulación de datos" que no están ordenados "ni alfabéticamente ni por fecha de nacimiento". De esta forma, la Sentencia tiene en cuenta los criterios de estructuración en virtud de personas y de fácil accesibilidad que permiten afirmar que existe un tratamiento de datos personales, en este caso manual. El segundo argumento consiste en afirmar acertadamente que en el sistema de jerarquía de fuentes, la regulación prevista en el Tratado internacional –en este caso, en el Acuerdo con la Santa Sede– debe ser interpretada conforme a la Constitución, teniendo en cuenta los derechos fundamentales reconocidos en la misma. Sin embargo, la Sentencia entiende –este es el tercer argumento, a nuestro juicio erróneo– que el único derecho afectado es el derecho fundamental a la protección de datos

tamente públicos –art. 9.2.e) de la propuesta de Reglamento, una previsión que

personales, sin tener en cuenta la libertad religiosa de los individuos y de las comunidades –que a diferencia de la protección de datos personales, sí encuentra un reconocimiento constitucional expreso en el art. 16, sin necesidad de esfuerzo jurisprudencial–, olvidando la necesidad de mantener una mínima información para la finalidad para la cual fue recogida, que es el ejercicio de la libertad religiosa, afirmando solemnemente que «los datos dejaron de ser necesarios para la finalidad que justificó su tratamiento cuando la persona deja de pertenecer a la institución». La Sentencia no tiene en cuenta que el derecho a la protección de datos personales –en este caso, la facultad de cancelación– no es un derecho absoluto y que, por tanto, la libertad religiosa, como otros muchos derechos fundamentales, supone un límite al derecho de cancelación –especialmente previsto en la Directiva y en la LOPD–, y permite al responsable mantener una información del interesado cuando siga siendo necesaria para su finalidad, en este caso, el ejercicio de la libertad religiosa –que requiere el mantenimiento de una mínima información de fecha de alta y baja de los ex miembros, que, además, no transciende al exterior–. La cancelación se ejerce sobre la información relativa a la pertenencia a la institución pero no alcanza a la supresión de toda información que sobre esta persona tenga la institución y que sea necesaria para el ejercicio de la libertad religiosa. Esta es la conclusión que se obtiene de la ponderación de derechos fundamentales en presencia, que ya se contenía tanto en la Directiva como en la LOPD, que recoge textualmente la propuesta de Reglamento y que ha omitido el Tribunal Supremo, dando prevalencia al derecho fundamental a la protección de datos de una forma que afecta a los intereses jurídicos que dan vida a la libertad religiosa y, por tanto, menoscabando su contenido esencial. Esto no es más que otro ejemplo de la necesidad de alcanzar un equilibrio de derechos fundamentales en este ámbito y de cómo la libertad religiosa, al igual que otros derechos, exige algunos tratamientos de datos personales sin consentimiento Por último, hay que señalar que ha sido criterio de la Agencia Española que no es necesario eliminar datos personales cuando son reflejo de hechos históricos y se llevan a cabo en virtud de actas de notoriedad, acreditadas con la presencia de padrinos y de testigos. Otra cosa es que se pueda llevar a cabo una anotación marginal en el expediente que deje constancia de que esa persona abandonó la institución o es apóstata y de que esta anotación se le comunique al interesado. Si prosperara el criterio contrario cualquier interesado podría exigir que se arrancaran y destruyeran las hojas de los libros de actas de Fundaciones o Asociaciones de las que se haya desvinculado, aunque sean exactos y adecuados –afectando al derecho de asociación– y aunque no sean objeto de tratamiento informático o formen parte de un fichero manual. Lo mismo podría suceder con los libros-registro de accionistas y libros de actas de las sociedades mercantiles, e incluso con los mismísimos libros del Registro Mercantil y del Registro de la Propiedad, lo que afectaría al ejercicio legítimo de la libertad de empresa. La preocupación por hacer compatible la protección de datos personales con otros derechos fundamentales la hemos manifestado en un libro que lleva precisamente por título *La protección de datos personales. En busca del* «equilibrio» –cit. pp. 35-36–.

Por último, en relación con el Acuerdo del Estado Español con la Santa Sede, hay que señalar que la propuesta de Reglamento, al igual que el art. 17 TFUE, respeta y no prejuzga el estatuto reconocido, en virtud del Derecho interno, a las iglesias y las asociaciones o comunidades religiosas en los Estados miembros –Considerando 128–. Así, la propuesta de Reglamento señala que cuando en un Estado miembro, las iglesias, asociaciones o comunidades religiosas apliquen un conjunto de normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, tales normas podrán seguir aplicándose, siempre que sean conformes con las disposiciones del presente Reglamento, si bien deberán disponer de una autoridad de control Independiente –art. 85, que lleva por título Normas vigentes sobre protección

ya se contenía en el art. 8.e) de la Directiva–, por ejemplo, a través de una actividad política o sindical, , o que el tratamiento sea necesario para el cumplimiento de una misión de interés público, sobre la base del Derecho de la Unión o la legislación de los Estados miembros, que establecerán medidas adecuadas para proteger los intereses legítimos del interesado –art. 9.2.g) de la propuesta de Reglamento–, sin admitir que esta excepción sea realizada por la propia autoridad de control, como contemplaba la Directiva[174].

La regulación de los principios que hace la propuesta de Reglamento incluye un artículo específico sobre el tratamiento de los datos personales relativos a los niños –art. 8–. Sin embargo, la novedad principal se encuentra, de nuevo, en el apartado de definiciones que considera niño a toda persona menor de 18 años[175]. Esta regulación está en contradicción con el art. 13 del RPDP, que acertadamente permitía el tratamiento de los datos de los mayores de catorce años con su consentimiento, sin perjuicio de los casos en los que la Ley exija la asistencia de los titulares de la patria potestad o tutela, y con la legislación que reconoce el ejercicio de los derechos y la autonomía de la voluntad del menor maduro, también en el ámbito sanitario. No obstante, la propuesta de Reglamento incluye una regulación específica –una excepción a esta mayoría de edad de 18 años– en relación con la oferta directa de servicios de la sociedad de la información donde el consentimiento o la autorización del padre o tutor sólo es necesaria en los tratamientos de datos personales relativos a niños menores de 13 años, lo que facilita el funcionamiento de las redes sociales virtuales, que tienen fijada la edad en 14 años –tuenti– o 13 años –Facebook–[176]. Existen

---

de datos de las iglesias y asociaciones religiosas– . Es decir, se obliga a las iglesias a tener una autoridad de control independiente como si fuera un Estado.

174. La Directiva permite que los Estados miembros establezcan otras excepciones a la prohibición de tratamiento de datos especialmente protegidos cuando existan motivos de interés público importantes –*substantial public interest*, no bastaba la misión de interés público–, mediante su legislación nacional o por decisión de su autoridad de control –art. 8.4–. El Considerando 34 de la Directiva lo restringía a sectores como la salud, la protección social o la investigación científica y estadística pública, debiendo establecerse las garantías apropiadas y específicas para proteger los derechos y la vida privada de las personas, algo que también hace el Considerando 42 de la propuesta de Reglamento como analizaremos después –*supra* V.E)–. Esta excepción del principio de prohibición del tratamiento debe ser notificada a la Comisión –art. 8.6–. Sin embargo, como señala el informe encargado por la Comisión, esta notificación raramente se produce por lo que la Comisión tiene una comprensión o un conocimiento incompleto sobre cómo se está poniendo en práctica la previsión contenida en el art. 8.4. En todo caso, como regla general se considera que las leyes nacionales prevén pocas excepciones al principio de prohibición del tratamiento de datos sensibles en virtud del art. 8.4, aunque hay que tener en cuenta que algunos países permiten la adopción por otras normas o han recurrido a autorizaciones *ad hoc* –en este último supuesto ha sido el caso de Francia y Gran Bretaña–.

175. El Considerando 29 de la propuesta de Reglamento señala que para determinar cuándo se considera que una persona es un niño, se sigue la definición establecida en la Convención de las Naciones Unidas sobre los derechos del niño.

176. Téngase en cuenta que la *Children's Online Privacy Protection Act* (COPPA) de EEUU considera menores aquellos que no han cumplido todavía 13 años. El tratamiento de los datos de los menores en las redes sociales y en ámbitos específicos como el sanita-

otras previsiones en la propuesta de Reglamento que tratan de proteger a los menores: la necesidad de que el responsable facilite especialmente cualquier información dirigida a niños de manera inteligible, sencilla, clara y adaptada a interesado –art. 11–[177]; el reconocimiento especial del derecho al olvido en Internet y a la supresión de los datos proporcionados siendo niño –art. 17–; la toma en consideración de que el interesado sea un niño en la ponderación entre la satisfacción del interés legítimo del responsable del tratamiento y los derechos y libertades fundamentales que requieran la protección de los datos personales –art. 6– o la exigencia de que el responsable de tratamientos de datos personales en ficheros a gran escala relativos a niños, al igual que en el caso de los datos biométricos o genéticos, lleve a cabo una evaluación de impacto en la protección de datos personales –art. 33–.

D) La transparencia de la información y el derecho al olvido en Internet.

Existe una necesidad de una mayor armonización en la transposición de los preceptos de la Directiva relativos al suministro de información a los interesados –arts. 10-11–. Las divergencias en este ámbito afectan especialmente a las empresas multinacionales que operan a nivel europeo y que se ven sometidas a cumplir en ocasiones unas obligaciones innecesarias que no incrementan, a juicio de la Comisión, el nivel de protección. Hay divergencias derivadas de la legislación de los Estados miembros que establecen que el responsable debe ofrecer al interesado una información suplementaria a aquella señalada por la Directiva[178]; otras diferencias provienen en ocasiones de interpretaciones de las propias autoridades de control[179]. Las divergencias están, pues, en relación a la información que hay que suministrar al interesado, el modo de hacerlo y el momento adecuado[180]. El art. 14 de la Propuesta de Reglamento aclara estas

---

rio, educativo o los servicios sociales es una cuestión compleja que hemos en *La protección de datos personales*, cit. pp. 1227-1242, 1347-1356 y 1401-1408.

177. Hay que señalar que el RPDP ya introdujo con mucho acierto un conjunto de garantías para la protección de los menores de edad que son ahora reproducidas en la propuesta de Reglamento, en especial, que la información sea comprensible y que existan procedimientos que garanticen que se ha comprobado de manera efectiva la edad del menor y la autenticidad del consentimiento de los padres o tutores –art. 13–. Esta última previsión ha sido expresamente respaldada en la STS, de 15 de julio de 2010. En todo caso, la identificación y la determinación de la edad de los menores y de la autenticidad del consentimiento prestado por los padres son cuestiones difíciles porque pueden generar un tratamiento masivo de datos personales y, por tanto, un problema mayor.

178. El art. 5 LOPD reproduce los arts. 10 y 11 de la Directiva –añadiendo la dirección del responsable–. En todo caso, las divergencias eran admitidas por la propia Directiva al señalar que la información a suministrar al interesado debería ser «al menos» la recogida en el art. 10, admitiendo que la legislación de los países estableciera exigencias suplementarias.

179. Cfr. *Primer informe sobre la aplicación de la Directiva*. cit..

180. Como señala el documento *Analysis and impact study on the implementation of Directive* cit.– «the laws in the Member States vary very considerably with regard to the kinds of information that must be provided, the form in which it must be provided, and the time at which it must be provided. They also differ as to the kinds of additional information that may need to be provided to ensure a fair processing. Some of them repeat the examples given in the Directive, others give somewhat different examples, and some give no examples at all».

cuestiones y lleva a cabo algunas aportaciones novedosas. La información al interesado debe incluir no sólo los fines del tratamiento sino también el interés legítimo del responsable; debe contener, además, información sobre el plazo dentro del cual se conservarán los datos personales, la fuente de la que proceden los datos –esto ya estaba en la LOPD–, el derecho a presentar una reclamación ante la autoridad de control y, en su caso, la intención del responsable de efectuar una transferencia internacional y el nivel de protección del tercer país[181].

La propuesta de Reglamento también mejora el ejercicio de los derechos de acceso, rectificación y cancelación de datos personales a nivel europeo, fijando plazos de respuesta a las peticiones de las personas afectadas, autorizando el ejercicio de estos derechos por vía electrónica y obligando a motivar las denegaciones –arts. 11-15–[182]. La normativa española ya es bastante completa en relación con el ejercicio de estos derechos, si bien, al igual que en el caso del principio de información, cuando el interesado solicite el ejercicio del derecho de acceso, el responsable tendrá ahora que facilitar información sobre el plazo durante el cual se conservarán los datos personales –plazo para la supresión que también está sometido a una obligación de documentación en virtud del art. 28.2.g) y, que, por tanto, está a disposición de la autoridad de control– y el derecho a presentar una reclamación ante la autoridad de control. En general, la regulación de los derechos del interesado, especialmente en lo relativo a la información al interesado y al ejercicio del derecho de acceso, está presidido por la obligación del responsable del tratamiento de aplicar políticas transparentes y fácilmente accesibles en lo que respeta al tratamiento de datos personales y al ejercicio de los derechos de los interesados[183]. El principio de transparencia exige, por tanto, que toda información dirigida al público o al interesado sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro[184]. Esta obligación de ofrecer información transparente y de fácil acceso

181. La información sobre el tratamiento de los datos de carácter personal debe facilitarse a los interesados en el momento de su recogida, o, si los datos no se recogieran de los interesados, en un plazo razonable, dependiendo de las circunstancias del caso. Si los datos pueden ser comunicados legítimamente a otro destinatario, se debe informar al interesado cuando se desvelan por primera vez –Considerando 49–.

182. También se establece en el art. 13 unos derechos en relación con el destinatario, que consiste en la obligación del responsable del tratamiento de informar a los destinatarios a los que haya comunicado sus datos –incluyendo al encargado del tratamiento–, de cualquier rectificación o supresión de datos en virtud del ejercicio de los derechos de los interesados, lo que tiene gran importancia en relación con el derecho al olvido en Internet, al que más adelante nos referiremos.

183. Tanto la información como el ejercicio de los derechos son gratuitos, salvo que la solicitud sea claramente excesiva por su carácter repetitivo, que justifique, en su caso la aplicación de una tasa, asumiendo el responsable la carga de la prueba de la demostración del carácter excesivo de la solicitud. Parece más acertada esta regulación que la normativa española que prohíbe el ejercicio del derecho de acceso a intervalos inferiores a doce meses, salvo que el interesado acredite un interés legítimo –art. 15 LOPD–, haciendo recaer sobre éste la carga de la prueba

184. Esto es especialmente importante en el caso de los niños, que, como acabamos de ver, merecen una protección específica, por lo que cualquier información y comunicación que les afecte debe ofrecerse en un lenguaje claro y llano que puedan comprender con

y comprensión se encuentra inspirada en la Resolución de Madrid relativa a estándares internacionales sobre protección de datos personales y privacidad[185]. Sin embargo, esta cuestión no es abordada por el art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea[186].

Especial mención merece la regulación que la propuesta de Reglamento hace del derecho de rectificación y de supresión o cancelación –art. 16-18–[187], al abordar de manera ambiciosa el derecho al olvido en Internet, que no es más que la aplicación en Internet de los derechos de oposición y cancelación, una cuestión que ha suscitado hasta ahora una cierta controversia[188]. La Comisión trata de dar respuesta a los desafíos que plantean los tratamientos de datos personales en redes sociales, motores de búsqueda, o servicios de computación en nube –por ejemplo, para compartir fotografías– y las dificultades que se presentan para que los interesados mantengan un control efectivo sobre sus datos personales –para que puedan recuperar o borrar sus datos personales de estos prestatarios de servicios en línea–. Frente a este problema, la propuesta de Reglamento reconoce el derecho al olvido en Internet, atribuyendo al interesado el derecho a que el responsable suprima los datos personales que le conciernan y se abstenga de darles más difusión cuando los datos ya no sean necesarios en relación con los fines, haya expirado el plazo de conservación autorizado –se haya cumplido el periodo de almacenamiento de datos–, el interesado retire el consentimiento o se oponga al tratamiento –art. 17.1–. De esta

---

facilitad. Este principio de transparencia es especialmente aplicable a la publicidad en línea, donde la proliferación de agentes y la complejidad tecnológica hace que resulte difícil para el interesado saber y comprender si se están recogiendo datos personales que le conciernen, por quién y con qué finalidad –Considerando 46 de la propuesta de Reglamento–.

185. Esta obligación de transparencia también se ha incorporado al art. 13.3 de la propuesta de Reglamento relativa a una normativa común de compraventa europea (COM (2011) 635 final).

186. El art. 8 de la Carta no menciona el principio de transparencia ni tampoco hace referencia a la necesaria información al interesado. Se limita a reconocer que «toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación» –art. 8.2–, de manera que ni siquiera reconoce el derecho de cancelación.

187. Destaca la previsión de que el derecho de rectificación incluye el derecho del interesado a que se completen los datos personales cuando resulten incompletos, en particular mediante una declaración rectificativa adicional, algo especialmente importante en el ámbito de las Administraciones Públicas, porque el mantenimiento de datos erróneos o incompletos puede dificultar el ejercicio de derechos fundamentales o la percepción de prestaciones sociales. La propuesta de reglamento establece el derecho a que se restrinja el tratamiento de datos en algunos supuestos., evitando la ambigüedad del término bloqueo. Se especifican asimismo los límites a la supresión cuando es necesaria la conservación de los datos por motivos de salud pública o para fines de investigación histórica, estadística o científica. La propuesta de Reglamento incluye también una interesante regulación sobre la conservación de datos a efectos probatorios –art. 17–.

188. El derecho al olvido en relación con la publicación de los medios de comunicación en Internet y el ejercicio de la libertad de información se analiza *infra* apdo. V.E).

forma, se reconoce expresamente el derecho de los usuarios a exigir a los proveedores de estos servicios de Internet que borren completamente sus datos personales –por ejemplo, sus fotos– cuando el cliente se dé de baja en el servicio o cuando dejen de ser necesarios para los fines para los que se recabaron[189]. Además, se establece expresamente que cuando *el responsable haya hecho públicos los datos personales*, éste *está obligado a adoptar las medidas razonables –incluidas las técnicas– en lo que respecta a los datos de cuya publicación sea responsable con miras a informar a los terceros que están tratando dichos datos de que un interesado les solicita que supriman cualquier enlace a estos datos personales, o cualquier copia o réplica de los mismos*. Además, *cuando el responsable del tratamiento haya autorizado a un tercero a publicar datos personales, será considerado responsable de la publicación* –art. 17.2–. De esta forma, cuando los datos personales se hayan hecho públicos, sobre todo en Internet, el responsable deberá velar por la cancelación de los mismos de cualquier *link*, copia o réplica de los mismos que se encuentre accesible en servicios de comunicación que faciliten su búsqueda.

El principal problema que plantea la publicación en Internet está en los efectos multiplicadores que realizan los buscadores por ejemplo, *Google* o *Yahoo!*>, que permiten localizar información relacionada con personas. La Comisión era consciente de que existía un problema y lo ha resuelto de la mejor manera posible –o, a nuestro juicio, de la única manera razonable–. Frente a quienes han mantenido que el derecho al olvido en Internet debía pivotar sobre el derecho de oposición ejercido sobre los motores de búsqueda como responsables de sus propios tratamientos –esta sería la posición de la AEPD en las Resoluciones de tutela de derechos frente a *Google*–, la propuesta de Reglamento construye el derecho al olvido en Internet sobre las obligaciones del responsable principal –de la *web máster*– que ha hecho público los datos[190]. Por ello, la regulación del derecho al olvido que hace la propuesta de Reglamento establece

189. Hay que destacar que la posición jurídica de los ciudadanos frente a las grandes corporaciones internacionales que llevan a cabo tratamientos de datos personales a través de redes sociales virtuales, motores de búsqueda o servicios de computación en nube ha mejorado considerablemente al contemplar la propuesta de Reglamento expresamente, como ya hemos señalado antes, el sometimiento a este de las entidades no establecidas en la Unión Europea que traten datos de residentes en la Unión para ofrecerles bienes o servicios o para controlar su conducta –art. 3.3–; además, los responsables del tratamiento no establecidos en la Unión tienen que designar un representante en la misma –art. 25–. A esto hay que añadir que, como ya hemos señalado, los proveedores de servicios de Internet y los buscadores tienen la obligación de limitar la recogida de datos al mínimo necesario –art. 5.c)–, y deberán informar a los usuarios de forma transparente sobre quién recoge y usa sus datos y sobre cómo, con qué fines y por cuánto tiempo lo hace –arts. 14 y 15–.

190. Esta es la posición que hemos mantenido desde el año 2008 en nuestros trabajos «Transparencia administrativa y protección de datos personales», cit. pp. 23-188, esp. pp. 101-112 y, recientemente, en *La protección de datos personales*, cit. pp. 816-831. Lógicamente, la Comisión está a la espera de que el Tribunal de Justicia resuelva la cuestión prejudicial ya citada planteada por la Audiencia Nacional en relación con las Resoluciones de tutela de derechos frente a *Google*.

una obligación del responsable de la publicación de los datos en Internet, no sólo de suprimir los datos personales sino de comunicar a terceros que están tratando dichos datos que el interesado solicita que se suprima cualquier enlace, copia o réplica de los mismos, relacionando una cosa con la otra, y exigiendo al responsable de la primera publicación que adopte «todas las medidas razonables, incluidas las técnicas», lo que, a nuestro juicio, le obliga a implantar mecanismos que impidan la indexación –aunque esta obligación de implementar tecnología que impida la difusión generalizada debería aparecer con más claridad en la propuesta de Reglamento–. De esta forma, tiene en cuenta las diferentes responsabilidades de la Administración y de los buscadores en relación con la publicación de boletines oficiales y páginas *web* institucionales en abierto de Internet. A nuestro juicio, el responsable del tratamiento es el órgano administrativo que ordena la publicación de la información y que tiene la competencia administrativa sobre la materia a la que se refiere la publicación de los datos personales. Es este órgano administrativo que aprueba la disposición o el acto y que ordena la publicación el que determina los datos personales que van a ser objeto de tratamiento ddatos de concursantes, datos de excluidos, datos de minusvalía, DNI, etc. , el tipo de publicidad ,el diario oficial, Internet, espacio privado en Internet, Intranete y el plazo de publicación –que debe terminar cuando se haya cumplido la finalidad–. Es este órgano el que puede informar al interesado de la finalidad de la publicación y de la disposición legal que la habilita. También es el que debe dar respuesta al interesado que ejercita los derechos de acceso, rectificación, cancelación y oposición y el que debe determinar la obligación de bloqueo de los datos publicados en un diario oficial, la limitación de la accesibilidad a los motores de búsqueda o la supresión de la publicación en Internet cuando el tratamiento ya no sea necesario, dando las instrucciones precisas al responsable del boletín oficial o de la *web* institucional. La garantía del «derecho al olvido» cuando la publicación de la información contiene tratamientos excesivos o ya no es necesaria para la finalidad y se ha cumplido el plazo que la justificaba pasa porque el responsable de la publicación se abstenga de darle más difusión, dejando de publicar la información o, al menos, implante las soluciones técnicas que limiten la facilidad de búsqueda *(findability/searchability)* de la información –en este caso, administrativa– que contenga datos personales[191]. De hecho, la propuesta de Reglamento obliga al

191. Que pasados los años cada vez que una persona ponga su nombre en un buscador en Internet aparezca que fue indultada por un delito, que no pagó una multa o fue perceptora de una renta mínima de inserción social es muy gravoso para esa persona y no hay aparentemente un interés público que lo justifique. Lógicamente, la implantación de este sistema de referencias negativas que impidan la localización y tratamiento de datos personales recogidos en boletines oficiales y en sitios webs en Internet a través de motores de búsqueda exige diferenciar qué información del boletín oficial o de la web debe permitir o no la indexación de su contenido, lo que conlleva también una modificación tecnológica. El documento del Grupo de Trabajo del Artículo 29 recomienda aprovechar las herramientas que facilitan los mismos buscadores con el fin de evitar que la información se guarde en la memoria temporal de éstos. A dichos efectos, es conveniente que los sitios webs utilicen herramientas técnicas e informáticas del tipo «NO ROBOT» que minimicen, en la medida de lo posible, la diseminación de la información de carácter personal, a la que se pueda acceder a través de los

responsable del tratamiento a implementar mecanismos para garantizar que se respetan los plazos fijados para la supresión de datos personales y/o para el examen periódico de la necesidad de conservar los datos –art. 17.7–. Además, establece que el responsable está obligado a limitar el tratamiento cuando ya no necesite los datos para la realización de su misión, pero éstos deban conservarse a efectos probatorios –art. 17.4–[192]. Se especifican asimismo los límites a la supresión cuando exista un deber legal de conservar los datos personales por motivos de interés público, pero obligando a respetar siempre el principio de proporcionalidad –art. 17.3.d)–, lo que requiere, a nuestro juicio, a limitar los tratamientos excesivos. Le faltaría a la propuesta de Reglamento especificar que esta limitación del tratamiento en el marco del derecho al olvido es una limitación de la publicidad[193].

---

motores de búsqueda. Hay que señalar que existe un acuerdo de los principales buscadores que obliga a respetar las instrucciones sobre indexación que se incluyan en el fichero *robots.txt* que se inserta dentro del código «html» de las páginas web. No se trata de una norma jurídica, sino de un acuerdo entre compañías que los buscadores principales respetan. A través del fichero *robots.txt* se pueden dar instrucciones para que no se indexe nada de un sitio web, de un directorio, de directorios concretos e incluso de ficheros específicos. Otro mecanismo disponible para limitar la indexación y que funciona a nivel de página web epor lo que no se puede aplicar a partes de una página webp son los TAGS META, a través de los que se puede indicar que una página web se indexe o no o bien que se impida o se permita el escaneo de los enlaces que aparecen en la misma.

192. La propuesta de Reglamento también establece que cuando el interesado impugne la exactitud de los datos personales, el responsable está obligado a limitar el tratamiento de datos, durante el plazo que le permita verificar la exactitud de los mismos –art. 17.4–.

193. La defensa de la limitación de los tratamientos –en especial de la publicidad– cuando esta no sea necesaria para la finalidad la hemos defendido en el apartado «La prohibición de tratamientos excesivos, la cancelación de la publicación, la integridad e inalterabilidad de los boletines oficiales y la problemática de los buscadores», *loc. cit.* pp. 67-75. Lógicamente como hemos señalado, «los límites a la buscabilidad no deben extenderse a la totalidad de la publicación del número del boletín –para lo que obviamente no tiene competencia el responsable que aprobó la resolución–, ni siquiera a la totalidad de la resolución –la parte dispositiva debe continuar siendo objeto de publicación–, sino únicamente a aquella parte que suponga un tratamiento de datos personales que sea considerado excesivo al haberse cumplido ya la finalidad que lo justificó. Esta limitación al tratamiento se refiere lógicamente a los datos personales publicados en la edición electrónica del boletín oficial y no, lógicamente, ni a la edición en papel –que no constituye un tratamiento de datos– ni a los datos personales incluidos en el procedimiento administrativo cuya resolución dio lugar a la publicación. Esto obliga a modificar la forma de publicación de la versión electrónica del boletín oficial, lo que conlleva una adaptación tecnológica. Por ello, el criterio de publicación del boletín oficial en Internet no puede ser el de hacerlo en un solo documento –Word o pdf–. Tiene que hacerse por partes y de manera dinámica, de forma que permita el bloqueo separado de la información, ya que un mismo número de boletín contendrá resoluciones con distintos plazos y fechas de caducidad –y lo mismo ocurre dentro de la misma resolución–. En definitiva, se trataría de dejar de publicar los «documentos electrónicos» como un todo a publicarlos como un «puzzle» –ya que habría que considerar en cada información el plazo de bloqueo–. Naturalmente, este planteamiento supone una modificación técnica de las plataformas que

Los buscadores se encuentran en una situación jurídica radicalmente distinta. Estos buscadores revisan las páginas de Internet cada cierto tiempo para indexar su contenido y actualizarlo si se han producido cambios, llevando a cabo un tratamiento en la memoria caché y almacenando una colección de información un diccionariou que facilita y agiliza las búsquedas. Está claro que el buscador es responsable de este tratamiento, especialmente cuando esta información ha desaparecido de la fuente inicial. Así, tienen que respetar el principio de calidad (art. 4 LOPD), que obliga a que los tratamientos sean exactos y puestos al día, de forma que respondan con veracidad a la situación actual del afectado, y aquellos que sean inexactos o incompletos deben ser cancelados y sustituidos de oficio, debiendo cancelar la información cuando haya dejado de ser necesaria o pertinente. Por tanto, los responsables de los motores de búsqueda deben adecuar los sistemas de recopilación de referencias, los índices y las estaciones de almacenamiento temporal de manera que respondan al contenido actual. Es responsabilidad de los buscadores anonimizar las búsquedas pasados los seis meses y borrar las *cookies*. Además, los buscadores deben garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición sobre sus propios tratamientos[194]. La propuesta de Reglamento reconoce al interesado el derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular –el art. 6.2 LOPD precisaba aún más señalando «motivos fundados y legítimos relativos a una concreta situación personal»– a que sus datos personales sean objeto de un tratamiento que se ha basado en la necesidad de proteger sus intereses vitales, en el cumplimiento de una misión de interés público o inherente al ejercicio del poder público o en la satisfacción de un interés legítimo perseguido por el responsable o por el cesionario, siempre que no prevalezca el interés o los derechos y libertades del interesado –arts. 19 y 6–[195]. El ejercicio de este derecho obliga al responsable a dejar de usar o a

dan soporte a la publicación de los boletines oficiales, que tiene un coste tanto en términos económicos como en plazo de implantación».

194. Cfr. el Informe del Grupo de Trabajo del Artículo 29, de 4 de abril de 2008, que analizó la protección de datos personales en relación con los buscadores de Internet.

195. Los motores de búsqueda tratan habitualmente datos procedentes de fuentes accesibles al público, lo que les permite acogerse a las excepciones al consentimiento y a la cesión establecidas en los arts. 6.2 y 11.2.b) LOPD, sin perjuicio de tener que respetar legalmente el derecho de oposición en virtud del art. 6.2 LOPD –con las dificultades que después señalaremos–. Lógicamente, el hecho de que la calificación como fuente accesible al público suponga unas excepciones al derecho a la protección de datos personales –y, por tanto, un límite a un derecho fundamental– requiere que se lleve a cabo una interpretación restrictiva de los tratamientos de datos personales que tienen esta consideración, salvo que se ejerza otro derecho fundamental –como sería la libertad de información y que influye en la delimitación de que se entiende por medio de comunicación social–. Por tanto, las fuentes accesibles al público en virtud del art. 3,j) de la LOPD y del art. 7 del RPDP tienen un carácter tasado, y entre éstas no se incluyen las páginas web publicadas en Internet –salvo, de nuevo, que se ejerza la libertad de información y puedan ser consideradas medios de comunicación social–. Esto obliga también a los buscadores a respetar los principios de finalidad y de consentimiento en los tratamientos de datos personales que se encuentren en páginas de Internet, lo que no siempre es posible. La AEPD ha insistido en el carácter taxativo de la calificación de fuentes accesibles al público en la LOPD, «lo que impide que

tratar de cualquier forma los datos personales[196]. El derecho al olvido y a la supresión obliga al responsable del tratamiento a suprimir los datos personales y a abstenerse de darles más difusión cuando el interesado se oponga al tratamiento de datos personales –art. 17.1c)–[197]. Sin embargo, no es razonable ni

consideremos a las páginas web como fuentes accesibles al público. Por ello, para tratar la información contenida en dichas páginas debería de obtenerse el consentimiento de los afectados. Por otro lado, para poder utilizar la información contenida en las mismas debe justificarse la finalidad, principio esencial en materia de protección de datos que se contempla en el artículo 4 de la Ley Orgánica». Cfr. Informe 0342/2008 del Gabinete Jurídico de la AEPD: «Recabar datos de páginas web, no constituye un tratamiento basado en fuentes accesibles al público», en *http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos*. También la Audiencia Nacional ha mantenido una interpretación restrictiva del concepto de «fuentes accesibles al público». Así, la Sentencia, de 18 de febrero de 2007 señala: «Del tenor literal de dicho precepto, se desprende con claridad que recoge un número clausus o enumeración cerrada de las Fuentes que pueden calificarse como accesibles al público, lo que se remarca con el empleo del término «exclusivamente» que se anuda a las concretas fuentes que enumera. Criterio este que es el seguido por la Sala entre otras en las SSAN, Sec 1ª, de 18-5-2006 (Rec.35/2005), 17 de marzo 2006 (Rec. 62/2004), 18-1-2007 (Rec. 240/2005), 24 de abril de 2007 (Rec. 304/05) etc, añadiendo en la última de las sentencias citadas, que en el inciso segundo de dicho precepto debe ser interpretado en relación con el primero». Cfr. LESMES SERRANO, C. (coord.), *La Ley de Protección de Datos. Análisis y Comentario de su jurisprudencia*, Valladolid, Lex Nova, 2008, 124-133.Cfr. DE LA SERNA BILBAO, N., en *Comentarios*, cit. pp. 256-295. La STJUE, de 6.11.2003, As. *Lindqvist* recuerda que las páginas de Internet que incluyan datos de personas identificadas o identificables constituyen tratamientos de datos personales: «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 de datos personales», por lo que está dentro del ámbito de aplicación de la Directiva 95/46/CE.

196. Cfr. VILLAVERDE MENÉNDEZ, I., «El derecho de oposición», en *Comentarios*, cit. pp. 494-501.

197. La AEPD ha reconocido el derecho de oposición de un ciudadano frente al tratamiento que *Google* ha hecho de sus datos publicados en un boletín oficial de la Diputación –R 1046/2007, de 20 de noviembre–. Google alegaba que «la solución dependía del bloqueo de la página de donde salen los resultados, por el titular de la web referenciada», es decir el boletín oficial de la Diputación. Entendía que las informaciones obtenidas a través de sus resultados de búsqueda se encuentran en páginas de terceros que son fuentes accesibles al público, por lo que para eliminar dicho contenido debería desaparecer también de la *web máster* de la página de terceros. *Google* señala que «aunque pudiéramos eliminar la página ofensiva de nuestro índice, ésta seguiría apareciendo en la red. Cada pocas semanas nuestros robots rastrean la *web* [...] si el sitio está disponible en Internet [...] será añadido a nuestro índice si el sitio está disponible en Internet». La AEPD, mantenía que las personas tienen un derecho de oposición para evitar la difusión pública que de sus datos personales hacen los buscadores a partir de fuentes de acceso público y que genera un efecto negativo permanente en contra de la voluntad de los afectados. La actividad de *Google* cuando indexa información de diarios oficiales no se encuentra amparada por la libertad de expresión y no hay una disposición legal que limite el ejercicio del derecho de oposición frente a los buscadores. Además, señalaba que *Google* tiene la obligación de contestar expresamente a la solicitud de ejercicio del derecho de oposición. Por lo que la AEPD concluye que «procede la exclusión de los datos personales del reclamante de los índices

posible centrar el derecho al olvido en Internet como una obligación que descansa principalmente en la responsabilidad de los motores de búsqueda, olvidando otras responsabilidades mucho más graves en las que incurre el responsable de la publicación inicial y haciendo caso omiso de las propias características de los tratamientos que llevan a cabo los motores de búsqueda –de carácter únicamente técnico–. La LOPD permite ejercer el derecho de oposición frente a los tratamientos que procedan de fuentes accesibles al público –art. 6.2–, un planteamiento adecuado para otra etapa tecnológica caracterizado por el uso que determinadas empresas de marketing o de solvencia patrimonial hacían de algunas fuentes accesibles al público como los repertorios telefónicos, las listas de personas pertenecientes a grupos profesionales o diarios oficiales, pero que no es igualmente trasladable a un supuesto de hecho completamente distinto: los enlaces, copias o réplicas de *web másters* que se producen en Internet. El ejercicio del derecho de oposición ante los responsables de los motores de búsqueda que llevan a cabo millones de enlaces a webs cada hora –y donde trabajan muy pocas personas– no puede ser el procedimiento principal para resolver el problema de los tratamientos de datos excesivos, que es, en el fondo, el problema del derecho al olvido en Internet cuando el responsable principal es, por ejemplo, una Administración Pública, un medio de comunicación –como veremos después– o una web institucional conocida– que han adoptado la decisión –no tecnológica– que ha conllevado una publicación de datos excesivos. No parece que el derecho al olvido en Internet de los afectados por las innumerables publicaciones de datos personales excesivas en diarios oficiales –de una sanción por orinar en la vía pública, de una situación de incapacidad permanente, de ser titular de una ayuda a la pobreza– vaya a ser resuelta a través del ejercicio del derecho de oposición ante el motor de búsqueda, que tendría que atender las innumerables reclamaciones de los afectados y cancelar las búsquedas de millones de personas potenciales. Tampoco los motores de búsqueda pueden diferenciar fácilmente entre webs institucionales donde hay que respetar el principio de finalidad y de consentimiento, y diarios oficiales que son fuentes accesibles al público, cuando todos ellos están publicados igualmente en Internet. Asimismo es fácil para el buscador diferenciar las solicitudes de oposición y cancelación relativas a tratamientos que provienen de publicaciones en diarios oficiales, que lleva a cabo una Administración pública sin ejercer un derecho fundamental, de aquellas otras que provienen de webs que manejando fuentes administrativas llevan a cabo una crítica política, que puede suponer un tratamiento de datos personales con fines periodísticos o de aquellas *web másters* que suponen tratamientos de datos personales con fines de expresión literaria

elaborados por *Google*, por lo que se estima el presente procedimiento de tutela de derechos». Sin embargo, a nuestro juicio, la problemática principal –la lesión del derecho fundamental– proviene en este supuesto del tratamiento excesivo de datos personales derivado de la publicación en un diario oficial de una resolución sancionadora por infracción de la ordenanza municipal de convivencia ciudadana que prohíbe orinar en la vía pública por lo que parece, que ante una previsible desatención por parte de la Corporación internacional radicada en EEUU, lo más adecuado primero es exigir el cumplimiento del principio de calidad a la Administración Pública que está cercana.

o artística, donde, como ya señalaremos más adelante, no se puede limitar la indexación por los motores de búsqueda como garantía de la libertad de expresión. Como hemos señalado, la decisión el responsable del tratamiento de publicar en abierto en Internet, pudiéndolo hacer en un espacio privado en Internet o en una Intranet– y la negativa de instrumentar mecanismos de no indexación le convierte en el responsable de la publicación y de los tratamientos posteriores. Por ello, parece que lo razonable es que la responsabilidad principal de garantizar el derecho al olvido recaiga en el responsable también principal que ha hecho públicos los datos. Lógicamente, la responsabilidad del buscador sí se extiende a algunos supuestos específicos: cuando la *web máster* está en un paraíso fiscal, no responde o ha desaparecido; cuando el buscador se niegue a borrar la información habiéndoselo comunicado el responsable principal; cuando los tratamientos de datos personales supongan actividades delictivas o que vulneran gravemente los derechos; situaciones concretas que sí pueden ser gestionados por los responsables de los motores de búsqueda a través de sus propios canales de denuncia como herramienta de autorregulación –que funcionan adecuadamente, como en el caso de *youtube*, que más adelante señalaremos– ante la solicitud de los propios perjudicados, requerimientos de las autoridades de control o medidas cautelares solicitadas por los jueces. En todo caso, sí le faltaría a la propuesta de Reglamento contener una referencia explícita a la facultad del interesado de dirigirse al responsable de los tratamientos relativos a enlaces, copias o réplicas de otros tratamientos principales.

Pues bien, esta posición es la que –*afortunadamente*– adopta la propuesta de Reglamento, que, al regular los tratamientos de datos personales que consisten en enlaces, copias o réplicas de los tratamientos principales, los excluye del derecho de oposición estableciendo que el derecho al olvido o a la supresión se materializa a través de un procedimiento específico ante el responsable que publicó inicialmente los datos –art. 17.2–. Así, se establece que le corresponde al responsable del tratamiento que ha hecho públicos los datos informar a los terceros que están tratando dichos datos que el interesado les solicita que supriman cualquier enlace a sus datos personales o cualquier copia o réplica de los mismos. Además, como hemos señalado antes, no le basta al responsable con informar a los terceros, sino que tiene que adoptar las medidas técnicas que impidan cualquier enlace, copia o réplica de los mismos. El derecho al olvido no se garantiza con un procedimiento en el que el interesado se dirige y le exige al buscador que cancele la información sino que tiene que ejercitar su derecho ante el responsable que publicó inicialmente los datos personales, quedando obligado este responsable a comunicar al tercero que trata los datos, «que el interesado les solicita que supriman cualquier enlace a estos datos personales, o cualquier copia o réplica de los mismos». El que atiende la solicitud de derecho al olvido es, por tanto, el responsable de la publicación inicial, no el buscador, y le corresponde al primero trasladar la petición al segundo, debiendo cancelar ambos. De hecho, el responsable de la publicación inicial no sólo deber tratar de informar a terceros sino de adoptar todas las medidas razonables, incluso las técnicas, para comunicar esta información. Pero aún va más allá la

propuesta de Reglamento: ante quien pretenda seguir interpretando que los motores de búsqueda tienen el carácter de responsables de sus propios tratamientos –ya que en el ámbito de la protección de datos sólo se pueden tratar los datos en calidad de responsable o de encargado y, obviamente, los motores de búsqueda no son encargados del tratamiento de la *web máster* principal–, y, que, por tanto, se encuentran obligados a suprimir los datos y abstenerse de darles más difusión *ex* art 17.1 primer párrafo, la propuesta de Reglamento es taxativa en cortar esa línea interpretativa de forma clara: «cuando el responsable del tratamiento haya autorizado a un tercero a publicar datos personales, será considerado responsable del tratamiento». Es decir, que el responsable del tratamiento de los links, copias o réplicas sigue siendo el responsable principal que publicó los datos. De esta forma, sólo puede actuarse frente al motor de búsqueda cuando este no siga las instrucciones del responsable. Es decir, la propuesta de Reglamento hace desaparecer el derecho de oposición frente al motor de búsqueda cuando se mantiene la publicación en la fuente principal.

Así, ha planteado problemas en España la determinación de cuál era el grado de responsabilidad del buscador cuando la información administrativa sigue siendo publicada en la fuente original Aen el boletín o diario oficial o en la *web* de la Administración . Era necesario precisar en qué medida se puede exigir una responsabilidad al buscador por encontrar una información que la Administración mantiene publicada y que se niega a cancelar en la página de Internet, a bloquear en el boletín o diario oficial o a limitar la posibilidad de indexación. Como hemos defendido en el pasado reiteradamente, existen en este caso dos responsables de tratamiento: el de la página principal que sería la Administraciónq y el buscador. Parece que la responsabilidad principal la tendría la Administración que mantiene la publicación en Internet. No es razonable exonerar de responsabilidad a la Administración, en virtud de la existencia de una habilitación legal o de la propia naturaleza de los boletines oficiales para atribuírsela en exclusiva y únicamente al buscador, olvidando que los primeros están también obligados a respetar el principio de calidad y de proporcionalidad[198]. A nuestro juicio, la Administración, que elige indebidamente el medio

198. El problema principal de que alguien que ha orinado en la vía pública o que ha recibido una ayuda a la pobreza aparezca publicado en un diario oficial lo ocasiona –valga la redundancia– quien lo ha publicado, no el buscador, y es, por tanto, el primero de ellos el que tiene que resolver el problema. De hecho, es mucho más rentable y eficaz para el ciudadano que la autoridad de control se centre en la Administración Pública que tiene muy cerca –por no decir al lado– a que se dirija al buscador que está afincado en EEUU. Pero también es verdad que para la autoridad de control es más valioso en términos de aparición en los medios de comunicación un litigio con una corporación internacional que con una Administración Pública. Esto último supone un desgaste a nivel político muy elevado. En general en muchas ocasiones, es más cómodo para una autoridad de control atribuirle la responsabilidad a una entidad privada que dirigirse contra la Administración iMinisterios, Consejerías o Direcciones GeneralesM. Esto le ocurre especialmente a las Agencias autonómicas en su relación con las Administraciones Autonómicas y con las Administraciones Locales donde se dan la mayoría de las publicaciones excesivas.

de publicación upublicando en el boletín oficial lo que podría estar en un espacio privado en Internetp, publica datos excesivos y se niega a ordenar que el boletín oficial o la *web* institucional realice los cambios organizativos necesarios para evitar los tratamientos excesivos es responsable de las infracciones en este ámbito y no puede diluir su responsabilidad en *Google* por poner un ejemplop, que se limita a buscar la información que la Administración mantiene publicada. No es razonable que la Administración Pública se niegue a implementar unos mecanismos sencillos ofrecidos por los propios buscadores para evitar la indexación de los contenidos y, al mismo tiempo, se atribuya únicamente la responsabilidad de la publicación a los buscadores. Además, téngase en cuenta que los boletines oficiales tienen en virtud de una Ley el carácter de fuente accesible al público, lo que permite que su consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación (art. 3 LOPD) y que su tratamiento y su cesión inicial pueden hacerse sin consentimiento del interesado (arts. 6.2 y 13.2.b) LOPD). Por tanto, nuestro planteamiento se encuentra más centrado en controlar a las Administraciones Públicas y someterlas al principio de calidad, que es, a nuestro juicio, el centro del problema. Además, existe en este punto una legislación de protección de datos personales y unos tratamientos de datos personales que caen inexcusablemente dentro del ámbito de control de las Agencias de Protección de Datos, sin necesidad de dirigirse a corporaciones internacionales que tienen su sede fuera de la Unión Europea–. Todo ello sin perjuicio de exigir en su caso alguna responsabilidad a los buscadores por los tratamientos en la memoria caché en los supuestos concretos antes mencionados. Pero no parece razonable eximir de responsabilidad a la Administración y obligar a los buscadores a no encontrar la información que ésta mantiene publicada en un diario oficial. Aunque los buscadores eliminaran la página del índice, seguiría siendo buscada en Internet por otros buscadores y en pocas semanas los robots volverían a rastrear si el sitio está disponible en Internet y añadirlo al índice. A nuestro juicio, el ciudadano que se encuentre con tratamientos de sus datos personales excesivos debe ejercer su derecho de cancelación ante el responsable del tratamiento principal, que es la Administración que mantiene publicada la información personal, no el buscador[199]. La

199. Sin embargo, la Resolución 463/2007 de la Agencia Española exime de cualquier responsabilidad al *Boletín Oficial de la Provincia de Barcelona* y reconoce un derecho de oposición frente a *Google*. Señala esta Resolución que la Ley «no dispone que los datos personales del reclamante figuren en los índices que utiliza Google para facilitar al usuario el acceso a determinadas páginas, ni tampoco dispone que figuren en las páginas que Google conserva temporalmente en memoria cache». Sin embargo, *Google* busca y trata una información del *Boletín Oficial de la Provincia de Barcelona* que es una fuente accesible al público. Cfr. también las Resoluciones de la AEPD R/01046/2007, de 20 de noviembre, R/00303/2007, de 25 de mayo, y R/00598/2007, de 27 de julio, que obligaban a *Google* a dejar de indexar el nombre de una persona que aparecía en una sanción administrativa publicada en el *Boletín Oficial de la Provincia*. Igualmente, la Resolución 266/2007 de la Agencia Española señala que «ningún ciudadano que ni goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen por la red sin poder reaccionar ni corregir la inclusión ilegítima de los mismos

responsabilidad por la infracción de no cancelar la información debe atribuirse principalmente a la Administración, no al buscador. Exigir la cancelación a los buscadores no parece lo más práctico cuando existen un número amplísimo de éstos dy muchos más que pueden crearse en el futuroy. Hay que señalar que en Internet todo se replica por distintos mecanismos. No sólo son los buscadores conocidos los que utilizan robots de búsqueda, sino que también los emplean los medios de comunicación, las empresas de multas, las editoriales jurídicas, etc., que disponen de sus propios robots programados de acuerdo con sus necesidades. Además, muchos de los buscadores se encuentran fuera de España

---

en un sistema de comunicación universal como Internet [...] Resulta palmariamente legítimo que el ciudadano que no esté obligado a someterse a la disciplina del ejercicio de las referidas libertades –de expresión e información– (por no resultar sus datos personales de interés público ni contribuir, en consecuencia, su conocimiento a forjar una opinión pública libre como pilar básico del Estado democrático) debe gozar de mecanismos reactivos amparados en Derecho (como el derecho de cancelación de datos de carácter personal) que impidan el mantenimiento secular y universal en la Red de su información de carácter personal. Pero la solución es dirigirse al responsable del tratamiento y no al buscador. La Audiencia Nacional ha dictado un auto en el que plantea una cuestión prejudicial al TJUE –Auto de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 27 de febrero de 2012–. Cfr. *supra* apdo. V.A). Cfr. recientemente el interesante trabajo de SIMÓN CASTELLANO, P. *El régimen constitucional del derecho al olvido digital*, Tirant lo Blanch, Valencia, 2012, pp. 135-212. Nuestro planteamiento de exigir las responsabilidades principalmente a la Administración y no al buscador se materializó tempranamente en la APDCM, a través de la Resolución del 13 de febrero de 2007, una tutela de derechos que reconoce el derecho a la cancelación hque en este caso equivaldría al bloqueoq en la edición digital del *Boletín Oficial de la Comunidad de Madrid* de la información de haber sido adjudicatario de una prestación económica de renta mínima de inserción social que se había publicado para cumplir la normativa de notificación de los actos administrativos establecida en el art. 59 de la Ley 30/1992, de 26 de noviembre. En esta resolución se exigió a la Dirección General de Servicios Sociales que ordenase al *Boletín Oficial de la Comunidad de Madrid* la cancelación lel bloqueoe de la publicación en la edición electrónica al considerar que el mantenimiento de esa publicidad en Internet, cumplida ya la finalidad de la notificación, era un tratamiento excesivo que no respetaba el principio de calidad, además de que dicha publicación contenía datos excesivos. Así, en los procedimientos de subvenciones o de ayudas sociales –para personas con discapacidad, víctimas de violencia de género– donde la información afecta a la intimidad y puede lesionar derechos y donde el interés público es menor, la publicación debe limitarse a una somera indicación del contenido del acto y del lugar donde los interesados pueden comparecer dentro del plazo correspondiente para tener acceso íntegro. Lo mismo debería hacerse cuando la publicación de datos personales se produce por problemas de notificación –por ejemplo, de resoluciones sancionadoras de la Administración–. Cfr. especialmente la Recomendación 2/2008, de 25 de abril, de la APDCM, sobre publicación de datos personales en boletines y diarios oficiales en Internet, en sitios webs institucionales y en otros medios electrónicos y telemáticos –llama la atención que la AEPD no haya aprobado todavía un texto semejante y siga centrando sus Resoluciones únicamente en los buscadores–. La explicación doctrinal de los criterios que permiten la actividad de ponderación entre la transparencia y la protección de datos personales y su aplicación a supuestos conflictivos la hemos hecho en «Transparencia administrativa», *loc. cit.* pp. 61-165 y *La protección de datos personales*, cit. pp. 760-904.

oconsecuencia lógica de la universalidad de Internetc y hasta ahora ha sido muy difícil garantizar la aplicación de la Directiva y de la ley española y la ejecución de las resoluciones de las autoridades de protección de datos de España. Quiero que se me entienda bien: existe también una responsabilidad del buscador secundaria del buscador pero en los temas que están a debate la responsabilidad principal la tiene la fuente original que es la Administración Pública, que ha publicado reiteradamente en un diario oficial o en Internet datos excesivos –incluso especialmente protegidos– para la finalidad y que los mantiene publicados a pesar de que se haya cumplido ésta, negándose a adoptar ningún mecanismo técnico que impida la indexación; en cambio, los buscadores son básicamente herramientas técnicas, y que tienen sin duda una responsabilidad, pero que no es, en absoluto, la principal[200].

La propuesta de Reglamento cierra el debate sobre la determinación de la responsabilidad de los diferentes actores –de quien publica inicialmente la información en Internet y de los motores de búsqueda que llevan a cabo los tratamientos posteriores– y ante quien deben ejercitarse los derechos. Así, la propuesta de Reglamento centra el derecho al olvido en Internet en que *el responsable de la publicación inicial suprima los datos y se abstenga de darles más difusión* (art. 17.1); obliga al responsable que haya hecho públicos los datos no sólo a suprimir la publicación sino también a *dirigirse a los terceros* que estén tratando dichos datos para informarles de que un interesado les solicita que supriman cualquier enlace a estos datos personales o cualquier copia o réplica de los mismos (art. 17.2); obliga al responsable a *adoptar medidas técnicas* para que los terceros supriman cualquier enlace, copia o réplica de los mismos, lo que le obliga a establecer límites a la indexación (art. 17.2); señala que cuando el responsable del tratamiento haya autorizado a un tercero a publicar datos personales –lo ha autorizado cuando publica la información en un boletín oficial que tiene el carácter de fuente accesible al público o se niega a establecer herramientas que impida la indexación– *será considerado responsable de la publicación* (art. 17.2 *in fine);* obliga al responsable del tratamiento a implementar mecanismos para garantizar que *se respetan los plazos fijados* para la supresión

200. Hay un debate de fondo sobre la responsabilidad de las herramientas. Esto ha surgido también cuando la industria de los contenidos ha pedido responsabilidad civil a los programadores que han diseñado sistemas de compartir archivos mediante redes descentralizadas en las que miles de internautas son al mismo tiempo clientes y servidores, creando una comuna informática anónima pprogramas P2P como *eMule* o *Piolet*>. La tecnología es siempre neutral. En todo caso, los buscadores deberían tratar de implementar aquellos mecanismos de privacidad por defecto que sean técnicamente posibles, aplicando una fórmula semejante a la que pueden emplear las empresas de publicidad o prospección comercial cuando emplean fuentes accesibles al público Guía de Telecomunicaciones, listados profesionalesG, en las que los interesados le han manifestado su derecho de oposición al tratamiento aunque todavía no ha podido ser hecho efectivo en la fuente accesible al público hasta la publicación de la siguiente edición. Los buscadores podrían valorar la posibilidad de manejar listados de excluidos –para facilitar el funcionamiento de los canales de denuncia en los supuestos ya señalados–, sin perjuicio de las obligaciones del responsable principal que ordena y mantiene la publicación de la información.

de datos personales y/o para el examen periódico de la necesidad de conservar los datos (art. 17.7)[201].

También merece destacarse en la propuesta de Reglamento el reconocimiento del derecho a la portabilidad de los datos, de manera que cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado –también cuando el interesado los haya facilitado con su consentimiento y en virtud de un contrato–, el interesado tenga derecho a obtener del responsable una copia de los datos en un formato electrónico que le permita seguir utilizándolos –art. 18–. De esta forma, el reconocimiento que hace la propuesta del Reglamento de la portabilidad de los datos supone el derecho de los interesados a retirar sus datos –fotos o una lista de amigos– de una aplicación o un servicio y transferirlos a otra aplicación sin que los responsables del tratamiento inicial puedan bloquearlo. Por último, otra buena muestra de cómo la propuesta de Reglamento va encaminada a atajar problemas es el reconocimiento del derecho de oposición cuando el tratamiento de los datos personales tenga por objeto la mercadotecnia directa, derecho que debe ofrecerse al interesado de manera explícita, inteligible y distinguible de cualquier otra información y sin que le suponga gasto alguno –art. 19.2-[202].

Las transferencias internacionales de datos personales a terceros países u a organizaciones internacionales se contempla en el Capítulo V –arts. 40-45– de la propuesta de Reglamento. La propuesta de Reglamento 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». Por ello, la regulación que se hace de las transferencias internacio-

201. La propuesta del Reglamento insiste en la importancia de suprimir los datos cuando ya no sean necesarios en relación con los fines y se haya cumplido el periodo de almacenamiento –17.1–, algo especialmente aplicable a la publicación de datos personales por las Administraciones Públicas. Así, establece que el límite al derecho de supresión derivado del cumplimiento de una obligación legal de conservar los datos personales, como puede ser la existencia de unos diarios oficiales, debe respetar el principio de proporcionalidad –art. 17.3.d–. Incluso regula la posibilidad de limitar el tratamiento de datos personales cuando ya no sean necesarios para la realización de su misión pero éstos deban conservarse a efectos probatorios –art. –art. 17.4.b)–. Nos centramos en este trabajo en exponer las principales novedades del Reglamento. La prohibición de tratamientos excesivos, la cancelación de la publicación y la integridad e inalterabilidad de los diarios oficiales lo hemos analizado en *La protección de datos personales*, cit. pp. 768-780.

202. La propuesta de Reglamento aborda también la problemática de los tratamientos de datos personales destinados a evaluar aspectos personales, analizar o predecir el rendimiento profesional, la situación económica, la localización, el estado de salud, las preferencias personales o la fiabilidad del comportamiento, teniendo en cuenta la Recomendación del Consejo de Europa sobre la elaboración de perfiles –CM/Rec (2010), 13–. El derecho reconocido en la LOPD a la impugnación de las valoraciones –art. 13– aparece ahora dentro del derecho de oposición a la adopción de medidas que produzcan efectos jurídicos que le conciernan o que le afecten de manera significativa basadas en la elaboración de perfiles –art. 20–.

nales va dirigida a una mayor flexibilización y simplificación de los trámites administrativos. Así, se regulan las transferencias en virtud de una decisión de adecuación, mediante garantías apropiadas y mediante normas corporativas vinculantes, y donde aparece como nota característica la desaparición de la obligación de notificación de la transferencia a la autoridad de control –en consonancia con la desaparición de la obligación de notificación del tratamiento–, reduciéndose al mínimo las exigencias de autorización. Así, la Comisión puede decidir que un tercer país o una organización internacional garantizan un nivel adecuado de protección de manera que no se requieran nuevas autorizaciones para la transferencia internacional, tomando en consideración su legislación –su Estado de Derecho–, la existencia de autoridades de control independientes y de recursos jurisdiccionales y los compromisos internacionales asumidos[203], introduciéndose ahora la posibilidad de que la Comisión evalúe el nivel de protección que ofrece un territorio o un sector de tratamiento en un tercer país. También la Comisión podrá decidir que estos países u organizaciones internacionales no garantizan un nivel adecuado de protección. Igualmente se regulan las transferencias en el supuesto de que el responsable o el encargado obtengan garantías apropiadas de un tercer país o de una organización internacional en lo que respecta a la protección de datos personales a través de un instrumento jurídico vinculante como pueden ser: las normas corporativas vinculantes de los grupos de sociedades que aparecen mencionadas específicamente –las *Binding Corporate Rules* (CPR), que deben haber sido aprobadas previamente por la autoridad de control mediante el mecanismo de coherencia y que permiten las transferencias internacionales de la Unión a organizaciones dentro del mismo grupo de empresas, siempre que estas normas corporativas incluyan garantías relativas a la protección de datos personales–; las cláusulas tipo aprobadas por la Comisión o por la autoridad de control[204] –en todos estos casos, la transferencia internacional no requiere autorización–; o las cláusulas contractuales entre el responsable o el encargado y el destinatario de los datos, que ofrecen una mayor flexibilidad a éstos pero que, a diferencia de las anteriores, deben ser autorizadas previamente por la autoridad de control[205]. Por último, la propuesta de Reglamento incorpora un régimen de excepciones que permite las transferencias internacionales aunque no se den los supuestos antes desarrollados. Se añade a

203. En la actualidad, la Comisión ha declarado a Argentina, Israel y Andorra como países que tienen un nivel adecuado de protección, y recientemente, en agosto de 2012, también a Uruguay.

204. Estas cláusulas tipo de protección de datos de la Comisión se encontraban también previstas en el art. 26.4 de la Directiva 95/46/CE. Cfr. también la Decisión de la Comisión de 5 de febrero de 2010 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46 en *http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/decisiones/common/pdfs/decision_comm_clausulas_contractuales_2010.pdf* La novedad es que las cláusulas tipo de protección de datos también pueden ser adoptadas por la autoridad de control y ser declaradas generalmente válidas por la Comisión.

205. En este caso se aplicaría el procedimiento de autorización descrito en el Capítulo V del Título IX del RPDP, arts. 137-144.

los supuestos contemplados en el art. 26 de la Directiva y en el art. 34 de la LOPD un supuesto nuevo, que va a reducir aún más la obligación de autorización, facilitando las transferencias internacionales puntuales a países que no tengan un nivel adecuado de protección: que la transferencia internacional sea necesaria para la satisfacción de un interés legítimo del responsable o del encargado, que no pueda ser calificada como frecuente ni masiva y que estos hayan evaluado y documentado todas las circunstancias que rodean a la operación de transferencia –prestando especial atención a la naturaleza de los datos, la finalidad y duración de la operación y situación de los países de origen y de destino–, y hayan ofrecido garantías apropiadas con respecto a la protección de los datos personales. En esta línea de mayor flexibilidad, hay que resaltar que la propuesta de Reglamento permite que la transferencia internacional la lleve a cabo no sólo el responsable sino también el encargado de tratamiento –art. 40–[206].

E) Los límites al derecho a la protección de datos personales. Especial referencia a la libertad de información y a los tratamientos de datos personales que llevan a cabo las Administraciones Públicas.

El derecho a la protección de los datos personales, como el resto de los derechos reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea, no es un derecho absoluto sino que se encuentra sometido a límites. Así, el art. 52.1 de la Carta, relativo al «Alcance e Interpretación de los derechos y principios», señala que «cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por Ley y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o la necesidad de protección de los derechos y libertades de los demás»[207]. Por tanto, no todos los límites al derecho fundamental a la protección de los datos personales son legítimos o se encuentran justificados sino que es necesario que estos límites cumplan unos requisitos: deben estar establecidos por Ley, respetar su contenido esencial y el principio de proporcio-

206. Inicialmente la Agencia Española entendía que el exportador de datos debía ser el responsable del fichero. Posteriormente, la Decisión 2010/87, de 5 de febrero, de la Comisión, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países –DOUE 12.2.2010- ha ofrecido esta posibilidad también a los encargados de tratamiento nacionales. Por ello, la Agencia Española ha presentado recientemente un nuevo modelo de cláusulas contractuales de transferencias internacionales de datos, en respuesta a la demanda surgida por parte de empresas españolas prestadoras de servicios que se dirigían directamente a la Agencia para solicitar autorizaciones de transferencias internacionales de datos.

207. Cfr. MANGAS MARTIN, A., «Comentario al Artículo 52», en MANGAS MARTIN, A., (Dir.), *Carta de los Derechos Fundamentales de la Unión Europea*, cit. pp. 826-851. A diferencia del CEDH, que establece expresamente en el mismo art. 8 que reconoce el derecho a tener vida privada cuáles son sus límites, la Carta proclama de manera absoluta el derecho a la protección de datos en el art. 8, estableciendo en el art. 52 una cláusula general de limitación de los derechos.

nalidad y debe ser unas limitaciones necesarias y responder efectivamente a objetivos de interés general de la Unión o a la protección de los derechos y libertades de los demás[208]. La Carta también señala que los derechos fundamentales reconocidos en ésta –lógicamente, también sus límites– deben interpretarse en armonía con las tradiciones constitucionales comunes a los Estados miembros –art. 52.4–. Así, la jurisprudencia del Tribunal Constitucional Español ha admitido que los poderes públicos puedan establecer límites a los derechos fundamentales, y, por tanto, al derecho fundamental a la protección de datos personales, pero ha fijado un concreto canon constitucional que deben respetar estos límites para que puedan considerarse legítimos y que es coincidente con el establecido ahora a nivel europeo: que las restricciones a los derechos deben estar establecidas en una Ley de forma suficiente y clara de manera que sea previsible para sus destinatarios; que la finalidad sea legítima, al estar orientada a alcanzar otro bien o valor constitucional; y que su aplicación sea motivada y proporcional. La jurisprudencia del Tribunal Constitucional ha acudido a dos técnicas para establecer un equilibro entre los derechos y sus límites: el contenido esencial de los derechos fundamentales –que es una garantía genérica o abstracta del derecho fundamental prevista en el art. 53.1 CE y definida en la STC 11/1981, de 8 de abril– y el principio de proporcionalidad. Lógicamente supone una vulneración del principio de proporcionalidad aquellos límites que afecten al contenido esencial de un derecho fundamental[209].

La Carta de Derechos Fundamentales de la Unión Europea también establece en el art. 52.3 que «[e]n la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán iguales a los que les confiere dicho Convenio. Esta disposición no impide que el Derecho de la Unión conceda una protección más extensa». La Carta no quiere reducir el nivel de protección de los derechos previsto en el Convenio de forma que no es legítimo que se recorten los derechos que en el CEDH no están sujetos a limitaciones o que se lleve a cabo una

208. El TJUE ha señalado que el derecho a la protección de datos de carácter personal no es un derecho absoluto, sino que se ha de considerar en relación con su función en la sociedad –Sentencia de 9.11.2010, C-92/09 y C-93/09, *Volker und Markus Schecke y Eifert*, Rec. 2010. Este Tribunal ha señalado reiteradamente que los límites a los derechos fundamentales sólo están justificados si responden a objetivos de interés general perseguidos por la Comunidad y respetan el principio de proporcionalidad. En caso contrario estos límites suponen una intervención desmesurada e intolerable que afecta a la propia esencia de los derechos.

209. Como ha señalado la STC 169/2001, de 16 de julio, «la exigencia constitucional de proporcionalidad de las medidas limitativas de derechos fundamentales requiere, además, de la previsibilidad legal, que sea una medida idónea, necesaria y proporcionada en relación con un fin constitucionalmente legítimo». Cfr. DIEZ-PICAZO, L. M., *Sistema de derechos fundamentales*, Civitas, Madrid, 2003, pp. 95-117; VILLAVERDE MENÉNDEZ, I., «Los límites de los derechos fundamentales» en AA.VV, *Teoría general de los derechos fundamentales en la Constitución Española de 1978*, Tecnos, Madrid, 2004. MEDINA GUERRERO, M., *La vinculación negativa del legislador a los derechos fundamentales*, McGraw Hill, Madrid, 1997.

limitación mayor que la que prevé el CEDH. El derecho a la protección de los datos personales ha sido configurado por el Tribunal Europeo de Derechos Humanos –TEDH– como una manifestación del derecho al respeto a la vida privada recogido en el art. 8.1 del CEDH. Este derecho no es reconocido como un derecho absoluto sino que pueden ser objeto de restricciones o injerencias por parte de los poderes públicos. El mismo artículo que reconoce este derecho establece cuáles pueden ser sus límites, fijando los requisitos que deben cumplir estas limitaciones al derecho a tener vida privada y a la protección de datos personales para que puedan reputarse como legítimas. Así, el art. 8.2 del CEDH señala que «[n]o podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida, que en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás». De esta forma, el CEDH exige tres requisitos para que se entienda que una injerencia –un límite, una restricción– al derecho fundamental deba entenderse legítima: que esté prevista en una ley, que sea para una finalidad legítima –seguridad nacional, seguridad pública, bienestar económico, defensa del orden, prevención del delito, protección de la salud o de la moral o de los derechos y libertades de los demás– y que la injerencia sea necesaria para una sociedad democrática. Si no se cumplen estos requisitos la injerencia no está justificada y supone una lesión del derecho fundamental a la protección de datos personales. De esta forma, en virtud del art. 52.3 de la Carta, la interpretación y aplicación de los límites al derecho a la protección de datos personales en el ámbito de la Unión Europea deben respetar tanto el Convenio 108 del Consejo de Europa, ya citado, como la jurisprudencia del TEDH sobre este derecho, si bien se trata de una exigencia de mínimos, ya que el Derecho de la Unión puede establecer en el desarrollo legislativo de este derecho una protección más extensa y exigente que la que actualmente presta el CEDH[210].

La primera exigencia para limitar el derecho fundamental a la protección de datos personales es que esta limitación tenga un fundamento legal. Esta es una exigencia que se encuentra en la Carta, en el CEDH, en las Constituciones de los Estados miembros y en la jurisprudencia del TEDH y de los Tribunales Constitucionales de los Estados miembros[211]. Tanto la Directiva 95/46/CE –art. 13.2– como la propuesta de Reglamento –art. 21.1– señala que se podrá limitar el alcance del derecho a la protección de datos personales por medio de medidas legales o legislativas. La exigencia de previsión legal no ha sido entendida por el TEDH como una exigencia de Ley en sentido formal sino en un sentido material que se remite a lo que se entienda por ley en los distintos ordenamien-

210. Cfr. MARTÍN Y PÉREZ DE NANCLARES, J., , «Comentario al Art. 8», *loc. cit.* p. 238.
211. El Tribunal Constitucional ha señalado en su Sentencia 207/1996, de 16 de diciembre, que «la limitación de dicho derecho [del derecho a la intimidad] sólo podría producirse con fundamento en una inexcusable previsión legislativa».

tos jurídicos[212]. En todo caso, el TEDH exige que la ley cumpla dos características: accesibilidad y previsibilidad[213]. Así, este Tribunal señaló en la Sentencia de 26 de abril de 1979 –caso *Sunday Times*– en relación con la expresión «previstas por la ley» que la primera condición «hace referencia a que la ley tiene que ser lo suficientemente accesible: el ciudadano tiene que disponer de informaciones suficientes que se adecuen a las circunstancias de las normas legales aplicables al caso; la segunda condición se refiere a que una norma no puede considerarse ley a menos que se formule con la suficiente precisión que permita al ciudadano adecuar su conducta; debe poder prever rodeándose para ello de consejos clarificadores, las consecuencias de un acto determinado». El Tribunal Constitucional, en la Sentencia 292/2000, de 30 de noviembre, en la que reconoció expresamente el derecho fundamental a la protección de datos y analizó sus límites, insistió también en la importancia de la accesibilidad y la previsibilidad, afirmando que «la Ley que establezca los límites sea accesible al individuo concernido por ella, que resulten previsibles las consecuencias que para él pueda tener su aplicación, y que los límites respondan a una necesidad social imperiosa y sean adecuados y proporcionados para el logro de su propósito» –F. J. 9º. Es especialmente importante en relación con la legitimidad de los límites al derecho fundamental a la protección de datos personales la condición de «previsibilidad», esto es, que la ley sea lo suficientemente clara y detallada que otorgue al ciudadano una información suficiente sobre las medidas que pueden ser aplicadas de manera que pueda adaptar su conducta. No obstante, hay que tener claro que una ley no puede regular absolutamente todos los supuestos que pueden justificar límites a este derecho fundamental. Así, una ley no vulnera la previsibilidad al establecer un poder discrecional siempre que precise con la suficiente claridad su alcance y la manera de ejercerlo, estableciéndose también los instrumentos de control. Así, en el caso *Malone*, de 2 de agosto de 1984, el TEDH señala que la ley debe indicar con claridad el nivel de discrecionalidad de los poderes públicos y su finalidad, de manera que el ciudadano tenga garantías suficientes para reaccionar frente a la arbitrariedad. En los casos *Kruslin* y *Huvig*, de 24 de abril de 1990, el TEDH señala el tratamiento de datos personales vulnera el derecho en el art. 8 del CEDH cuando la Ley no establece las garantías necesarias. El TEDH establece que para que una norma legal que limite el derecho a la protección de datos cumpla la condición de previsibilidad es necesario que sea clara y concisa, que establezca las circunstancias que justifiquen el tratamiento, el procedimiento que se va a seguir; la información que va a ser recogida o almacenada, y en este último supuesto, por cuánto tiempo y bajo qué condiciones; los procedimientos de acceso y cesión de datos personales, las autoridades que pueden tener acceso y a quiénes pue-

212. Así, por ejemplo, en el Derecho de la Unión Europea no existe el concepto de ley en sentido formal.

213. Cfr. sobre esta cuestión tempranamente la Sentencia del TEDH de 25 de marzo 1993, –caso «Costello-Roberts/Reino Unido» y las Decisiones de la CEDH, núms. 8239/1978 y 8278/1978.

den cederse los datos; y los procedimientos de información, rectificación y cancelación de los datos recopilados.[214].

La segunda exigencia que debe respetar los límites al derecho fundamental a la protección de datos personales es que vaya encaminada a alcanzar una finalidad legítima –un bien o valor constitucional–. El art. 8.2 CEDH detalla las finalidades que pueden justificar injerencias en la vida privada: la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, y la protección de los derechos y las libertades de los demás. El cumplimiento del requisito de la finalidad legítima no ha supuesto un serio obstáculo en el TEDH ya que éste se ha limitado hasta ahora a constatar si en el supuesto concreto se ha invocado uno de estos fines legítimos mencionados. De esta forma, es legítimo el tratamiento de datos personales sin consentimiento del interesado y sin su conocimiento siempre que se alegue que se busca, entre otros bienes jurídicos, por ejemplo, la seguridad nacional, la seguridad pública, la defensa del orden, la prevención del delito o más concretamente, la lucha contra el terrorismo. El TEDH entiende que los Estados tienen un amplio margen de configuración, correspondiéndole a la autoridad nacional determinar si la injerencia responde a uno de los fines legítimos señalados[215]. Así, la protección de los derechos y las libertades de los demás es una finalidad legítima que pude justificar la limitación del derecho fundamental a la protección de datos personales. La Carta de Derechos Fundamentales de la Unión Europea, a diferencia del CEDH, no establece un conjunto tasado de fines legítimos que pueden justificar restricciones a los derechos fundamentales –algo lógico, ya que se trata de una cláusula general de limitación– sino que únicamente señala que los límites a los derechos fundamentales deben ser necesarios y responder efectivamente a «objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás" –art. 52.1–. Los Tribunales Constitucionales Europeos también reconocen límites a este derecho en razón de los intereses generales, especialmente cuando los tratamientos de datos personales los llevan a cabo las Administraciones Públicas[216].

---

214. Cfr. el análisis de la jurisprudencia del Tribunal Europeo de Derechos Humanos en ARENAS RAMIRO, M., *op. cit.* pp. 114-118 y 136-140.

215. La expresión que utiliza frecuentemente el Tribunal de Estrasburgo para justificar las excepciones al artículo 8 del Convenio es *pressing social need*. Cfr. sobre la cuestión la Sentencia *Klass and others v Federal Reepublic of Germany*, de 6 de septiembre 1978. La jurisprudencia de este Tribunal reconoce límites a este derecho en virtud de la seguridad del Estado –caso *Leander*, de 26 de marzo de 1987–, la persecución de infracciones penales –casos *Z vs. Finland*, de 25 de febrero de 1997, y *Funke*, de 25 de febrero de 1993–. Cfr. RUIZ MIGUEL, C., *El derecho a la protección de la vida privada*, cit.

216. El Tribunal Constitucional Federal Alemán, que en la célebre Sentencia de la Ley del Censo reconoció la existencia de un derecho a la autodeterminación informativa dentro del derecho general de personalidad y de la dignidad personal –art. 2.1 *GG* en relación con el art. 1.1 *GG*-, señala también que «el individuo no goza de un derecho entendido como un dominio absoluto ilimitable sobre sus datos personales; el individuo no es sino una personalidad que se despliega en el seno de una comunidad social. La información, aunque sea personal, representa un aspecto de la realidad social, la

La normativa que ha desarrollado el derecho fundamental a la protección de datos personales –el Convenio 108, la Directiva 95/46/CE y las leyes de los Estados– justifican excepciones al régimen general de protección de datos y a las facultades del titular de los datos cuando sea una medida necesaria para alcanzar las siguientes finalidades: seguridad nacional, defensa, seguridad pública, prevención, investigación, descubrimiento y persecución de infracciones penales, un interés económico y financiero importante y la protección del interesado o los derechos y libertades de otras personas. Además, la Directiva 95/46/CE y las leyes nacionales prevén el tratamiento de datos especialmente protegidos, sin consentimiento del interesado, para una finalidad de asistencia sanitaria. En especial, hay que señalar que el art. 13 de la Directiva, titulado *Excepciones y limitaciones*, señala que los Estados miembros podrán adoptar medidas legales para limitar el derecho fundamental a la protección de datos personales «cuando tal limitación constituya una medida necesaria para la salvaguardia –"*when such a restriction constitutes a necessary measure to safeguard*»– de la seguridad del Estado; la defensa; la seguridad pública; la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública; la protección del interesado o de los derechos y libertades de otras personas»[217]. Según el informe de la Comisión, estas restricciones deben tener en cuenta la necesidad de luchar contra el crimen o proteger la salud pública en emergencias[218]. Otras previsiones de la Directiva contienen posibilidades semejantes para estas limitadas excepciones como es el supuesto ya mencionado la misión de interés público o los motivos de interés público importantes –*importantpublic interest*–[219]. La determinación de qué se

cual no puede depender, en último término, de la voluntad del individuo. [...] De ahí que el individuo haya de tolerar límites a su derecho a la autodeterminación informativa por *razón de los intereses generales*». Así, el Tribunal Constitucional Alemán ha hecho depender la legitimidad del tratamiento de datos personales por los poderes públicos de la finalidad para la cual van a utilizarse los datos. Cfr. ARENAS RAMINO, M., *op. cit.* pp. 412-413.

217. La legislación nacional de protección de datos personales no se ha limitado a transponer la Directiva europea sino que ha desarrollado el derecho fundamental a la protección de datos personales en cada uno de sus países, por lo que abarca materias propias del antes denominado tercer pilar como policía, seguridad pública o justicia. Así debe entenderse el art. 13 de la Directiva que permite establecer excepciones en materias como la seguridad del Estado, la defensa, la seguridad pública o la prevención, investigación, detección y represión de infracciones penales. Hay que dejar claro que una cosa son los tratamientos de datos personales que caían dentro del antes denominado tercer pilar –por ejemplo, los de la policía– y otra cosa distinta es que tratamientos de datos dentro del llamado primer Pilar puedan encontrarse exceptuados de algunas de las obligaciones establecidas en la Directiva.

218. Cfr. *Segundo Informe sobre la aplicación de la Directiva*, cit..

219. La Directiva 95/46/CE legitima el tratamiento sin consentimiento del interesado para el cumplimiento de una «misión de interés público» –art. 7.e)–, previsión que mantiene el art. 9.g) de la propuesta de Reglamento. También la Directiva establecía que

entiende por *«a necessary measure»* y "*an important public interest*" ha sido, sin duda, una de las fuentes de mayores discrepancias entre las legislaciones nacionales[220]. Pues bien, la propuesta de Reglamento mantiene en su art. 21 –Limitaciones»– en gran medida y con la misma redacción los límites al derecho a la protección de datos personales que se encontraban en el art. 13 de la Directiva. Así, establece que tanto el Derecho de la Unión como los Estados miembros –la Directiva sólo hacía mención a los segundos– pueden limitar por medio de medidas legislativas el alcance de los derechos relativos a la protección de los datos personales cuando tal limitación constituya «una medida necesaria» –se mantiene pues la expresión– [...] «para la seguridad pública; la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales; otros intereses públicos de la Unión o de un Estado miembro, en particular un interés económico y financiero importante de la Unión o de un Estado miembro, especialmente en los ámbitos fiscal, presupuestario y monetario, así como la protección de la estabilidad y la integridad de los mercados; la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas; una función reglamentaria de ins-

---

los Estados miembros podrían «por motivos de interés público importante» establecer excepciones a la prohibición de tratamiento de datos especialmente protegidos, por decisión de la legislación nacional o de la autoridad de control –art. 8.4–, lo que el Considerando 34 concretaba a «sectores como la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, la investigación científica y las estadísticas públicas». En cambio, el art. 9.2.g) de la propuesta de Reglamento justifica las excepciones al tratamiento de categorías especiales de datos cuando esto sea necesario para el cumplimiento de una «misión de interés público» –abandona el concepto más exigente de «interés público importante»–, si bien exige que esto se haga sobre la base del Derecho de la Unión o la legislación de los Estados miembros que establecerán medidas adecuadas para proteger los intereses legítimos, y no por decisión de la autoridad de control. El Considerando 42 de la propuesta de Reglamento sí limita la finalidad de este tratamiento que debe ser la protección de otros derechos fundamentales «cuando así lo justifiquen razones de interés público, incluidas la sanidad pública, la protección social y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o para fines de investigación histórica, estadística y científica –cfr. *supra* V.C)–. En cambio, el art. 9 contempla ahora «los motivos importantes de interés público» en los tratamientos de datos especialmente protegidos relativos a condenas penales o medidas de seguridad afines –art. 9.2.j)–. Igualmente la propuesta de Reglamento mantiene la transferencia de datos a un tercer país o a una organización internacional en ausencia de una decisión de adecuación o de las garantías prevista en la propuesta de Reglamento «por motivos importantes de interés público –art. 44.1.d) –, una excepción también prevista en el art. 26.1.d) de la Directiva para «la salvaguarda de un interés público importante».

220. La Directiva establece también la posibilidad de limitar de forma justificada el derecho de acceso del interesado a sus datos personales cuando se vayan a tratar exclusivamente con fines de investigación científica o con fines estadísticos –art. 13.2–. Esta restricción es indeterminada, lo que permite diferencias de interpretación entre los distintos Estados.

pección o de supervisión relacionada, incluso ocasionalmente, con el ejercicio de la autoridad pública [...]; la protección de interesado o de los derechos y libertades de otras personas».

Por tanto, analizando las limitaciones al derecho fundamental a la protección de datos personales que se recogen en el art. 21 de la propuesta de Reglamento a la luz de los textos normativos ya citados, en la Unión Europea son finalidades legítimas que permiten limitar el derecho fundamental a la protección de los datos personales la seguridad del Estado y la defensa –lo que el CEDH llama seguridad nacional–, sin perjuicio de que en la propuesta de Reglamento desaparezcan estas referencias ya que no es de aplicación a la política exterior y de seguridad común ni la Carta de Derechos Fundamentales de la Unión Europea ni el TFUE, ni la propuesta de Reglamento, disponiendo el antiguo segundo pilar de una regulación específica en el art. 39 del TUE, que se desarrollará por decisión del Consejo; también es una finalidad legítima la seguridad pública y la persecución de infracciones penales –lo que el CEDH señala como defensa del orden y prevención del delito– que se mantienen en el art. 21.1.a) y b) de la propuesta de Reglamento –sin perjuicio de que esta materia se encontrará regulada por la propuesta de Directiva del Parlamento Europeo y del Consejo 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 la libre circulación de dichos datos–. Igualmente es una finalidad legítima la persecución de las infracciones de normas deontológicas en las profesiones reguladas, una referencia que no estaba prevista en el CEDH y cuya excepción se mantiene en el art. 211.d) de la propuesta de Reglamento, aunque diferenciándola de la relativa a la persecución de infracciones penales. Se mantiene en el art. 21.c) de la propuesta de Reglamento la limitación al derecho a la protección de datos personales en virtud de un interés económico y financiero importante de un Estado miembro o de la Unión en los ámbitos fiscal, presupuestario y monetario –lo que el CEDH calificaba como bienestar económico del país–, ampliándola no sólo a la protección de la estabilidad y la integridad de los mercados –lo que se justifica en el actual contexto de crisis económica– sino a otros intereses públicos de la Unión o de un Estado miembro, una cláusula indeterminada que no contemplaba la Directiva como excepción general a los principios y derechos de protección de datos, va más allá del CEDH –si bien en este punto el TEDH deja un amplio margen de configuración a los Estados– y no parece compatible con la jurisprudencia constitucional española establecida en la Sentencia 292/2000, de 30 de noviembre[221], aunque encajarían dentro de las limitaciones del

221. La LOPD –al igual que la LORTAD– citaba el interés público como excepción a los derechos de acceso, rectificación y cancelación cuando «ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección» –antiguo art. 24.2–. Sin embargo, este precepto fue declarado inconstitucional por la Sentencia 292/2000, de 30 de noviembre que consideraba que la expresión «interés público», como fundamento de la imposición de límites a los derechos

ejercicio de los derechos y libertades que «responden efectivamente a objetivos de interés general reconocidos por la Unión» previsto en el art. 52.1 de la Carta. Por último, la propuesta de Reglamento conserva las excepciones en relación con la función de inspección o de supervisión relacionada con el ejercicio de autoridad pública –art, 21,1,e)– y con la protección del interesado y con los derechos y libertades de otras personas –art. 21.1.f)–, lo que se encuadraría dentro de la previsión del CEDH relativa a la protección de los derechos y libertades de los demás y la protección de la salud o de la moral, y, en especial, en las limitaciones a los derechos que responden «a la necesidad de protección de los derechos y libertades de los demás» previsto en el art. 52.1 de la Carta, *in fine*–.

Estas finalidades legítimas que permiten establecer límites al derecho fundamental a la protección de los datos personales no sólo aparecen en el artículo de la propuesta de Reglamento titulado «limitaciones» –art 21–. Así, son distintas las excepciones a los principios y derechos de protección de datos que encuentran su justificación en las finalidades legítimas antes señaladas y que se encuentran desgranadas en todo el texto de la propuesta de Reglamento. Esto se manifiesta especialmente en los tratamientos de datos personales que llevan a cabo las Administraciones Públicas que se desarrollan para garantizar la efectividad de los derechos constitucionales[222]. Es cierto que la propuesta de Reglamento –siguiendo también en este punto la Directiva– no establece en un título

fundamentales del art. 18.1 y 4 CE encerraba un elevado grado de incertidumbre. El art. 9 del Convenio 108 y el art. 13 de la Directiva 95/46/CE sí justifican límites a estos derechos, por ejemplo, para la defensa del Estado, la seguridad pública, la protección de los derechos y libertades de terceros, la necesidad de las investigaciones o el cumplimiento de obligaciones tributarias, lo que recoge el art. 23 LOPD. Sin embargo, no habilitan la posibilidad de suprimir los derechos de acceso, rectificación y cancelación por razones de interés público o ante intereses de terceros más dignos de protección, que son dos cláusulas genéricas, que dejan libertad a la Administración para decidir qué actividad administrativa puede limitar estos derechos ya que toda ella está orientada al interés general –art. 103 CE–. Además estas limitaciones no están justificadas en la protección de otros derechos fundamentales y no respetan, por ello el principio de proporcionalidad. La interpretación del derecho a luz de la opinión generalmente admitida de lo que este derecho significa –teniendo en cuenta el art. 8 del Convenio 108 o el art. 12 de la Directiva– incluye los derechos de acceso, rectificación y cancelación como parte del contenido esencial del derecho fundamental a la protección de datos personales, sin los cuales este derecho no es reconocible como perteneciente a su tipo previo, como una facultad imprescindible sin cuyo ejercicio los intereses jurídicos que dan vida a este derecho resultan desprotegidos. Por ello, limitar el ejercicio de este derecho «por razones de interés público o ante intereses de terceros más dignos de protección» vulnera el contenido esencial del derecho fundamental a la protección de datos, imponiéndole restricciones injustificadas y desproporcionadas que lo hacen impracticable y lo despojan de su necesaria protección. Esta cuestión la hemos analizado en *La protección de datos personales*, cit. pp. 165-168.

222. El TEDH ha otorgado a los Estados un cierto «margen de apreciación» en relación a la legitimidad de la injerencia en la vida privada de las personas, especialmente cuando el supuesto afecte a temas de política general del Estado (social, económica, medio ambiente, planificación urbana y rural). Cfr. ARENAS RAMIRO, M., *op. cit*. pp. 122-130 y 140.

específico una regulación para los tratamientos de datos personales que llevan a cabo las Administraciones Públicas, a diferencia de la LOPD, que dentro del margen de maniobra que permitía la Directiva contenía disposiciones sectoriales específicas para los ficheros de titularidad pública –arts. 20-24–. Además, hay que destacar especialmente que la propuesta de Reglamento aplica las sanciones administrativas de naturaleza económica a los incumplimientos del Reglamento cualquiera que sea el carácter del responsable del tratamiento –sea una Administraciones Públicas o una empresa privada–[223], un planteamiento cuestionable que no beneficia directamente en nada al ciudadano y que va a alterar sustancialmente el régimen sancionador por infracciones de protección de datos personales a las Administraciones Públicas de nuestro país[224]. Sin embargo, la pro-

223. El Considerando 119 de la propuesta de Reglamento señala que «deben imponerse sanciones a aquellas personas, ya sean de Derecho público o privado, que no cumplan lo dispuesto en el presente Reglamento».

224. Las Administraciones Públicas en España han tenido hasta ahora un régimen de infracciones específico previsto en el art. 46 LOPD que tiene como consecuencia una Resolución del Director de la Agencia de Protección de Datos que declara la infracción o infracciones –muy grave, grave o leve–, el establecimiento de medidas para que cesen o se corrijan los efectos de la infracción, la notificación de la infracción no sólo al responsable sino también al órgano del que dependa jerárquicamente, a los afectados –si los hubiera– y al Defensor del Pueblo y la propuesta, en su caso, de inicio de actuaciones disciplinarias, que se rigen por el régimen disciplinario de las Administraciones Públicas. De esta forma, las infracciones cometidas por las Administraciones Públicas tienen como principal consecuencia la responsabilidad política –la dimisión o el cese del cargo público– y el coste político en términos de gestión pública –al hacerse eco de la Resolución los medios de comunicación y la Memoria anual del Defensor del Pueblo–, todo ello sin perjuicio de que el afectado ejercite su derecho a la indemnización del art. 19 LOPD por los daños o lesiones en sus bienes o derechos –como también puede hacer frente a los responsables de ficheros de titularidad privada–, lógicamente siguiendo el régimen de responsabilidad patrimonial de las Administraciones Públicas. Este planteamiento del legislador era coherente. La ausencia de sanción económica para las Administraciones Públicas tiene en cuenta que ésta no es abonada por los cargos políticos o por los funcionarios responsables de la infracción –que no tienen ninguna reducción en sus ingresos– sino por la propia Administración, lo que supone en la práctica la imposibilidad de ejecutar otras actuaciones administrativas ya presupuestadas que puedan beneficiar al ciudadano o una modificación o redistribución de créditos de distintos programas presupuestarios de las Administraciones Públicas, que van al programa presupuestario de la Agencia –de cuyo remanente de tesorería se nutren las Administraciones sancionadas si son del mismo nivel territorial–, todo ello sin ninguna ventaja para el ciudadano. En cambio, las sanciones económicas frente a un responsable privado alcanzan un pleno sentido punitivo porque es la empresa que pretendía obtener un beneficio económico por los tratamientos de datos personales quien debe asumir el pago de la sanción económica. Hay que tener en cuenta que en el ámbito de la Administración Pública las infracciones no son consecuencia de un interés económico sino de una deficiente gestión pública o de una búsqueda de una rentabilidad política, por lo que la sanción debe estar centrada en el coste político. Hay que tener en cuenta, y esto frecuentemente se olvida, que las sanciones establecidas por las autoridades de control son incorporadas al fondo de tesorería de la Agencia y no son cobradas por los sujetos perjudicados. No obstante, el art. 19 LOPD reconoce un derecho a la indemnización por el daño o lesión en los bienes o derechos ocasionados por un incumplimiento de las previsiones de esta Ley y que se ejerce tanto ante los responsable de ficheros públicos como privados, cada

puesta de Reglamento, al igual que la Directiva 95/46CE, tiene en cuenta que el desarrollo de muchas funciones administrativas que tratan de garantizar bienes constitucionales y que justifican determinadas facultades y prerrogativas de las Administraciones Públicas también demanda una regulación específica que adapte los principios y derechos de protección de datos en este ámbito[225]

Así, se mantienen en la propuesta de Reglamento las excepciones a los principios y a los derechos de protección de datos personales que estaban presentes en la Directiva para los tratamientos de datos personales que llevan a cabo las Administraciones Públicas dentro de las finalidades legítimas antes señaladas. La propuesta de Reglamento conserva los supuestos de legitimidad del tratamiento de datos personales sin consentimiento del interesado que se recogían en el art. 7.c) y e) de la Directiva, como es que el «cumplimiento de una misión de interés público o inherente al ejercicio de poder público conferido al responsable del tratamiento» –art. 6.1.e)–, así como el cumplimiento de una obligación jurídica a la que esté sujeta el responsable del tratamiento –art. 6.1.c)–, si bien la propuesta de Reglamento añade una importante novedad que no se encontraba en la Directiva: tanto la misión de interés público o inherente al ejercicio de poder público como la obligación jurídica deben estar establecidas en el Derecho de la Unión o en la legislación del Estado, que debe cumplir un objetivo de interés público o ser necesaria para proteger los derechos y libertades de terceros –art. 6.3–[226]. Hasta ahora, la mayoría de las leyes nacionales habían transpuesto la Directiva estableciendo como principio para la legitimación del tratamiento que éste sea necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, es decir, en los mismos términos que el art. 7.e) de la Directiva sin una mayor precisión. Como señala el Considerando 32 de la Directiva, corresponde a las legislaciones nacionales determinar si el responsable del tratamiento que tiene conferida una misión de interés público o inherente al ejercicio del poder público debe ser una Administración Pública u otra persona de derecho público o privado, como por ejemplo una asociación profesional. También la mayoría

---

uno en su orden jurisdiccional específico –jurisdicción contencioso-administrativa o jurisdicción civil, respectivamente–.

225. Hemos señalado en distintas ocasiones que el derecho a la protección de datos de los ciudadanos tiene contenidos distintos frente a tratamientos realizados por las Administraciones Públicas y por los particulares. Así, existe un menor derecho a la protección de los datos de carácter personal frente a los responsables de ficheros públicos ya que en este caso es necesario hacer un *balancing* constitucional entre este derecho y la vertiente objetiva de otros derechos fundamentales que exigen que se lleve a cabo un tratamiento de datos personales. La diferencia esencial entre lo público y lo privado en ese ámbito y la necesidad de una regulación específica de la protección de datos personales para las Administraciones Públicas la hemos realizado en *La protección de datos personales*, cit. pp. 263-288.

226. Llama la atención que la propuesta de Reglamento sólo establezca para la legislación del Estado y no para el Derecho de la Unión el deber de cumplir un objetivo de interés público o ser necesaria para proteger los derechos y libertades de terceros.

de Estados permiten el tratamiento de datos personales sin consentimiento del interesado cuando sea necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público, sin exigir que esta concreta función administrativa se encuentre establecida por Ley. En cambio, otros Estados han sido más restrictivos ya que sólo han permitido los tratamientos siempre que esta función pública se encuentre prevista en una Ley o normativa aprobada en virtud de una Ley, que establezca las tareas y las funciones[227]. En España, como es sabido, la LOPD permite el tratamiento de datos personales sin consentimiento del interesado «para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias» –art. 6.2–[228]

227. Cfr. *Analysis and impact study on the implementation of Directive*, cit. ARENAS RAMIRO, M., cita como excepción el caso de Letonia y Polonia donde se exige que la misión de interés público se encuentre expresamente recogida en una Ley.

228. La LOPD no hace referencia expresa al «interés público» –salvo en el antiguo art. 24.2 ya analizado– sino que ha preferido la expresión «funciones propias de las Administraciones públicas en el ámbito de sus competencias» para permitir los tratamientos de datos personales sin consentimiento –y que no pueden suponer un límite al derecho de acceso–. Hay que tener en cuenta que la actividad de las Administraciones Públicas en el ejercicio de sus competencias –la misión de interés público–, que sí justifica la legitimidad del tratamiento y de las cesiones sin consentimiento del interesado, no sirve para limitar los derechos de acceso, rectificación y cancelación como tampoco sirve para exceptuar el principio de información. Así, la STC 292/2000, de 30 de noviembre, declaró inconstitucional la excepción del principio de información al afectado en la recogida de datos cuando ésta «impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas» o «afecte a la persecución de infracciones administrativas yart. 24.1 LOPDa. Así, es legítimo la excepción del principio de información cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales, que se mantienen en el art. 24.1 LOPD y que sí tenían acogida entre las excepciones previstas el art. 9 del Convenio 108 y en el art. 13 de la Directiva 95/46 CE. En cambio la excepción del principio de información cuando impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la persecución de infracciones administrativas no tenía cobertura en el art. 9 del Convenio 18, ni tampoco en el art. 13 de la Directiva 95/46/CE, que curiosamente sí admitía la excepción del principio de información para la salvaguarda de «una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública» en la prevención, investigación, detección y la represión de las infracciones de la deontología en las profesiones reglamentadas –art. 13.1.f) en relación con el art. 13.1.d)–, lo que se mantiene la propuesta de Reglamento –art. 21.1.d) y e)–. Ya hemos criticado en otro momento que no parece razonable que las infracciones deontológicas dispongan de una posición privilegiada en relación con las infracciones administrativas, algo que ha corregido la propuesta de Reglamento si entendemos que la persecución de las infracciones administrativas es un interés público de la Unión, sin limitar éste a los intereses económicos y financieros –art. 21.1.c) de la propuesta de Reglamento–. En todo caso, lo que hay que resaltar aquí es que esta excepción al principio de información del art. 24.1 LOPD, al igual que ocurría con las excepciones a los derechos ya analizadas recogidas en el art. 24.2de la LOPD, era tan genérica que adolecía de falta de previsibilidad ya que toda actividad administrativa que implique una relación jurídica con el administrado conllevaría la posibilidad de llevar a cabo una función de verificación y control de que éste ha actuado de conformidad con el régimen jurídico, lo que atribuiría a la Administración la facultad de denegar la información al interesado –con mayor

sin que se exija una previsión legal específica, si bien el RPDP ha añadido recientemente que estas funciones deben estar atribuidas por una norma con rango de ley o una norma de derecho comunitario» –art. 10.3–. Esto es algo innecesario para la mayoría de las Administraciones de los Estados que están vinculadas al principio de legalidad y ejercen sus competencias constitucionales dentro de la reserva de Administración –*verwaltungsvorbehalt*–[229] lo que implica que sus Administraciones Públicas sólo pueden actuar habilitadas por una Ley que describe sus funciones y competencias de manera general pero con una amplia colaboración reglamentaria. Nuestra Constitución reconoce expresamente el principio de legalidad y de interdicción de la arbitrariedad de los poderes –art. 9.3– y obliga a las Administraciones Públicas a actuar con sometimiento pleno a la Ley y al Derecho –art. 103.1–. Por tanto, una cosa es que la misión de interés público o el cumplimiento de una obligación jurídica como fundamentos jurídico del tratamiento estén previstos en la legislación del Estado o en el Derecho de la Unión –que exista una cobertura legal de las competencias y funciones de las Administraciones Públicas– y otra cosa distinta es que la legislación del Estado o el Derecho de la Unión tenga necesariamente que prever la existencia de un tratamiento de datos personales sin consentimiento, lo que es claramente innecesario[230]. La habilitación legal de las competencias administrativas da suficiente cobertura a los tratamientos de datos personales sin consentimiento[231]. No obstante, la precisión del concreto tratamiento

gravedad ahora si entendiéramos que se puede exceptuar el principio de información cuando haya un interés público–. Por ello, hay que señalar que el principio de información, al igual que los derechos de acceso, rectificación y cancelación, es una de las garantías esenciales de este derecho fundamental, que forma parte de su naturaleza jurídica y que lo hace reconocible como perteneciente a su tipo previo y su restricción elimina una de sus facultades esenciales, lo que ocasiona que los intereses jurídicos que le dan vida queden desprotegidos, afectando gravemente al contenido esencial de derecho fundamental. De hecho, el principio de información es una garantía esencial del derecho fundamental a la protección de datos personales en las Administraciones Públicas donde los tratamientos de datos personales se hacen sin consentimiento del interesado y donde sólo el principio de información permite dar a conocer al interesado la existencia de un tratamiento con sus datos personales y facilita el ejercicio de los derechos de acceso, rectificación y cancelación –cfr. *La protección de datos personales*, cit. pp. 162-165–.

229. Sobre la reserva de Administración, cfr. TRONCOSO REIGADA, A., *Privatización, empresa pública y Constitución*, Marcial Pons, Madrid, 1997, pp. 130-135; y DREIER, H., «Zur Eigeständigkeit der Verwaltung», *Die Verwaltung*, nº 25-2, 1992, pp. 137-156.

230. El Considerando 31 de la propuesta de Reglamento señala que «para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento de la persona interesada o sobre alguna otra base legítima establecida por ley, ya sea en el presente Reglamento ya sea en otros actos legislativos del Estado miembro o de la Unión referidos en el presente Reglamento», por lo que el propio Reglamento podría ser una base legítima suficiente.

231. De hecho, el art. 6 de la propuesta de Reglamento –al igual que hacía el art. 7 de la Directiva 95/46/CE– diferencia la licitud del tratamiento para el cumplimiento de una obligación jurídica a la que está sujeto el responsable –c)–, del tratamiento que es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento-e)–. Hay que tener en cuenta, además, que el art. 33.5 exime de la obligación de llevar a cabo una evaluación

que lleve a cabo una Administración Pública debe hacerse a través de disposiciones de carácter general –como estaba previsto en el art. 20 LOPD– que establezcan la finalidad del tratamiento y las personas sobre las que se pretenda obtener los datos, una obligación que es consecuencia del sometimiento de la Administración Pública al principio de legalidad y que subsiste aunque desaparezca la obligación de notificación de los tratamientos[232]. Además, no tiene sentido una interpretación estricta de la propuesta de Reglamento para exigir que la excep-

---

de impacto en los tratamientos de datos personales «cuando el responsable del tratamiento sea una autoridad u organismo público y cuando el tratamiento se efectúe en cumplimiento de una obligación legal de conformidad con lo dispuesto en el art. 6.1.c)», lo que implica la concurrencia de dos elementos inicialmente distintos.

232. Hay que recordar que la LOPD también permitía la comunicación de datos entre Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas «cuando la comunicación hubiera sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso» –antiguo art. 21.1–. Este apartado fue declarado inconstitucional por la STC 292/2000, de 30 de noviembre, de manera que se exige que exista una Ley para entender legítima la cesión, salvo que la comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias –art. 10.4.c) RPDP–. Sin embargo, la Administración Pública actúa siempre vinculada positivamente a la ley y al Derecho –*positive bindung*– y sometida al principio de legalidad administrativa por lo que, a nuestro juicio, la cesión puede hacerse en virtud de competencias administrativas que dispongan de una suficiente habilitación legal o de la necesidad de cumplir un deber que impone una Ley, no siendo necesario que la ley autorice expresamente la comunicación de datos personales. Esto no impide criticar al legislador por haber previsto una cesión en virtud de normas reglamentarias, sin exigir que éstas delimiten las causas que la justifican, y sin hacer mención a la vigencia en la comunicación de datos personales entre Administraciones Públicas del principio de información y del principio de calidad, finalidad y proporcionalidad. En todo caso, no tiene mucho sentido exigir la habilitación legal para la cesión al mismo tiempo que se reputa como legítimo el tratamiento de datos personales sin consentimiento para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias –art. 6.2 LOPD–. De hecho, da la impresión de que el artículo 6.2 de la LOPD y el texto inicial del art. 21.1 LOPD declarado inconstitucional eran correcta transposición del art. 7.e) de la Directiva 95/46/CE, al considerar legítimos «los tratamientos de datos sin consentimiento para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento *o a un tercero a quien se comuniquen los datos*», mientras que el art. 11 LOPD –a la luz de la STJUE, de 24.11.2011, ya analizada– y el artículo 21.1 –después de la STC 292/2000, de 30 de noviembre– son demasiado restrictivos. Hay que tener en cuenta también la crítica que la Comisión Europea –ver nota 81– ha realizado a la transposición de la Directiva realizada en la legislación española, por dificultar las cesiones al regularlas de manera específica y diferenciarlas de los tratamientos, algo que no hacía la Directiva ni tampoco ahora la propuesta de Reglamento. Por ello, si el Convenio 108 y la Directiva 95/46/CE no exigían una habilitación legal para la cesión de datos entre Administraciones Públicas, no se entiende la interpretación del art. 18,4 CE que hizo la STC 292/2000, de 30 de noviembre para poder llegar a afirmar la inconstitucionalidad del artículo 21.1 LOPD en virtud de la doctrina del contenido esencial de los derechos fundamentales y de la referencia a la noción generalmente admitida por los juristas y en el Derecho comparado de lo que este derecho significa. Cfr. la crítica a esta Sentencia en *La protección de datos personales*, cit. pp. 143-162. Cfr. también nuestra trabajo «La comunicación de datos personales», *loc. cit.* pp. 963-997.

ción del consentimiento para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable se encuentre prevista en el Derecho de la Unión o en la legislación del Estado miembro, porque la propuesta de Reglamento permite los tratamientos y las cesiones cuando son necesarios para la satisfacción de un interés legítimo del responsable y no prevalezcan los derechos y libertades de los interesados –art. 6.1f)–, sin requerir ningún fundamento jurídico alguno[233]. Hay que señalar que también la propuesta de Reglamento conserva la posibilidad de llevar a cabo una transferencia de datos personales a terceros países u organizaciones internacionales sin las garantías ya analizadas cuando concurran motivos importantes de interés público –art. 44.1.d–, interés público –y no la concreta transferencia– que debe estar reconocido por el Derecho de la Unión o del Estado miembro a que esté sujeto el responsable del tratamiento –art. 44.5–[234]. La propuesta de Reglamento también establece algunos beneficios procesales para las Administraciones Públicas. Así, señala que cuando el responsable del tratamiento sea una autoridad pública en el ejercicio de un poder público, el interesado no tiene la facultad de elección del órgano jurisdiccional en el que tenga su residencia sino que tiene que interponer el recurso judicial en el Estado miembro en el que la Administración Pública tenga su residencia –art. 75–. No obstante, no todo son ventajas para las Administraciones Públicas sino que éstas también están sometidas a obligaciones específicas, como es la obligación de designar un delegado de protección de datos –art. 35.1.a)–. Se trata de acentuar las garantías, permitiendo al mismo tiempo el desarrollo normal de la actividad administrativa en beneficio del interés general, que requiere ordinariamente los tratamientos de datos personales sin consentimiento del interesado.

La protección de los derechos y libertades de otras personas es otra finalidad legítima que permite establecer límites a los principios y derechos de protección de datos –art. 21.1.f)–, lo que también se manifiesta en distintos apartados de la propuesta de Reglamento. El derecho a la protección de datos personales, como ha señalado el TJUE, «no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el

233. Esta previsión podría ser aplicable a las Administraciones Públicas ya que no hay un interés legítimo mayor por antonomasia que el interés público –el interés general–. Sin embargo, el art. 6.1.f) *in fine* de la propuesta de Reglamento señala expresamente que no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

234. También la propuesta de Reglamento permite la transferencia cuando sea necesaria para el reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial –art. 44.1.e)–. Esta excepción junto con la realizada por motivos de interés público se contenían ya en el art. 26.1.d) de la Directiva 95/46/CE. La LOPD especificaba que tenía el carácter de interés público la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias» –art. 34.h)–, a lo que añade como ejemplos la propuesta de Reglamento las transferencias entre servicios competentes en materia de seguridad social o de gestión de la pesca, sin requerir en estos casos otra fundamentación jurídica específica como la prevista en el art. 6.3 de la propuesta de Reglamento.

equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad»[235]. Así, poniendo sólo algunos ejemplos, el derecho a la protección a la salud, como bien constitucional individual –que implica la asistencia sanitaria– y colectivo –que alcanza la salud pública– requiere la existencia de tratamientos de datos especialmente protegidos sin consentimiento –art. 81 de la propuesta de Reglamento–, también con fines de investigación. De hecho, la regulación de la protección de datos personales no puede suponer una traba para uno de los objetivos de la Unión Europea, que es realizar un espacio europeo de investigación –art. 179.1 TFUE–[236]. La libertad de empresa justifica

235. Cfr. el Considerando 139 de la propuesta de Reglamento, donde se cita la voluntad del presente Reglamento de observar otros derechos reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea, como la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa o el derecho a la tutela judicial efectiva. Igualmente, los Elementos jurídicos de la propuesta de Reglamento –en concreto el apdo. 3.3 que contiene el «Resumen de las cuestiones relativas a los derechos fundamentales»– señala que otros derechos fundamentales potencialmente afectados y consagrados en la Carta son la libertad de expresión, la libertad de empresa, el derecho a la propiedad y, especialmente, la protección de la propiedad intelectual, la prohibición de toda discriminación, y, en particular, la ejercida por razón de raza, orígenes étnicos, características genéticas, religión o convicciones, opiniones políticas o de cualquier otro tipo, discapacidad u orientación sexual, los derechos del menor, el derecho a un alto nivel de protección de la salud humana, el derecho de acceso a los documentos o el derecho a la tutela judicial efectiva y a un juez imparcial.

236. La propuesta de Reglamento aborda con acierto los tratamientos para fines de investigación histórica, estadística y científica –dentro de la investigación científica, el Considerando 126 incluye investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado–. Así, se permite la conservación de datos para periodos más largos siempre que se traten exclusivamente para fines de investigación –art. 5–, señalando, además, la licitud de estos tratamientos sin consentimiento sometidos a unas condiciones establecidas en el art. 83. La primera condición a la que tienen que someterse los tratamientos con fines de investigación histórica, estadística o científica es el respeto al principio de calidad. Así, sólo puede hacerse la investigación con datos personales si no es posible hacerla de otro modo, siendo necesario que los datos personales se conserven por separado –que exista una disociación reversible– siempre que los fines puedan alcanzarse, cuestiones que ya se recogían en la Ley 14/2007, de 3 de julio, de Investigación Biomédica. La segunda condición es el respeto al consentimiento del interesado en la publicación de los datos personales en las investigaciones, salvo que este los haya hecho ya públicos o que la publicación sea necesaria para presentar los resultados de la investigación y para facilitarla, siempre que no prevalezcan los derechos del interesado. En todo caso, merece la pena resaltar las posibilidades que brinda para los tratamientos de datos personales sin consentimiento en el ámbito de la investigación biomédica el art. 7.f) de la Directiva 95/46, que tiene, como ya hemos visto, efecto directo, y que establece que el tratamiento de datos personales es lícito si 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. La actividad investigadora en el sector sanitario, tanto en el ámbito del propio responsable como las cesiones que se produzcan en el marco de una investigación en red, suponen la persecución de un interés legítimo y pueden prevalecer cuando se lleva a cabo una ponderación de los distintos derechos, sobre todo, cuando se tratan o se ceden datos codificados o reversiblemente disociados, cuando haya un

asimismo el tratamiento sin consentimiento de datos del interesado para la satisfacción de un interés legítimo del responsable del tratamiento –art. 6.1.f) de la propuesta de Reglamento–. La libertad religiosa exige la excepción del consentimiento para el tratamiento y para la conservación de datos especialmente protegidos –at. 85 de la propuesta de Reglamento–. El derecho a la tutela judicial efectiva también justifica el tratamiento de datos especialmente protegidos –art. 9.2.f) y las transferencias internacionales –art. 44.1.e)–. Los derechos de propiedad intelectual, los derechos de autor y el secreto industrial también suponen un límite al derecho al acceso a los propios datos personales cuyo ejercicio «no puede afectar negativamente a los derechos» –Considerando 51 de la propuesta de Reglamento–, etc.[237].

Este sería también el caso de la libertad de expresión, que justifica un régimen específico para los tratamientos de datos personales con fines periodísticos o de expresión literaria o artística que contemplan tanto el art. 80 de la propuesta de Reglamento como el art. 9 de la Directiva y que merece una atención más específica[238]. La libertad de expresión, especialmente cuando se efectúa con fines periodísticos, ha sido considerada tradicionalmente como una libertad preferente –un *primus inter pares*–[239] ya que este valor procedimental

---

informe favorable del Comité de ética de la investigación o cuando sea una investigación de interés general y no sea posible hacerla de otra forma, criterios estos que están presentes en el art. 58.3 de la Ley de 14/2007, de 3 de julio, de Investigación Biomédica.

237. Esta previsión se contenía antes en el Considerando 41 de la Directiva 95/46/CE–. Así, unos de los motivos del rechazo al derecho de acceso a los datos personales en EEUU es la protección de la propiedad intelectual y el derecho de autor en relación con el programa informático. En otros momentos hemos analizado los supuestos en los que el respeto a los derechos fundamentales supone un límite a la protección de datos personales, como aquellos otros donde la protección de datos personales es una garantía institucional de otros derechos fundamentales.

238. Hay que valorar también el interés que ha mostrado por esta cuestión la Comisaria Europea de Justicia, Viviane Reding, que es periodista.

239. Así, el Tribunal Constitucional ha señalado, en Sentencia 171/1990, de 12 de noviembre, que: «Dada su función institucional, cuando se produzca una colisión de la libertad de información con el derecho a la intimidad y al honor aquélla goza, en general, de una posición preferente y las restricciones que de dicho conflicto puedan derivarse a la libertad de información deben interpretarse de tal modo que el contenido fundamental del derecho a la información no resulte, dada su jerarquía institucional desnaturalizado ni incorrectamente relativizado. En todo caso, el Tribunal Constitucional en la Sentencia 336/1993, de 15 de noviembre, sostiene en lo relativo a las relaciones entre la libertad de expresión y los derechos reconocidos en el art. 18 CE que «la ponderación entre los derechos constitucionales en conflicto requiere que se tenga en cuenta la posición prevalente –aunque no jerárquica– que respecto al consagrado en el art. 18.1 CE ocupan los derechos a la libre comunicación de información y a la libertad de expresión del art. 20.1 C.E. cuando su ejercicio tiene lugar dentro del ámbito constitucionalmente protegido, dado que éstos constituyen no sólo libertades individuales de cada ciudadano sino también la «garantía institucional de una opinión pública indisolublemente unida al pluralismo democrático». La jurisprudencia del Tribunal Constitucional ha señalado que la libertad de información ocupa una posición prevalente cuando se ejercita por un *medio institucionalizado de creación de la opinión pública* –cuestión importante, como veremos después–; existe veracidad subjetiva –en

es básico para alcanzar una opinión pública libre, condición indispensable para una auténtica sociedad democrática y para limitar el poder[240]. La preferencia de la libertad de información sobre el derecho a la protección de datos personales es también una consecuencia lógica de la libertad ideológica, del valor pluralismo político y, en definitiva, del principio democrático. Esta preferencia de la libertad de información sobre la protección de datos personales también facilita la necesaria transparencia administrativa y la publicidad de la información administrativa aunque ésta contenga datos personales[241]. Así, el art. 80 de la pro-

---

el concepto desarrollado por el Tribunal Constitucional de buena praxis profesional del informador que le obliga a comprobar y contrastar de modo diligente los hechos sobre los que versa la información con carácter previo a su difusión (SSTC 6/1988, de 21 de enero; 105/1990, de 6 de junio; 240/1992, de 21 de diciembre y 61/2004, de 19 de abril)–; se trata de asuntos públicos que son de interés general por las materias a las que se refieren o por las personas que intervienen y contribuye a la formación de la opinión pública (SSTC 105/1983, de 23 de noviembre; 107/1988, de 8 de junio; 132/1995, de 11 de septiembre); y las informaciones vertidas no incluyan expresiones injuriosas, vejatorias o insultos, que además son innecesarios para el mensaje que se quiere transmitir, aunque la Constitución no prohíba las expresiones hirientes, molestas o desabridas (STC 112/2000, de 5 de mayo, 49/2001, de 26 de febrero y 110/2000, de 5 de mayo).

240. Véase en esta dirección a ELY, que justifica el activismo procedimental Vla preferencia de los valores procedimentales sobre los sustantivosl y representa una justificación dogmática de la jurisprudencia Warren. Cfr. ELY, J. H., *Democracy and distrust. A Theory of Judicial Review*, Harvard University Press, Massachussets, 1980, pp. 43-72; ARAGÓN, M., Aragón, *Constitución y democracia*, Tecnos, Madrid, 1990. Cfr. TRONCOSO REIGADA, A., «Método jurídico, interpretación constitucional y principio democrático», en ESPÍN, E., y DÍAZ REVORIO, F. J., *La justicia constitucional en el Estado democrático*, Tirant lo Blanch, Valencia, 2000, pp. 450-454.

241. El acceso a información pública, además de ser elemento necesario para el ejercicio del derecho fundamental a la participación en asuntos públicos del art. 23 CE –otro valor procedimental imprescindible en una sociedad democrática–, es una exigencia en muchas ocasiones del derecho a comunicar o recibir información veraz por cualquier medio de difusión –art. 20.1.d) CE–, entendido no sólo como un derecho a recibir información a través de los medios de comunicación, sino como un derecho a recibir toda la información accesible al público en general. Existe, a nuestro juicio, una clara conexión entre el derecho a comunicar y recibir información veraz y la garantía institucional de una opinión pública libre, que exigen la búsqueda y la comprobación de la información, con el derecho de acceso a los archivos y registros administrativos, especialmente cuando la solicitud de información administrativa la desarrollan medios de comunicación social. En este caso, el derecho de acceso a información administrativa por los medios de comunicación sería una garantía de la propia libertad de información. De esta forma, el art. 20.1.d) CE no sólo prohíbe que el Estado interfiera en la recepción de la información por parte de los ciudadanos ino sólo sería un derecho de libertad que implicaría el respeto a la actividad de los medios de comunicaciónn, sino que establece una obligación a los poderes públicos de facilitar al público el libre acceso a la información administrativa ,tendría una clara dimensión prestacional que obligaría a proporcionar información–. Obviamente, no siempre las solicitudes de acceso de los ciudadanos están vinculados a la existencia de una opinión pública libre o de una sociedad democrática ílo que sí ocurre en el caso de los medios de comunicacióne ya que en muchas ocasiones se trata de un acceso instrumental para el ejercicio de otros derechos. En todo caso, el acceso a fuentes administrativas es más importante para configurar una opinión pública libre y una

puesta de Reglamento permite a los Estados miembros disponer de exenciones o excepciones a los principios y derechos de protección de datos, a las obligaciones del responsable y del encargado, a la regulación de las transferencias de datos personales e incluso, a las competencias de las autoridades de control y a los mecanismos de cooperación y de coherencia «en el referente al tratamiento de datos personales efectuado exclusivamente con fines periodísticos o de expresión literaria o artística, para conciliar el derecho a la protección de datos personales con las normas que rigen la libertad de expresión»[242]. De esta forma,

---

sociedad democrática avanzada por estar estrechamente vinculada a los procesos de participación políticap que la prevalencia de la libertad de expresión sobre el derecho al honor y a la intimidad de las personas en otros ámbitos, como aquellos de los que se ocupa la llamada «prensa del corazón». Sin embargo, el Tribunal Supremo en la Sentencia de 19 de mayo de 2003, que analizó la denegación del ejercicio del derecho de acceso de un periodista del Diario *El Mundo* a un expediente administrativo relativo a los créditos FAD concedidos a la empresa pública FOCOEX, ratificó la Sentencia de la Audiencia Nacional afirmando que el art. 20.1.d) –que el recurrente había invocado a través del procedimiento de amparo contencioso– no puede confundirse con el derecho de acceso a archivos y registros administrativos del art. 105.b) CE. Hasta ahora el Tribunal Constitucional ha señalado en la Sentencia 161/1988, de 20 de septiembre, que las reglas y principios contenidos, entre otros, en el art. 105.b) de la Constitución «son inadecuadas para fundamentar una petición de amparo en cuanto que en ninguno de ellos se reconocen derechos fundamentales y libertades políticas de los incluidos como amparables en el artículo 53.2 de la Constitución». En todo caso, el derecho de acceso a información administrativa, aun considerado como derecho constitucional diferente de la libertad de información, tiene un carácter de libertad preferente o*preferred freedoms*>, al ser un valor procedimental necesario para una sociedad abierta y para el funcionamiento de un Estado democrático. Como señaló Ely, los valores procedimentales ,entre los que podríamos incluir el acceso a la información públicae tienen preferencia sobre los valores sustantivos, ya que estos valores procedimentales, al permitir mantener abiertos los canales de participación, contribuyen a que los valores sustantivos sean reflejo de la voluntad general. Cfr. más ampliamente sobre la cuestión VILLAVERDE MENÉNDEZ, I., *Estado democrático e información. El derecho a ser informado y la Constitución Española de 1978*, Junta General del Principado de Asturias, Oviedo, 1995, y *Los derechos del público*, Tecnos, Madrid, 1995. Cfr. también FERNÁNDEZ RAMOS, S., *El derecho de acceso a los documentos administrativos*, Marcial Pons, Madrid, 1997, pp. 350-357; POMED SÁNCHEZ, L. S., *El acceso de los ciudadanos a los archivos y registros administrativos*, INAP, Madrid, 1989; MESTRE DELGADO, J. F., *El derecho de acceso a archivos y registros administrativos*, Civitas, Madrid, 1993. Cfr. más recientemente el interesante trabajo de GUICHOT, E., *Transparencia y acceso a la información en el Derecho Europeo*, Editorial Derecho Global, Sevilla. 2010, pp. 154-181. Sin embargo, la STJCE, de 16.12.2008, as. *Satakunnan Markkinapörssi y Satamedia* (C-73/07, Rec. 2008, p. I-9831) señala que la publicación en forma de catálogo de los datos fiscales de ciudadanos finlandeses, incluidos los datos sobre sus ingresos y patrimonio, si se trata de datos procedentes de documentos públicos, puede considerarse una actividad periodística si su finalidad es divulgar al público información, opiniones o ideas por cualquier medio de transmisión.

242. Cfr. PAISSAN, M., *Privacy e giornalismo*, Garante per la protezione dei dati personali, 2003, esp. pp. 17-47. Cfr. COTINO HUESO, L., «Datos personales y libertades informativas. Medios de comunicación social como fuentes accesibles al público» y ARIAS MÁIZ, V., «Una excepción al principio de consentimiento informado no contemplada en el art. 6 LOPD: el uso de datos personales por medios de comunicación», ambos en *Comentarios*, cit. pp. 295-322 y 560-577, respectivamente; CAZURRO BARAHONA, V., *El*

el reconocimiento del derecho al olvido en Internet, que obliga al responsable del tratamiento a suprimir los datos sin demora, se encuentra limitado por el ejercicio de la libertad de expresión que permite la conservación de los datos personales –art. 17.3.a) de la propuesta de Reglamento–, lo que supone la continuidad de la publicación de la información en medios de comunicación digitales. También la Directiva 95/46/CE había establecido una restricción importante del derecho fundamental a la protección de datos personales en beneficio de la libertad de información y de expresión cuando el tratamiento de datos personales tenga fines periodísticos o de expresión artística o literaria. Así, los Considerandos 17 y 37 de la Directiva señalan que los principios de la misma deben ser aplicados de forma restringida o pueden justificarse excepciones cuando estemos en presencia de tratamientos de datos personales, incluido de sonido o imágenes, aplicados con fines periodísticos o de expresión literaria o artística, en particular en el sector audiovisual, siempre que esto sea necesario para conciliar los derechos fundamentales de la persona con la libertad de expresión y, en particular, la libertad de recibir o comunicar informaciones garantizado en el art. 10 del CEDH[243]. Corresponde a los Estados ponderar el derecho fundamental a la protección de datos y la libertad de expresión y de información, estableciendo las excepciones o restricciones necesarias a la legislación de protección de datos que permitan el ejercicio de estos derechos. Así, en esta dirección el art. 9 de la Directiva *«Tratamiento de datos personales y libertad de expresión»* establece que «[e]n lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión». Así, también en virtud de la Directiva 95/46/CE no puede exigirse el consentimiento del interesado para el tratamiento de sus datos personales –también de su imagen y sonido– o para la cesión o publicación de la información –de ahí también el límite al derecho al olvido y a la supresión– cuando éstas se llevan a cabo exclusivamente con fines periodísticos o de expresión literaria o artística. Estas excepciones previstas en las leyes de los países europeos podrían afectar también, como señalan los Considerandos de la Directiva, por ejemplo, a las transferencias de datos a terceros países o a las competencias de las autoridades de control.

Este es uno de los ámbitos donde, a juicio de la Comisión, *«least convergence can be discernid»*[244]. A pesar de ello, la propuesta de Reglamento respeta

---

principio de calidad en los tratamientos de datos personales en los medios de comunicación, tesis doctoral, Universidad de Valladolid, 2012.

243. La Memoria explicativa sobre el Convenio 108 señala la libertad de expresión como uno de «los derechos y libertades de los demás», para cuya protección los legisladores nacionales, de conformidad con lo dispuesto en la letra b) del apartado 2, del artículo 9 del Convenio, pueden apartarse de los principios básicos de la protección de datos.

244. Cfr. *Analysis and impact study on the implementation of Directive*. cit .. La Recomendación 1/1997, de 27 de febrero, del Grupo de Trabajo del Artículo 29 sobre la normativa de protección de datos y los medios de comunicación señalaba que en aquel momento las diferentes legislaciones nacionales habían abordado la cuestión con arreglo a uno

el amplio margen de maniobra que la Directiva concedía a los Estados al ser una cuestión nuclear del Estado constitucional, correspondiéndoles a los Estados miembros establecer las excepciones a los principios y derechos de protección de datos en este ámbito con la finalidad de conceder una protección preferente a la libertad de expresión y de información, quedando obligados a notificar a la Comisión las disposiciones legislativas que se adopten para establecer estas excepciones –art. 80.2 de la propuesta de Reglamento–. Así, por ejemplo, la LOPD no hace ninguna referencia a los tratamientos de datos personales para el ejercicio de la libertad de información y de expresión –no establece un régimen de excepciones a la aplicación de la normativa de protección de datos en relación con los tratamientos con fines periodísticos–, conteniendo únicamente previsiones relativas a la publicación de datos personales por los medios de comunicación social a los que atribuye el carácter de fuente accesible al público[245] por lo que no es necesario el consentimiento del interesado para el tratamiento y para la cesión –arts. 6.2 y 11.2.b)–. El hecho de que la LOPD no mencione los tratamientos de datos personales llevados a cabo por los medios de comunicación no significa que éstos tratamientos se encuentren excluidos del ámbito de aplicación de la legislación[246]. Hay que señalar que en España no hay ninguna Ley que tenga como objeto específico regular la libertad de información .aunque sí se aprobó tempranamente 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 . La ausencia de regulación de la libertad de información y de expresión es consecuencia de una voluntad consciente del legislador de no limitar en exceso el ejercicio de este derecho fundamental, dejando la definición de sus límites a la doctrina del Tribunal Constitucional y la resolución de los conflictos a la jurisdicción ordinaria. En todo caso, la propia Constitución Española, al tiempo que reconoce la libertad de expresión y de

---

de los enfoques siguientes: «a) En algunos casos, la normativa relativa a la protección de datos no contempla exención expresa alguna de la aplicación de sus disposiciones para los medios de comunicación. Tal es la situación actual en Bélgica, Portugal, Suecia, Reino Unido y España [en nuestro país, tal como hemos visto, los medios de comunicación son contemplados como fuentes accesibles al público, lo que suponía una concretización de la previsión del art. 7.f) de la Directiva 95/46/CE]. b) En otros casos, los medios de comunicación están exentos de la aplicación de varias disposiciones de la normativa de protección de datos. Tal es la situación actual en el caso de Alemania, Francia, los Países Bajos, Austria y Finlandia. El proyecto de normativa italiana [al que después haremos mención] prevé excepciones similares. c) Y, en otros casos, los medios de comunicación quedan exceptuados de la normativa general de protección de datos y están regulados por disposiciones específicas en este ámbito. Es el caso de Dinamarca, para todos los medios de comunicación, y de Alemania, en relación con las empresas públicas de radiodifusión, que están cubiertas por las normativas federal o de los estados federados de protección de datos, pero están sujetas disposiciones específicas de protección de datos establecidas en los tratados interestatales que las regulan».

245. Cfr. arts. 3 j) de la LOPD y 7.1.e) del RPDP.

246. De hecho, no se encuentran estos tratamientos entre los excluidos del ámbito de aplicación de la LOPD ni tampoco entre los remitidos a su legislación específica –art. 2 LOPD–.

información, establece que estas libertades tienen un límite expreso en el derecho al honor, a la intimidad y a la imagen –art. 20.4 CE–.

Por tanto, la libertad de expresión y de información no es tampoco un derecho absoluto y no puede suprimir el derecho a la intimidad y a la protección de datos personales que se fundamentan en la dignidad de la persona y que son necesarios para mantener una calidad de vida humana[247]. Como hemos señalado en otra ocasión, la protección de datos personales, como todo derecho fundamental, tiene una vertiente subjetiva, en este caso muy importante, ya que su objeto es la información sobre personas. No obstante, es necesario hacer hincapié en que la protección de los datos personales, si bien tiene como beneficiario directo a la persona interesada, no afecta sólo al sujeto individual sino a toda la sociedad en su conjunto ya que el ejercicio de los derechos y libertades –la capacidad de decisión y la autonomía– exige preservar un ámbito de privacidad. Hay que superar una concepción individualista de este derecho, derivada de una lógica iusprivatista y propia del constitucionalismo liberal, que analiza el derecho fundamental a la protección de datos personales como un derecho individual, vinculado al derecho de propiedad, que concierne principalmente a las partes interesadas a las que atribuye el control de la propia información personal. Sin negar la función social de la libertad de información, es necesario afirmar que la protección de datos personales «es un elemento esencial y objetivo que afecta al conjunto de la sociedad y concierne a la calidad de una democracia que demanda ciudadanos libres y con capacidad de decisión. Existe un interés público en el respeto a la protección de los datos personales al ser también un instituto de garantía de otros derechos fundamentales, de tal manera que protegiendo los datos personales frente a los tratamientos estamos protegiendo al mismo tiempo el ordenamiento constitucional»[248]. Por este motivo, el ejercicio de la libertad de información debe respetar también principios y derechos de protección de datos personales. e esta forma, no se trata de exceptuar por completo la normativa de protección de datos personales en este ámbito sino de establecer sólo aquellas restricciones necesarias que faciliten la libertad de información y de expresión.

Hay que tener en cuenta que tanto la propuesta de Reglamento como la Directiva protegen la libertad de expresión que se materializa a través de tratamientos de datos personales «con fines periodísticos o de expresión literaria o artística» y no sólo la libertad de información[249], a diferencia de nuestro Tribu-

---

247. Así, el Tribunal Constitucional en la Sentencia 57/1994, de 28 de febrero, lo reconoce como un derecho «estrictamente vinculado a la propia personalidad y que deriva, sin duda, de la dignidad de la persona humana (...) entrañando la intimidad personal constitucionalmente garantizada la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario –según las pautas de nuestra cultura– para mantener una calidad de vida humana».

248. Sobre la protección de datos personales como instituto de garantía de otros derechos fundamentales, cfr. la «Presentación» de *La protección de datos personales*, cit. pp. 27-40.

249. Tanto el Considerando 121 de la propuesta de Reglamento como el Considerando 37 de la Directiva señalan la necesidad de conciliar la protección de datos con la libertad de expresión, si bien hacen una mención particular al derecho a recibir o comunicar

nal Constitucional que ha señalado que sólo ocupa una posición preferente el derecho a una comunicación pública libre que desarrollan los medios de comunicación –los medios institucionalizados de creación de la opinión pública– y los periodistas, y no la libertad de expresión genérica[250]. Así, la propuesta de Reglamento –art. 80–, al igual que la Directiva –art. 9–, no sólo permiten excepciones en los tratamientos con fines periodísticos sino también en los de expresión literaria o artística, señalando la necesidad de conciliar el derecho a la protección de datos personales con las normas que rigen *la libertad de expresión*, todo ello en preceptos titulados «tratamiento de datos personales y

informaciones, como se garantiza en el art. 11 de la Carta de los Derechos Fundamentales de la Unión Europea y en el art. 10 CEDH, respectivamente. En todo caso, el desarrollo de Internet –de *blogs*, de la *web 2.0*– ha hecho que cualquier persona –y no sólo algunos profesionales– tenga la capacidad de informar y de que esta información llegue al conjunto de la sociedad.

250. El Tribunal Constitucional señala que la libertad de información «alcanza un máximo nivel cuando [...] es ejercitada por los profesionales de la información a través del vehículo institucionalizado de formación de la opinión pública que es la prensa, entendida en su más amplia acepción» –SSTC 165/1987, de 27 de octubre, y 29/2009, de 26 de enero–. Así, Agustín Puente, Jefe del Gabinete Jurídico de la AEPD, afirmó en la *Primera Sesión Anual Abierta de la AEPD*, de 22 de abril de 2008 que «podrán considerarse incluidos en fuentes accesibles al público los datos que hayan sido objeto de difusión a través de prensa, radio y televisión (convencional o digital). Las revistas puramente científicas no deberían considerarse fuentes accesibles al público a los efectos de la aplicación de la LOPD. *Internet no es, a los efectos de protección de datos, un medio de comunicación social sino un canal de comunicación, por lo que no es fuente accesible al público*». Cfr. PUENTE ESCOBAR, A., «Ámbito de aplicación y principios. Responsable y encargado. Derechos. Ficheros específicos. FAQs», en *http://www.agpd.es/portalwebAGPD/jornadas/1_sesion_abierta/*. En esa dirección, la Resolución de la AEPD 224/2007, de 19 de abril señala que «los datos personales contenidos en Internet no se consideran dentro de la categoría de medio de comunicación, con independencia de que en el ámbito penal, el Tribunal Supremo pueda entender que los delitos de calumnias e injurias cometidos a través de Internet, se asimilen a los que se produzcan a través de medios de comunicación». Para la Agencia no es equiparable un medio de comunicación institucionalizado y profesionalizado, con el periodismo ciudadano con presencia en la red y mucho menos con extender el concepto a todo lo difundido en Internet. La Agencia sólo aplica la excepción de la libertad de información si la ejercen periodistas profesionales, con un fin periodístico y desarrollan una función social. Cazurro analiza muchas Resoluciones de la AEPD que terminan con un archivo de actuaciones en virtud de la prevalencia de la libertad de expresión y de información sobre el derecho fundamental a la protección de datos personales, señalando que la inmensa mayoría de los denunciados son medios de comunicación institucionalizados –diarios, ediciones digitales de periódicos–. Este autor señala que muy pocas veces se aplican las excepciones relativas a la libertad de expresión y de información a las publicaciones hechas en páginas *web* corporativas. CAZURRO, V., *loc. cit.* pp. 156-157.Ya hemos visto antes como la AEPD, en su Informe 342/2008, no considera a las páginas *web* como fuentes accesibles al público. Tiene sentido la interpretación restrictiva de la categoría de fuentes accesibles al suponer un límite a un derecho fundamental. Sin embargo, no puede hacerse una interpretación igualmente restrictiva del concepto de medio de comunicación social como fuente accesible al público porque en este caso, a diferencia del resto de las fuentes –diarios oficiales, repertorios telefónicos–, se puede estar ejerciendo las libertades reconocidas en el art. 20 CE.

libertad de expresión». También señala que el derecho al olvido en Internet se encuentra limitado por la libertad de expresión –art. 17.3.a)–. El Considerando 121 de la propuesta de Reglamento señala que «con objeto de tomar en consideración la importancia del derecho a la libertad de expresión en toda sociedad democrática, *es necesario interpretar en sentido amplio conceptos relativos a dicha libertad, como el periodismo*. Por consiguiente, los Estados miembros deben clasificar determinadas actividades como «periodísticas» a efectos de las exenciones y excepciones que se han de establecer al amparo del presente Reglamento *si el objeto de dichas actividades es la comunicación al público de información, opiniones o ideas, con independencia del medio que se emplee para difundirlas. No tienen por qué circunscribirse a empresas de comunicación y pueden desarrollarse con o sin ánimo de lucro»*[251]. Este planteamiento es coherente con el reconocimiento constitucional del derecho a expresar y difundir libremente pensamientos, ideas y opiniones, mediante la palabra, el escrito *o cualquier otro medio de reproducción* –art. 20.1.a)–. Esto obliga a modificar el criterio restrictivo en nuestro país, que sólo aplicaba la excepción de los tratamientos de datos personales con fines periodísticos a los que desarrollaban los medios de comunicación institucionalizados –a las empresas de comunicación con ánimo de lucro y a los profesionales del periodismo– en virtud de su calificación en el art. 3.j) LOPD, para adoptar ahora una doctrina que incluya también los tratamientos de datos personales que llevan a cabo los ciudadanos con fines periodísticos que pretenden comunicar al público información, opiniones o ideas, con independencia del medio que empleen para difundirlos –aunque se haga sin ánimo de lucro–, e incluso para acoger aquellos tratamientos que son plasmación de una libertad de expresión más genérica, que incluiría la literaria o artística, todo ello para favorecer la libertad de expresión en la red. Lógicamente, el hecho de que cualquier persona pueda esgrimir el ejercicio de la libertad de expresión para limitar el derecho a la protección de datos personales obliga, por una parte, a delimitar cuando se está ejerciendo realmente la libertad de expresión a través de un tratamiento de datos personales; y por otra, a llevar a cabo una especial labor de ponderación entre derechos fundamentales y a la aplicación del principio de proporcionalidad que garantice el equilibrio entre ambos derechos , algo que no era posible con la calificación de los medios de comunicación como fuentes accesibles al público[252].

---

251. La propuesta de Reglamento tiene en cuenta la interpretación del art. 9 de la Directiva 95/46/CE por la STJUE, de 16.12.2008, as. *Satakunnan Markkinapörssi y Satamedia* cit., donde se señalaba que la publicación de documentos públicos puede considerarse actividades periodísticas si su finalidad es divulgar al público información, opiniones o ideas por cualquier medio de transmisión, no estando reservada la excepción de la Directiva a las empresas de comunicación que ejercen esta actividad con ánimo de lucro. Recientemente, la Sentencia de la Audiencia Nacional, de 11 de abril de 2012, ha revocado una Resolución de la AEPD entendiendo que la publicación de determinados datos en una página web estaba amparada por la libertad de expresión.

252. El problema reside en que la calificación de una publicación como medio de comunicación supone en virtud de la LOPD su consideración de fuente accesible al público y, por tanto, la imposibilidad de llevar a cabo una actividad de ponderación. Esto ha llevado a la Agencia Española a mantener una interpretación restrictiva del concepto de medio de comunicación y de las personas que pueden alegar el ejercicio de la

Tanto la propuesta de Reglamento –art. 80.1– como la Directiva –art. 9– exigen para beneficiarse de la excepción que los tratamientos de datos personales se realicen *«exclusivamente* con estos fines periodísticos o de expresión literaria o artística». Así, el hecho de que el régimen especial de los tratamientos de datos personales se aplique no en virtud del sujeto –que sea una empresa de comunicación o un periodista– sino de la finalidad de los tratamientos, sea cual sea la cualidad del sujeto que lo haga o del medio que emplee para difundirlas, obliga a prestar una atención especial a que realmente *«el objeto* de dichas actividades [sea] la comunicación al público de información, opiniones o ideas» –Considerando 121–[253]. Las excepciones al derecho a la protección de datos que se aplican a los tratamientos con fines periodísticos se justifican en que

libertad de expresión e información para exceptuar el derecho a la protección de datos personales. Hay que tener en cuenta, de nuevo, que en España no se encuentra traspuesta la previsión del art. 7.f) de la Directiva –que tiene efecto directo (cfr. *supra* apdo. IV.B y C)–, que permite el tratamiento para la satisfacción de un interés legítimo perseguido por el responsable o por el tercero a quien se comunique sus datos y que facilita una ponderación con los derechos de los interesados a la protección de sus datos personales, sino que sólo está prevista la existencia de unas fuentes accesibles al público, lo que suprime el consentimiento para el tratamiento y para la cesión. Esto ha obligado a una interpretación restrictiva de estas fuentes accesibles al público incluidas en el art. 3.j) LOPD y en el art. 7 RPDP. Una interpretación muy amplia del concepto de medios de comunicación, que permitiera a cualquier persona el tratamiento y la publicación de datos personales sin consentimiento con sólo esgrimir el ejercicio de la libertad de expresión, afectaría al contenido esencial del derecho fundamental a la protección de datos personales. También hemos interpretado de manera restrictiva la excepción al consentimiento para el tratamiento de datos personales y para las cesiones en relación con la actividad investigadora que se encuentra en la legislación universitaria y en el art. 11.2.e) de la LOPD –también en el art. 13.2 de la Directiva–, aplicándola sólo a la investigación institucional de los profesores en las Universidades públicas y no a su actividad de investigación individual, a. Esta es una cuestión que aborda el art. 83 de la propuesta de Reglamento en relación con los tratamientos de datos para fines de investigación histórica, estadística y científica, una cuestión que no podemos abordar ahora. Hay que señalar que si bien las excepciones al derecho a la protección de datos personales por tratamientos personales vinculados a la libertad de expresión tienen acogida en el art. 80 de la propuesta de Reglamento –y en el art. 9 de la Directiva–, también le sería de aplicación la referencia a la satisfacción de un interés legítimo del art. 6.1.f) de la Propuesta de Reglamento –no el cumplimiento de una misión de interés público del art. 6.1.e), que es sólo aplicable a las Administraciones Públicas–, lo que permite la vigencia del principio de proporcionalidad. Mientras que se aprueba la propuesta de Reglamento, el efecto directo del art. 7.f) de la Directiva permite una interpretación más amplia del concepto de medio de comunicación, coherente con el ejercicio de las libertades del art. 20 CE, y que al mismo tiempo facilita la ponderación y el equilibrio con el derecho a la protección de datos personales, que su calificación automática como fuente accesible al público impedía. Hay que tener en cuenta que el art. 9 de la Directiva prevé también una actividad de ponderación que no ha podido desarrollarse con la previsión del art. 3.j) LOPD.

253. La STJUE, de 16.12.2008, as. *Satakunnan Markkinapörssi y Satamedia* cit. también aplicaba la excepción del art. 9 de la Directiva 95/46/CE a los tratamiento de datos efectuados exclusivamente con fines periodísticos, si tales actividades se ejercen exclusivamente con la finalidad de divulgar al público información, opiniones o ideas por cualquier medio de transmisión.

estos tratamientos son una materialización del «derecho a la libertad de expresión, y, en especial, del derecho de recibir o de comunicar informaciones, como se garantiza especialmente en el artículo 11 de la Carta de los Derechos Fundamentales», dada «la importancia del derecho a la libertad de expresión en toda sociedad democrática» –Considerando 121–. Como ha señalado la STC 171/1990, de 12 de noviembre la posición preferente de la libertad de información frente a otros derechos fundamentales no es absoluta, puesto que «si viene reconocido como garantía de la opinión pública, solamente puede legitimar las intromisiones en otros derechos fundamentales que guarden congruencia con esa finalidad, es decir, que resulten relevantes para la formación de la opinión pública sobre asuntos de interés general»[254]. La prevalencia de estos derechos se da si se ejercen en su ámbito constitucional protegido, que es la garantía institucional de una opinión pública libre. Por tanto, es necesario que el tratamiento de datos personales que pretenda exceptuarse del régimen general de protección de datos en virtud del ejercicio de la libertad de expresión tenga «exclusivamente» esa vocación de comunicar al público información, opinión o ideas y, contribuir, por tanto, a una opinión pública libre en una sociedad democrática. Lógicamente, el abandono del criterio del sujeto –que sea un medio de comunicación institucionalizado o periodistas profesionales quienes que ejerzan la libertad de información– por el de la finalidad del tratamiento, que permite a cualquier persona apelar al ejercicio de la libertad de expresión en Internet, fomenta el pluralismo informativo en una sociedad democrática pero también obliga a llevar a cabo una cuidadosa labor de delimitación en cada supuesto concreto[255]. Además, la exigencia normativa de que la excepción al régimen general de protección de datos personales sólo vaya destinada a los tratamientos de datos personales que se realicen «*exclusivamente* con estos fines periodísticos o de expresión literaria o artística», también supone un importante

254. Así, como señala la STC 171/1990, de 12 de noviembre, carecen de tal efecto legitimador cuando «las libertades de expresión y de información se ejerciten de manera desmesurada y exorbitante del fin en atención al cual la Constitución le concede su protección preferente. De ello se deriva que la legitimidad de las intromisiones en el honor e intimidad personal requiere no solo que la información cumpla la condición de la veracidad, sino también que su contenido se desenvuelva en el marco del interés general del asunto al que se refiere; de otra forma, el derecho de información se convertiría en una cobertura formal para, excediendo el discurso público en el que debe desenvolverse, atentar sin límite alguno y con abuso de derecho, al honor, y la intimidad de las personas, con afirmaciones, expresiones o valoraciones que resulten injustificadas por carecer de valor alguno para la formación de la opinión pública sobre el asunto de interés general que es objeto de la información. El efecto legitimador del derecho de información, que se deriva de su valor preferente, requiere, por consiguiente, no sólo que la información sea veraz –requisito necesario directamente exigido por la propia Constitución, pero no suficiente–, sino que la información tenga relevancia pública, lo cual conlleva que la información veraz que carece de ella no merece la especial protección constitucional».

255. Lógicamente, el abandono del criterio del sujeto es también consecuencia de que Internet, como medio y estructura de comunicación, difumina las diferencias entre los profesionales de la información que desarrollan el periodismo institucional y los particulares que ejercen la libertad de expresión.

límite para las empresas de comunicación. Así, no estarían protegidos por la libertad de expresión y de información aquellos tratamientos de datos personales que llevan a cabo los medios de comunicación institucionalizados que no tienen en sí mismo un fin periodístico o de expresión literaria o artística, como son, por ejemplo, los tratamientos en el ámbito de los recursos humanos, las promociones comerciales y de marketing, los tratamientos de las personas físicas suscriptoras[256] u otros tratamientos, muchos de ellos masivos, como son los relativos a la participación en concursos, juegos o sorteos y que no tienen ni un fin periodístico ni de expresión literaria o artística[257]. Por tanto, estos tratamientos están sometidos al régimen general de protección de datos personales.

Además, es necesario llevar a cabo una ponderación entre la libertad de expresión y de información y el derecho a la protección de datos personales, aplicando el principio de proporcionalidad, de forma que se garantice el equili-

256. Los datos de personas físicas suscriptoras de medios de comunicación no sólo no están excluidos de la normativa de protección de datos sino que merecen una protección especial porque pueden servir para establecer perfiles e, incluso, en ocasiones, revelar ideología, religión u orientación sexual, una cuestión que no podemos abordar aquí.

257. La Agencia Española impuso una sanción de 1,08 millones de euros a la productora *Zeppelin Televisión S A*, por el incumplimiento de la LOPD en el tratamiento de 7.000 candidatos a participar en programa *Gran Hermano*, que emitía Tele 5. El Tribunal Supremo, en la Sentencia de 17 de abril de 2007, confirmó la sanción –que previamente había sido ratificada por la Audiencia Nacional–. Este tratamiento de datos personales de la productora no se realizaba exclusivamente con fines periodísticos o de expresión literaria o artística y que no estaba excluido de la vigencia de los principios y derechos de protección de datos en virtud de la libertad de información y de expresión, sin perjuicio de que se le apliquen otras excepciones relativas a la existencia de una relación jurídica –art. 11.2.c) LOPD–. La productora incumplió su obligación de implantar medidas de seguridad lo que permitió que los datos relativos a un «considerable número de aspirantes» a participar en el concurso televisivo acabaran apareciendo en Internet. La productora no respetó el principio de calidad, recabando, además, datos personales sin cumplir el principio de información y cediéndolos a empresas con las que no le unía ningún lazo contractual. El Tribunal señaló que la tramitación del expediente sancionador puso de manifiesto «el más completo desprecio (de la productora televisiva) hacia la exigencia del consentimiento consciente e informado de los afectados para que sus datos personales (información relativa a gustos, ideología, creencias religiosas, raza, salud o vida sexual) fueran almacenados, tratados y cedidos». Así, se señala que «la participación en un programa, incluso en el de *Gran Hermano*, no puede 'despojar' a un ciudadano de su derecho a la intimidad, porque su libertad sigue intacta y conserva el pleno derecho a que nadie trate, ceda o revele sus datos personales». La AEPD desarrolló en el año 2002 una Inspección Sectorial de Oficio, en el sector de *Concursos, juegos y sorteos de televisión*, que finalizó con una Recomendación que los somete a la normativa general de protección de datos y donde se señala que «no se recabarán datos personales cuyo conocimiento por parte del responsable no esté justificado por la finalidad para la que se recaban y de la cual el usuario no haya sido previamente informado». Cfr. *Inspección Sectorial de oficio «Concursos, juegos y sorteos de televisión». Conclusiones y recomendaciones*, Madrid, 18 de octubre de 2002, en *http://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones*

brio entre ambos derechos. No se trata de exceptuar por completo la normativa de protección de datos personales a los tratamientos de datos personales efectuados con fines exclusivamente periodísticos o de expresión literaria o artística sino de establecer sólo aquellas restricciones necesarias que faciliten la libertad de información y de expresión o eviten ponerla en peligro. La Directiva establece que no caben todas las exenciones y excepciones sino «sólo [aquellas] en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión» –art. 9 y Considerando 37–. Además, el Considerando 37 de la Directiva, por una parte, no admite excepciones a las medidas que garanticen la seguridad de los tratamientos y, por otra, si bien acepta excepciones en lo relativo a las competencias de las autoridades de control, señala que debe concederse a éstas «al menos una serie de competencias a posteriori como por ejemplo publicar periódicamente un informe al respecto o bien iniciar procedimientos legales ante las autoridades judiciales». La regulación que hace la propuesta de Reglamento es bastante semejante, aunque la Directiva es algo más garantista, porque reitera explícitamente el juicio de necesidad para valorar la proporcionalidad de la injerencia y limita las materias sujetas al régimen de excepciones. El art. 80 de la propuesta de Reglamento menciona la necesidad de establecer excepciones o exenciones «para conciliar el derecho a la protección de los datos de carácter personal con las normas que rigen la libertad de expresión». Las excepciones y exenciones que se mencionan expresamente «son las relativas a los principios generales, los derechos del interesado, el responsable y encargado del tratamiento, la transferencia de datos a terceros países u organizaciones internacionales, las autoridades de control independientes, así como en la cooperación y la coherencia». Le corresponde a los Estados miembros adoptar las medidas legislativas «necesarias a efectos de equilibrar estos derechos» –Considerando 121–. Así, es lógica la excepción al principio de consentimiento del interesado cuya exigencia haría imposible el ejercicio de la libertad de expresión. De hecho, las previsiones de la propuesta de Reglamento y de la Directiva hay que entenderlas principalmente como supuestos de legitimación del tratamiento para fines periodísticos o de expresión literaria o artística, y, por tanto, como excepciones al consentimiento del interesado. La LOPD, al considerar los tratamientos de los medios de comunicación como fuentes accesibles al público, ha establecido la excepción del consentimiento para el tratamiento y para la cesión –arts. 6.2 y 11.2.c) LOPD–. Algo semejante puede decirse de la necesidad de establecer límites al principio de información en los tratamientos con fines periodísticos o de expresión literaria o artística.

La excepción al derecho del interesado a la cancelación de sus datos personales objeto de tratamiento es también algo consustancial al ejercicio de las libertades reconocidas en el art. 20 CE. Esto es de especial aplicación al derecho al olvido en Internet. De hecho, el Considerando 121 de la propuesta de Reglamento señala que estas excepciones a la protección de datos personales «debe[n] aplicarse en particular al tratamiento de los datos personales en el ámbito audiovisual y en los archivos de noticias y hemerotecas». Así, la propuesta de

Reglamento establece como límite del derecho del interesado a que el responsable del tratamiento suprima los datos personales que le conciernen y se abstenga de utilizarlos, que la «conservación de los datos sea necesaria para el ejercicio de la libertad de expresión» –art. 17.3.a)–. De esta forma, le corresponde al medio de comunicación o a la persona que trata datos personales con fines periodísticos o con fines de expresión literaria o artística decidir si mantiene publicada la información accesible en Internet porque continúa el interés público o su relevancia para formar la opinión pública o limita su indexación[258]. Lógicamente, esta decisión puede verse motivada por el ejercicio por el interesado de los derechos de rectificación, oposición y cancelación, alegando los criterios que más adelante señalaremos –tratamiento de datos excesivos, ausencia de interés público por la materia o por las personas a las que se refiere, falta de veracidad, expresiones vejatorias, etc.–.. Como señalaremos después, le corresponde al legislador nacional regular sistemáticamente el ejercicio del derecho de rectificación que forma parte de los derechos de protección de datos personales frente a los tratamientos con fines periodísticos o de libertad de expresión, con el derecho de rectificación, que se encuentra regulado en la Ley Orgánica 2/1984, de 26 de marzo. Lógicamente, la determinación de la rectificación o de la supresión no afecta a la versión en papel, sino a la versión electrónica –a una parte de la versión electrónica a la que ya no se le da publicidad–. Ya hemos señalado anteriormente que la regulación del derecho al olvido de la propuesta de Reglamento contempla la posibilidad de que el responsable del tratamiento, en lugar a proceder a la supresión, limite el tratamiento de los datos –y, por tanto, a nuestro juicio, limite la publicidad– cuando el interesado impugne la exactitud de los datos –durante el plazo que permita al responsable del tratamiento verificar la exactitud de los datos–; o cuando el responsable del tratamiento «ya no necesite los datos personales para la realización de su misión» –art. 17.4–. Además, la propuesta de Reglamento obliga al responsable del tratamiento a llevar a cabo un examen periódico de la necesidad de conservar los datos –art. 17.7–. Todos estas previsiones legales facilitan al responsable del tratamiento llevar a cabo una actividad de ponderación acerca del mantenimiento de la publicidad de la información y su accesibilidad a los buscadores, aplicando el principio de proporcionalidad para evitar los tratamientos excesivos que suponga una injerencia excesiva en los derechos de las personas[259]. Estas cuestiones, a nuestro juicio, deben ser abordadas principalmente a través

---

258. Para M. CARRILLO, «la justificación jurídica se fundamenta en la veracidad y el interés público de la información que aparece en la red. Porque lo que fue de interés público en un momento determinado –la comisión de un delito– no puede desaparecer de la historia. De lo contrario estaríamos ante una falsedad». Cfr. CARRILLO, M.: «El derecho al olvido en Internet», *El País*. 30 de enero de 2010.

259. Hemos desarrollado en otro momento los criterios que delimitan cuándo la publicación de datos personales por la Administración Pública supone un tratamiento excesivo para la finalidad y debe bloquearse o cancelarse –cfr. *La protección de datos personales*, cit. 768-780–. Sin embargo, estos criterios no son igualmente trasladables a los tratamientos de datos personales con fines periodísticos o de libertad de expresión porque estos suponen el ejercicio de una libertad preferente.

de la autorregulación. Lógicamente, como he señalado antes, esta actividad de ponderación le corresponde al responsable del tratamiento, esto es al medio de comunicación o a la persona que lleva a cabo el tratamiento de datos personales con fines periodísticos o de expresión literaria o artística y que ha hecho pública la información; no, obviamente, al motor de búsqueda.

La propuesta de Reglamento también establece que esta previsión «no debe llevar a los Estados miembros a establecer exenciones de las demás disposiciones del presente Reglamento» –art. 80.1–. De hecho, hay exigencias de la normativa de protección de datos personales que no sólo no perjudican el ejercicio de la libertad de expresión y de información sino que lo garantizan, como son las relativas a las normas de seguridad, que mencionaba expresamente la Directiva[260]. También sería de aplicación –en este caso a los medios de comunicación institucionalizados y a las empresas de comunicación– muchas de las obligaciones que la propuesta de Reglamento establece para el responsable del tratamiento como es la conservación de la documentación de los tratamientos, la realización de la evaluación de impacto en la privacidad o la designación de un delegado de protección de datos, cuyo cumplimiento en nada perjudica el ejercicio de la libertad de expresión[261]. Los responsables de los tratamientos también deben contestar a los interesados en el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición, aunque sea, para desestimar la solicitud. Lógicamente, los tratamientos de datos personales por los medios de comunicación, a pesar de que se encuentren sustentados por la libertad de información y tengan el carácter de fuentes accesibles al público en nuestro país, están sometidos al control judicial[262].

Mención específica merece el respeto al principio de calidad en los trata-

---

260. Así, es necesario aplicar medidas de seguridad para garantizar la integridad e inalterabilidad de lo publicado en medios de comunicación en Internet –evitando ataques informáticos que modifiquen la información–. También es necesario implantar medidas de seguridad a los tratamientos de datos personales sobre informaciones aún no publicadas, aunque sea complicado el establecimiento de algunas de ellas, como los controles de acceso, por la forma de trabajar de los periodistas que no es individual. Obviamente, no tiene sentido aplicar medidas de seguridad que garanticen la confidencialidad de la información cuando ésta esté siendo publicada en abierto en Internet –por la misma razón que no tiene sentido exigir medidas de seguridad de nivel alto a los ficheros internos de diputados y senadores de las Cámaras si esta información debe publicarse sin consentimiento en virtud de la función de representación política–, además de que se trata de datos que el interesado ha hecho manifiestamente públicos –art. 9.2.e) de la propuesta de Reglamento–.

261. De hecho, los medios de comunicación como las fuentes accesibles al público tenían la obligación de notificación de los tratamientos. Téngase en cuenta que incluso los responsables policiales de los ficheros para la investigación del terrorismo y de formas graves de delincuencia organizada debían comunicar previamente su existencia, sus características generales y su finalidad a la Agencia de Protección de Datos –art. –art. 2.2.c) LOPD–.

262. El TJCE, en la Sentencia *Lindqvist* –ya citada– ha señalado que las previsiones de la Directiva 95/46/CE no suponen, en sí mismas, una restricción contraria a la libertad de expresión o de otros derechos fundamentales y que corresponde a las jurisdicciones nacionales ponderar en cada supuesto de conflicto qué derecho debe primar.

mientos de datos personales con fines periodísticos o de expresión literaria o artística. De hecho, la ponderación entre la libertad de expresión y el derecho a la protección de datos debe hacerse principalmente desde el principio de calidad, no desde el principio de consentimiento, que implica un automatismo acrítico, ni tampoco desde el principio de información porque conllevaría la implantación de soluciones básicamente burocráticas[263]. El principio de calidad, que es el más importante dentro del contenido esencial del derecho fundamental a la protección de datos personales en los ámbitos donde hay excepciones al consentimiento[264], alberga dentro de sí: el principio de adecuación y prohibición de exceso, que exige que los datos que se publiquen sean idóneos y pertinentes para la finalidad periodística y que no se publiquen datos excesivos, evitando que la libertad de expresión se ejerza de una manera desmesurada y exorbitante que no sirva para el debate político[265]; el principio de finalidad legítima, que demanda que los tratamientos de datos personales tengan exclusivamente fines periodísticos o de expresión artística o literaria, teniendo que guardar las intromisiones en la protección de datos congruencia con la finalidad de formación de la opinión pública libre, que es lo que justifica su protección preferente[266]; el principio de exactitud de la información, que obliga a que ésta

263. La Sentencia de la Audiencia Nacional, de 12 de enero de 2001, al analizar la relación entre los arts. 18.4 y 20 CE, señala que: «pese a la carencia de regulación específica, la mejor doctrina entiende que visto el contenido del art. 6.1 de la LORTAD [...] la expresión *salvo que la Ley disponga otra cosa* permite entender que no es necesario el consentimiento del afectado, cuando el art. 20 del CE permite el tratamiento. Lo que exigirá una ponderación del caso concreto y desde los principios de adecuación, pertinencia y congruencia recogidos en el artículo 4 de la LOPD». Cfr. también las Sentencias de la Audiencia Nacional, de 2 de febrero de 2006 y de 16 de marzo de 2006. Cfr. LESMES SERRANO, C. (coord.), *op. cit.* pp. 199-202.

264. Cfr. nuestro trabajo «El principio de calidad», *loc. cit.* pp. 341-394.

265. Esto ocurre cuando se publican datos íntimos, expresiones injuriosas o vejatorias, datos que no sean veraces, datos de menores, etc.. Así, en muchas ocasiones se publican datos personales cuando el interés público se alcanza igualmente publicando un menor número de datos o anonimizando o disociando la información personal –eludiendo la divulgación de datos de menores que han sufrido abusos, evitando que en las fotografías aparezcan carteles con teléfonos, pixelando las imágenes, etc.–. En muchas ocasiones, el tratamiento de datos es excesivo para la finalidad. Así, la Sentencia de la Audiencia Nacional, de 9 de julio de 2009, estima un recurso interpuesto contra una Resolución de archivo de la AEPD, que había considerado prevalente la libertad de información sobre la protección de datos personales en un supuesto de publicación de imágenes de enfermos: «aunque las imágenes no sean de buena calidad, puede entenderse que el tratamiento del dato de la imagen ha sido excesivo tomando en consideración que no se encuentra amparado por el consentimiento de los afectados (no consta que conocieran la publicación de las imágenes) y tampoco se encuentra amparado por la libertad de información y, en todo caso, parece que se ha producido un empleo desmedido de la imagen como dato personal puesto que el carácter noticiable de la información se cumplía suficientemente sin necesidad de incluir imágenes directas de los enfermos». Las exigencias del principio de adecuación y prohibición de exceso se refieren a la publicación de la información pero no impiden estos tratamientos de datos antes de que la información sea publicada.

266. Sin embargo, hay elementos del principio de finalidad, como la determinación, la explicitud o el respeto a la finalidad originaria en todas las fases del tratamiento que no son aplicables a estos supuestos.

sea veraz, y a rectificar y cancelar los datos erróneos o inexactos, algo especialmente aplicable a la publicación de medios de comunicación en Internet, teniendo en cuenta la permanencia de la información y su fácil localización a través de los buscadores[267]; El principio de calidad explica mejor la jurisprudencia constitucional que pondera la libertad de información y la privacidad y que es aplicable claramente en este ámbito[268]. Así, la mayoría de los criterios para

267. No nos podemos detener ahora en la problemática de que los medios de comunicación manipulen o retoquen fotografías de los afectados y cuál es su relación con el principio de exactitud de los datos y la necesidad del consentimiento del interesado.

268. Como es sabido, la libertad de información tiene que respetar el derecho a la intimidad de las personas y el derecho fundamental a la protección de datos personales. Nuestra jurisprudencia constitucional ha fijado una serie de criterios que son útiles en la delimitación entre la libertad de información y el derecho a la intimidad y que sirven también para la protección de datos personales. Para que prevalezca la libertad de información es necesario que lo difundido o que los datos personales objeto de tratamiento por el medio de comunicación sean de interés público, es decir, tengan un carácter noticiable, bien en razón del objeto –porque su contenido resulte de interés colectivo o general–, bien por el sujeto –por la relevancia y dimensión pública de la persona objeto de la información–. Un asunto tiene relevancia pública porque su conocimiento sirve al interés general al referirse a un acontecimiento o a una cuestión que es objeto de controversia social que afecta a los ciudadanos en general y no sólo a unos particulares. Hay personas que por su profesión o cargo público se encuentran en el escenario público y están sometidas por ello a la crítica y a un nivel de escrutinio público superior al de una persona anónima –cfr. SSTC 171/1990, de 12 de noviembre y 204/1997, de 25 de noviembre–. No obstante, la libertad de información también tiene límites. Las personas sobre las que hay un interés del público, por el cargo que ostentan o por la profesión que realizan, mantienen un grado de derecho a la intimidad. Además, la información debe ser veraz, lo que a juicio del Tribunal Constitucional –Sentencia 61/2004, de 19 de abril, implica que el informador haya realizado una labor de indagación con la diligencia que le es exigible a un profesional. Asimismo, las informaciones vertidas en los medios no pueden incluir expresiones injuriosas, vejatorias o insultos sin relación con las ideas u opiniones que se expongan y que resulten innecesarias para su exposición –la STC 104/1986, de 17 de julio–.Cfr. más ampliamente CARRILLO, M., *El Derecho a no ser Molestado. Información y vida privada*, Thomson, Aranzadi, 2003, pp. 25-37 y 77-91. La Agencia Española de Protección de Datos ha aplicado alguno de estos criterios elaborados por la jurisprudencia constitucional para delimitar la libertad de información del derecho a la intimidad. La Resolución 775/2007 –donde curiosamente se mantiene un concepto más amplio de medio de comunicación– archivó la denuncia contra Esquerra Unida del País Valencià por publicar datos de nombre, apellidos, puesto laboral que ocupaba en el Ayuntamiento de Paiporta, así como las retribuciones que cobraba por desempeñar dicho puesto. Esta información se publicó tanto en la web del partido político como en un boletín informativo. La Agencia Española entiende: «en primer lugar, que la información publicada era veraz, puesto que los datos que fueron asociados al nombre y apellidos del denunciante coinciden con los datos que figuran en los Presupuestos Anuales del Ayuntamiento de Paiporta. En segundo lugar, la información publicada tenía una indudable trascendencia pública y social para la localidad de Paiporta, al publicar datos sobre el incremento extraordinario que había efectuado el Ayuntamiento de Paiporta a las retribuciones correspondientes al puesto que se había adjudicado al denunciante, reciente ex-concejal del citado Ayuntamiento, por tanto dicha información no fue publicada con la intención de desacreditar al denunciante, sino únicamente en el ejercicio legítimo de informar a los ciudadanos sobre los asuntos de mayor trascenden-

la ponderación de derechos –el interés público por razón del sujeto o del objeto, la veracidad o exactitud de la información, la esencialidad de la información, la sensibilidad de los datos, etc.–tienen cabida dentro del principio de calidad. Hay temas que por ser de interés público pueden ser difundidos y pueden justificar la recogida y tratamiento de datos personales, aunque afecten a la intimidad de las personas o aunque supongan un límite a su derecho a controlar su información personal. La persona no puede oponerse a la publicación de esa información o al tratamiento de sus datos personales por el medio de comunicación, aunque afecten al ámbito privado. No hay que proteger los datos íntimos

---

cia o notoriedad, como parte de sus funciones de partido político y para contribuir a la formación de una opinión pública en torno a los asuntos de interés local. En consecuencia, del análisis efectuado de la información publicada en el boletín y en la página Web de ESQUERRA, se desprende que ésta era veraz, tenía indudable trascendencia pública en la localidad de Paiporta y fue publicada dentro del ejercicio de sus funciones como partido político y con la finalidad de contribuir a la formación de una opinión pública, por lo que de acuerdo a los criterios de la doctrina expuesta, en este caso concreto, prevalecería el derecho fundamental a la información recogido en el artículo 20 de la Constitución Española sobre el derecho fundamental a la protección de los datos personales establecido en el artículo 18.4 de dicha Constitución. Por ello, de acuerdo a las anteriores consideraciones, procede estimar las alegaciones efectuadas por ESQUERRA y el archivo de la infracción del artículo 6.1 de la LOPD, que se imputaba en el presente procedimiento sancionador». Igualmente, la AEPD en la Resolución 598/2007 resolvió una tutela del derecho de cancelación alegando la STC 107/1998, que concreta que «el valor preponderante de las libertades públicas del art. 20 de la CE, en cuanto se asienta en la función que éstas tienen de garantía de una opinión pública libre indispensable para la efectiva realización del pluralismo político, solamente puede ser protegido cuando las libertades se ejerciten en conexión con asuntos que son de interés general por las materias a que se refieren y por las personas que en ellos intervienen y contribuyen, en consecuencia, a la formación de la opinión pública, alcanzando entonces su máximo nivel de eficacia justificadora frente al derecho al honor, el cual se debilita, proporcionalmente, como límite externo de las libertades de expresión e información, en cuanto sus titulares son personas públicas, ejercen funciones públicas o resultan implicadas en asuntos de relevancia pública, obligadas por ello a soportar un cierto riesgo de que sus derechos subjetivos de la personalidad resulten afectados por opiniones o informaciones de interés general, pues así lo requieren el pluralismo político, la tolerancia y el espíritu de apertura, sin los cuales no existe sociedad democrática». La AEPD ha recogido esta jurisprudencia constitucional relativa a la libertad de información y el derecho a la intimidad para resolver distintas Resoluciones. En su Resolución de 24 de febrero de 2009 cita la jurisprudencia del TC en la que se tiende a «otorgar una posición preferente a la libertad de expresión frente a otros derechos constitucionales, siempre y cuando los hechos comunicados se consideren de relevancia pública (STC 105/1983, STC 107/1988) y atendiendo a la veracidad de la información facilitada (STC 6/1988, STC 105/1990, STC 240/1992)». Y en función de lo anterior, concluye que, por todo ello, cabe proclamar que un ciudadano que no goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen por la red sin poder reaccionar ni corregir la inclusión ilegítima de los mismos en un sistema de comunicación universal como Internet». Esta cita proviene de la Resolución de 7 de abril de 2008 y se encuentra, también en la Resolución de 24 de febrero de 2010. Todas las Resoluciones se encuentran publicadas en *https://www.agpd.es/portalwebAGPD/resoluciones/archivo_actuaciones/index-ides-idphp.php* y han sido analizadas por CAZURRO, V., *op. cit*. pp. 89-246.

de una persona de relevancia pública cuando existe interés público, especialmente cuando su comportamiento privado contrasta con su discurso público –por ejemplo, las fotos de las fiestas privadas de Berlusconi– y esto puede ser valorado por la opinión pública, ser criticado y favorecer el cambio político –algo esencial en el valor procedimental de la libertad de información–[269]. Que el principio de calidad sea el que mejor explica la necesidad de conciliar el derecho a la protección de los datos de carácter personal con la libertad de expresión no encubre que la ponderación en el cada caso concreto no sea una actividad fácil. Es necesario analizar pausadamente cada supuesto de hecho porque hay casos claros pero también abundantes *hard cases*, y muchos más habrá con el reconocimiento abierto del derecho al olvido en Internet en la propuesta de Reglamento, lo que incrementará exponencialmente las reclamaciones al responsable del tratamiento. Es necesario valorar en cada caso que el tratamiento de datos personales se ha efectuado «exclusivamente» con fines periodísticos o de expresión literaria o artística; que todos los datos publicados tienen interés público y son necesarios para una opinión pública libre y no se trata de un «mero interés público» –expresión de la curiosidad de una amplia parte de la sociedad, que no legitima ninguna intromisión en ningún derecho

269. En todo caso, incluso en relación con los personajes públicos existen tratamientos de datos que pueden suponer una publicación excesiva. La intimidad de los personajes públicos debe ser respetada si los datos tratados no tienen relevancia con su función pública y no son imprescindibles para favorecer la libertad de información y la opinión pública libre –creencias, datos de salud, orientación sexual–, no existiendo un interés público que justifique la publicidad. El Decreto Legislativo, de 30 de junio de 2003, que aprueba en Italia el *Codice in materia di protezione dei dati personali –Codice Della Privacy-* recoge la excepción del consentimiento para que los periodistas traten datos especialmente protegidos, siempre que se cumpla la *esencialidad de la información* en relación con los acontecimientos de interés público –art. 137.2–.
Hay que recordar que el Defensor del Pueblo Europeo ha manifestado que «no debería hacerse referencia a la protección de datos cuando, por ejemplo, las personas están actuando en calidad pública, cuando participan en un proceso de toma de decisiones público por propia iniciativa o cuando intentan influir en dicha toma de decisiones». Cfr. la Carta del Defensor del Pueblo Europeo al Presidente de la Comisión, de 30 de septiembre de 2002, y el documento *Openness and data protection* en *http://ombudsman.europa.eu/*. No obstante, el Grupo del Artículo 29 en su Dictamen 3/1999, de 3 de mayo, relativo a la «Información del sector público y protección de los datos personales». «Contribución a la consulta iniciada con el Libro Verde de la Comisión Europea titulado *La información del sector público: un recurso clave para Europa*«, COM (1998)585« señala que «el legislador, cuando desea que un dato se vuelva accesible al público no considera sin embargo que haya que convertirse en *res nullius*. Tal es la filosofía del conjunto de nuestras legislaciones. El carácter público de un dato de carácter personal, resulte de una normativa o de la voluntad de la propia persona a la que alude el dato, no priva, *ipso facto* y para siempre, a dicha persona de la protección que le garantiza la ley en virtud de los principios fundamentales de defensa de la identidad humana». Cfr. el documento en *http://ec.europa.eu/justice_home/fsj/privacy/policy_papers/policy_papers_topic_en.htm#public_registers*. Esto obliga a llevar a cabo una ponderación y a aplicar el principio de proporcionalidad, una cuestión que hemos abordado en otro momento –*La protección de datos personales*, cit. pp. 729-731 y 781-796-

fundamental y que no tiene nada que ver con el auténtico interés público, como elemento objetivo que define la importancia de una información en Internet[270]–; que la información es veraz y que con carácter previo a su difusión se ha llevado a cabo una labor diligente de indagación; que las expresiones sobre las personas, aún siendo hirientes, moletas o desabridas, no son injuriosas o vejatorias; que se respeta al menos el grado de intimidad mínima que merecen las personas sobre las que hay un interés del público, por el cargo que ostentan o por la profesión que realizan; etc. Lógicamente, no basta con afirmar la necesidad de conciliar la libertad de expresión con el derecho a la protección de datos personales sino que es necesario que alguien vele porque esta conciliación se produzca. La aplicación del generoso régimen de excepciones a los tratamientos de datos personales en Internet con fines periodísticos o de expresión artística o literaria no puede dar lugar a la indefensión de los interesados o a la percepción de que en este ámbito ni la legislación ni los derechos prevalecen. No es fácil que esta función de ponderación en toda su variedad de matices la puedan cumplir las Agencias de Protección de Datos, tal y como están configuradas actualmente, más habituadas a la adopción de decisiones automáticas cuando no automatizadas en virtud de la existencia o no de una habilitación legal[271]. Tampoco parece una cuestión clara que sea la Agencia de Protección de Datos, que no deja de ser una Administración Pública –aunque independiente–, pueda tener competencias para limitar el ejercicio de un derecho fundamental tan importante para una sociedad democrática como es la libertad de expresión e información. Esto no se deduce de la LOPD que atribuye a la Agencia la función de velar por el cumplimiento de la legislación de protección de datos personales –art. 37.a)–, sin hacer mención alguna a la libertad de expresión y de información[272]. Esta cuestión se deja claramente abierta en la propuesta de reglamento que incluye dentro de las excepciones a los tratamientos de datos personales con fines periodísticos o de expresión literaria o artística lo relativo a las autoridades de control independientes y a la cooperación y coherencia. Es necesario en este punto un pronunciamiento claro del legislador nacional, al que se remite en este punto la propuesta de Reglamento. Sí parece claro que la responsabilidad última de la aplicación de las excepciones a los tratamientos de datos con fines periodísticos o de libre expresión literaria o artística y de la conciliación de los derechos en presencia le corresponde a los órganos jurisdiccionales[273]. También

270. Cfr. ARIAS MÁIZ, V., *loc. cit.*
271. Habitualmente la AEPD ha otorgado prevalencia a la libertad de expresión e información sobre el derecho a la protección de datos personales en relación con la relevancia pública de los asuntos, y negándosela cuando un ciudadano «no goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública», sin incidir en otras cuestiones como la veracidad o la ausencia de expresiones vejatorias o insultantes, y sin interesarse en si el tratamiento es excesivo o se podía alcanzar la finalidad legítima disociando la información.
272. Carrillo señala que las restricciones al derecho a la intimidad deben ser adoptadas por la autoridad juridicial, si bien ésta no es una prescripción que se derive del artículo 18.1 CE, por lo que también podrán ser acordadas por autoridades administrativas, siempre que para ello exista una habilitación legal. Cfr. CARRILLO, M., *op. cit.* p. 50.
273. Cfr. la SJUE, de 16.12.2008, as. *Satakunnan Markkinapörssi y Satamedia* y la Sentencia *Lindquist*.

parece meridianamente claro en la propuesta de Reglamento que esta labor de ponderación no la puede hacer los motores de búsqueda.

La publicación de los medios de comunicación en Internet, así como la existencia de los buscadores, hace que se produzca una intromisión continuada en los derechos de las personas. Como hemos señalado ya, el responsable del tratamiento principal es el medio de comunicación que publica la información en Internet y que se encuentra amparado por el ejercicio de la libertad de información (art. 20 CE) –, o la persona que lleva a cabo los tratamientos de datos personales con fines periodísticos o de expresión literaria o artística, utilizando la expresión en un sentido amplio que da el Considerando 121 de la propuesta de Reglamento. Por tanto, la responsabilidad de lo que se publica es del medio de comunicación –o de la persona que lleva a cabo el tratamiento en ejercicio de la libertad de expresión–, no del buscador. Por ello, no parece razonable atribuir la responsabilidad de las posibles infracciones al buscador que se limita a localizar la información que los medios de comunicación sque, al igual que los diarios oficiales, son fuente accesible al público *ex* art. 3 LOPD publican en Internet al mismo tiempo que se exonera al medio de comunicación, protegido por la libertad de información. La LOPD señala expresamente que el carácter de fuente accesible al público implica que la consulta puede ser realizada por cualquier persona, autorizando el tratamiento y la cesión sin consentimiento –arts. 6.2 y 11.2.b)l. Además, como hemos analizado antes, la propuesta de Reglamento establece que cuando el responsable del tratamiento haya autorizado a un tercero a publicar datos personales –y lo ha autorizado cuando lo publica en un medio de comunicación, que tiene el carácter de fuente accesible al público o cuando no implanta ningún mecanismo que evite la indexación y la difusión masiva–, será considerado responsable de esta publicación –art. 17.2–[274]. Hay que tener en cuenta, además, que mientras que la publicación de datos personales en diarios oficiales o webs institucionales o en relación con las personas que pertenezcan a grupos profesionales no supone el ejercicio de un derecho fundamental, los tratamientos de datos personales con fines periodísticos o de expresión literaria o artística están amparados por la libertad de expresión. Así, aún en el marco de la LOPD, que reconoce un derecho de oposición frente a los tratamientos de datos personales que provengan de fuentes accesibles al público –ex art. 6.2–[275], hay que subrayar que no se encuentra en la misma situación el ejercicio de un derecho de oposición en relación con el tratamiento de datos procedentes de fuentes accesibles al público como pueden ser repertorios telefónicos, listados de personas que pertenecen a grupos profesionales o un eventual censo promocional, donde no se ejercita ningún derecho fundamental –salvo, en su caso, la libertad de empresa, que no tiene una posición preferente en nuestro sistema constitucional–, que el ejercicio del derecho

274. La responsabilidad de quien lleva a cabo la publicación –medio de comunicación, diario oficial– y de los buscadores se ha analizado *supra* apdo. V.D).

275. Hemos analizado anteriormente las dificultades del ejercicio del derecho de oposición y de cancelación frente a los buscadores –*supra* apdo. V.D)–.

de oposición en relación con los tratamientos de datos personales que llevan a cabo los buscadores y que tienen su origen en los medios de comunicación o en tratamientos con fines periodísticos o de expresión literaria o artística porque estos se encuentran protegidos por el ejercicio de una libertad preferente que es garantía de una opinión pública libre dentro de una sociedad democrática. Hasta ahora las posibles intromisiones en los derechos de las personas ocasionados por el ejercicio de la libertad de información han sido resueltas por los Tribunales, en virtud de lo previsto en la Ley Orgánica 1/1982 por la vía preferente y sumaria del amparo civilp y a través de la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación. No parece razonable afirmar que corresponde a los buscadores la limitación de la información que publican los medios de comunicación en Internet, de manera que, a petición de los interesados, tuvieran que limitar la buscabilidad de una información que, además, continua publicándose por los medios de comunicación en Internet. Posiblemente los buscadores disponen de medios técnicos para no buscar una información relativa a una persona. Sin embargo, sin querer entrar a analizar ahora la naturaleza de Internet, nos parece esencial que en la Red nque es sobre todo un espacio de libertadq los buscadores sean herramientas neutrales y no establezcan ningún tipo de censura previa. Es un peligro que la herramienta deje de ser neutral, que alguien sea buscado o no sea buscado en función de que lo determine el propio interesado o el buscador[276].

A nuestro juicio, la libertad de expresión incluye dentro de su contenido la búsqueda, recepción y difusión de ideas a través de Internet. Los buscadores son herramientas indispensables para el libre acceso a la información. Los ciudadanos tienen por ello un derecho a buscar información en Internet y acceder a ella. Los límites a la libertad de circulación de contenidos en Internet y a la búsqueda de la información también suponen límites a la libertad de expresión y de información. Además, los buscadores no están en condiciones de determinar o no la veracidad, la exactitud, el mayor o menor interés público de la información que se publica en Internet, ya que son sólo herramientas de bús-

276. El concepto de neutralidad de la red se basa en la idea de que la información en Internet debe ser transmitida con imparcialidad, sin tener en cuenta el contenido, el destino o el origen. Existe una «Comunicación de la Comisión Europea sobre neutralidad de la red y una Internet abierta en Europa», de 19 de abril de 2011 (COM (2011) 222 final). El Supervisor Europeo de Protección de Datos ha emitido también un Dictamen sobre la neutralidad de la red, donde incide en que la supervisión por parte de los proveedores de Internet de las comunicaciones de los usuarios puede violar las normas sobre la protección de datos personales y la confidencialidad de las comunicaciones. Así, establece la necesidad de que se señalen las áreas donde las prácticas de inspección son legítimas, por ejemplo, aquellas necesarias para garantizar la fluidez del tráfico [lo que puede parecer cuestionable, a nuestro juicio, ya que esto puede hacerse disociando la información, además de que esta injerencia no superaría el juicio de proporcionalidad en sentido estricto] o por motivos de seguridad; determinar también cuándo dicha supervisión requiere el consentimiento previo de los usuarios, por ejemplo en el caso de la utilización de filtros que tienen como objetivo limitar el acceso a ciertas aplicaciones y servicios, como el llamado «peer to peer». Cfr. el Dictamen en *www.edps.europa.eu*

queda de información. Por ello, cualquier reclamación de los ciudadanos por la información que aparece publicada en Internet ,incluida la solicitud de cancelación de la publicación de la informaciónl tienen que dirigirla a los responsables de los sitios *web*, que son también responsables del tratamiento principal, sobre todo cuando éste es conocido es el caso de un medio de comunicación, o como hemos señalado en un apartado anterior, de un boletín oficial o de una página *web* institucional en Internet de una Administración Pública[277]. Esta es una

277. Hay que resaltar también en Argentina el asunto C 7181/2008 I, *Miragaya Eduardo Daniel c/ Yahoo! de Argentina S.R.L y otras medidas cautelares*, de 23 de diciembre de 2008, donde el Fiscal Federal de la Nación pidió a *Yahoo!* y a *Google* el bloqueo de su nombre y de cualquier tipo de información relativa a su persona a la que se accede a través de sus respectivos portales, ya que manifestaba que al incluir su nombre en el campo de búsqueda «aparecía información deshonrosa, mendaz y temeraria sobre su actividad como Fiscal Federal de la Nación». En este caso, si bien inicialmente el Tribunal accedió a las medidas cautelares, posteriormente dictó una resolución de revocación. Entendió el Tribunal que el responsable principal era conocido se trataba de un medio de comunicacións y debía dirigirse a él: «No se advierte óbice para que el actor *dirija su pretensión contra los responsables de esos sitios y eventualmente debata con ellos la veracidad o exactitud de las noticias* que considera que lesionan su honor, cuestión que *Google y Yahoo! no están en condiciones de hacer, habida cuenta de que administran una herramienta de búsqueda de información*. En efecto, lo contrario implicaría ejecutar las medidas contra quienes no son los responsables de la concreta información a la que se atribuye consecuencias lesivas para el honor del actor, es decir contra quienes no son los habilitados para contradecir respecto de la materia que se debate en autos».

En cambio, en España, la Agencia Española de Protección de datos, como hemos señalado antes –*supra* apdo. V.D)–, ha atribuido la responsabilidad, obligando a cancelar la publicación, únicamente a Google y nunca a la Administración General del Estado o al medio de comunicación. Así, en relación con las Resoluciones de tutela de derechos de la Agencia Española de Protección de Datos que obligan a *Google* España a cancelar la información en sus motores de búsqueda y que han sido recurridas a la Sala de lo Contencioso Administrativo de la Audiencia Nacional, el Auto de 27 de febrero de 2012 de ésta ha planteado una cuestión prejudicial en relación con la actividad de los buscadores como proveedores de contenidos en relación con la Directiva 95/46/CE de Protección de Datos. Así, en relación con la actividad del buscador de la empresa «Google» en internet consistente en localizar la información publicada o incluida en la red por terceros, indexarla de forma automática, almacenarla temporalmente y finalmente ponerla a disposición de los internautas con un cierto orden de preferencia, cuando dicha información contenga datos personales de terceras personas, plantea la Audiencia Nacional si debe interpretarse una actividad como la descrita comprendida en el concepto de «tratamiento de datos» contenido en el art. 2.b de la Directiva 95/46/CE, lo que obviamente merece una respuesta afirmativa. Igualmente señala si debe interpretarse el artículo 2.d) de la Directiva 95/46/CE, en el sentido de considerar que la empresa que gestiona el buscador «*Google*» es «responsable del tratamiento» de los datos personales contenidos en las páginas *web* que indexa –obviamente, como hemos señalado en el texto, el buscador es responsable de sus propios tratamientos, no de los realizados por los medios de comunicación o por la Administración–. En tercer lugar, la Audiencia Nacional pregunta si puede la autoridad de protección de datos, tutelando los derechos contenidos en el art. 12.b) y 14.a) de la Directiva 95/46/CE, requerir directamente al buscador de la empresa «Google» para exigirle la retirada de sus índices de una información publicada por terceros, *sin dirigirse previa o simultáneamente al titular de la página web en la que se ubica dicha*

cuestión que hemos mantenido tradicionalmente[278] y que aparece ahora recogida en la propuesta de Reglamento que señala que cuando el responsable haya hecho públicos los datos personales, es éste el que está obligado a adoptar las medidas razonables –incluidas las técnicas– para informar a los terceros que están tratando dichos datos de que un interesado les solicita que supriman cualquier enlace a estos datos personales, o cualquier copia o réplica de los mismos –art. 17.2–, de forma que cualquier ejercicio de derechos tiene que dirigirse al responsable del tratamiento de datos con fines periodísticos o de libertad de expresión, y no al buscador. Ya hemos señalado en otro momento de este trabajo que no nos parece razonable responsabilizar al buscador por encontrar una información administrativa que se publica en un boletín oficial en Internet y, al mismo tiempo, eximir a la Administración de bloquear la publicidad o de establecer límites a la indexación por buscadores a través de protocolos «NO ROBOT». Quien es capaz de determinar si existe o no un interés público que justifique todavía el mantenimiento de la publicación o la veracidad de un concreto dato no puede ser el robot de *google* sino quien ordenó la publicación. No obstante, sí existe una responsabilidad de los buscadores sobres sus tratamientos en su memoria caché –de cancelarlos cuando se haya cancelado la fuente principal–, por lo que existe una responsabilidad compartida entre *web máster* y buscadores, lo que debe llevar también a buscar soluciones compartidas.

Dicho esto, hay que reconocer que existen determinadas publicaciones en sitios *webs* en Internet que utilizan la imagen de la persona sin su consentimiento, vulnerando su intimidad o dañando su honor gravemente. Este sería el caso, por ejemplo, de *webs* que utilizan indebidamente la imagen de una persona, haciendo referencia a actividades relacionas con el mercado del sexo o la

---

información –nosotros hemos defendido en el apdo. V.D) que hay que dirigirse simultáneamente a ambos. En cuarto lugar, se pregunta si se excluiría la obligación de los buscadores de tutelar estos derechos cuando la información que contiene los datos personales se haya publicado lícitamente por terceros y se mantenga en la página web de origen-ya hemos respondido en texto que estaría excluida esta obligación porque si el tratamiento de la *web máster* se encuentra fundamentado en la libertad de expresión se mantiene, también puede mantenerse el del motor de búsqueda–. Por último, en relación con el derecho de cancelación y/oposición y el derecho al olvido se plantea si debe interpretarse que los derechos de supresión y bloqueo de los datos, regulados en el art. 12.b) y el de oposición, regulado en el art. 14.a) de la Directiva 95/46/CE comprenden que el interesado pueda dirigirse frente a los buscadores para impedir la indexación de la información referida a su persona, publicada en páginas web de terceros, amparándose en su voluntad de que la misma no sea conocida por los internautas cuando considere que puede perjudicarle o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros –ya hemos señalado que si la publicación se encuentra amparada por la libertad de información y de expresión es lícita, no existiría derecho al olvido en este caso, como aclara el art. 17.3 de la propuesta de Reglamento, tampoco ante los buscadores–.

278. Este planteamiento lo habíamos mantenido en «Transparencia administrativa y protección de datos personales», *loc. cit.* pp. 101 y 112 y *La protección de datos personales*, cit. pp. 197-212 816-831.

pornografía, y que en absoluto estarían amparadas en la libertad de expresión y de información. La protección del derecho al honor, a la intimidad o a la imagen en Internet se complica al publicarse frecuentemente esta información en *webs* de difícil localización, de forma que es complejo determinar quién es el responsable final del tratamiento de esta información. Los particulares que ven sus derechos vulnerados tienen que dirigirse al portal *web* que vulnera sus derechos para solicitar la cancelación inmediata de la publicidad de esta información. Pero, al mismo tiempo, pueden dirigirse a los buscadores para solicitar la cancelación de la información que se encuentra en su memoria caché. En ocasiones, los responsables de la *web* sobre todo si es conocidas cancelan la publicación de la información. No tendría sentido que la página *web* principal borrara la información y el buscador siguiera ofreciéndola, por lo que en este caso sí existiría una clara responsabilidad de los buscadores por sus propios tratamientos. Sin embargo, en otras ocasiones, no se puede localizar al responsable de la *web* o éste no cancela la publicación de la información. En ese caso, es razonable que el interesado, sin perjuicio del inicio de las acciones judiciales correspondientes contra el responsable de la *web*, se dirija al buscador para solicitar que bloquee la publicidad de sus datos personales que aparecen en determinadas *webs*. Si bien los buscadores son inicialmente reacios a este tipo de acciones que limitan el libre acceso a la información, no obstante tienen que implantar mecanismos de autorregulación y de privacidad en el diseño que permitan bloquear la búsqueda de una información cuando manifiestamente ésta supone una vulneración del derecho al honor, a la intimidad o a la imagen de las personas por ejemplo, cuando se da publicidad como prostituta a alguien que no lo esp. Así, por ejemplo, *youtube* o incluso redes sociales como *Tuenti* tienen instrumentos de autorregulación, y cuando existe una denuncia relativa a sexo explícito, contenido xenofobo o uso de imagen sin consentimiento retiran esa información de Internet[279]. Lo mismo debe hacer en este caso los buscadores, poniendo límites a la indexación de algunas *webs*, sin perjuicio del ejercicio de las acciones judiciales por el interesado. Es muy importante, en este punto, la autorregulación de los propios buscadores, que no deben esperar en ocasiones a una resolución judicial mientras se siguen vulnerando derechos. El ciudadano también podrá reclamar como medida cautelar dentro de un procedimiento judicial que el juez dicte una resolución dirigida a la página *web* principal para que bloquee la publicidad y al buscador para que deje de reproducir esta información.

Los buscadores tienen obligación de acatar las medidas cautelares que establece un juez[280]. Hay que señalar que esta resolución judicial que limita el

279. Hay que analizar en el ámbito de los tratamientos de datos con fines de libertad de expresión la posibilidad que brinda para la autorregulación la aprobación de códigos tipo. Cfr. TASCÓN LÓPEZ, R., «Los Códigos Tipo para la protección de datos personales», *REPD*, núm. 7, 2010, pp. 151-181; CAZURRO BARAHONA, V., *op. cit.* pp. 312-332.

280. Por ejemplo, en Argentina, *Google* sigue adelante con la publicación cuestionada a pesar de la orden judicial en contra, mientras que *Yahoo!* acata la resolución, incorporando un texto donde explica que no puede mostrar el *link* porque existe una medida judicial que así lo impide.

acceso a la información en Internet no vulnera la libertad de información y de expresión, que debe ser compatibilizada con otros derechos también de rango constitucional como la intimidad, el honor o la propia imagen[281]. Tampoco debe entenderse como censura, ya que la información ha podido ser buscada, reproducida, almacenada y difundida libremente. En todo caso, es necesario que la medida cautelar que se establezca sea proporcional. Así, es excesivo impedir todas las búsquedas por un nombre de manera indefinida, ya que esto sí supondría un supuesto de censura previa. Bastaría bloquear aquella información que vulnera derechos, dejando aquella otra que es crítica o desagradable pero respetuosa con el honor, la intimidad o la imagen, ya que en caso contrario sí que se estaría vulnerando la libertad de información y de expresión[282].

Por ello, es necesario en este punto un pronunciamiento más claro del legislador en nuestro país, que tenga en cuenta que la publicación de los medios de comunicación en Internet y los tratamientos de datos personales por los ciudadanos con fines periodísticos o de expresión literaria o artística incrementan tanto la libertad de información y de expresión y la opinión pública libre como las posibles vulneraciones a los derechos de otras personas. Igualmente, es necesario materializar el principio de calidad como principio de exactitud en el ámbito de los medios de comunicación y relacionar el derecho de rectificación de la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación, con el derecho de rectificación y cancelación de la propuesta de Reglamento –en la actualidad de la LOPD–. La Ley Orgánica 2/1984, de 26 de marzo, mantiene la necesidad de que el director del medio de comunicación publique o difunda íntegramente la rectificación, dentro de los tres días siguientes al de su recepción, con relevancia semejante a aquella en que se publicó o difundió la información que se rectifica, sin comentarios ni apostillas (art. 3), una regulación que estaba pensada para la edición impresa en papel pero no para la edición electrónica y que, lógicamente, no ha previsto la cancelación len este caso, el bloqueoe de la versión electrónica de estas noticias en Internet si se alcanza una sentencia favorable. A esto se une las dificultades que plantea que una autoridad administrativa de protección de datos personales limite el ejercicio de la libertad de expresión e información. Por ello, es necesaria la aprobación de una legislación que resuelva los conflictos que plantea la publicidad de los medios de comunicación y de los tratamientos de datos personales con fines

281. Hay que mencionar en Argentina el Expte. n.º 67.068 (23.392/07), *Mazza, Valeria Raquel c/ Yahoo! de Argentina S.R.L y otros s/medidas precautorias*, que llevó el abogado Gustavo Tanús.

282. En el asunto antes citado *Miragaya Eduardo Daniel c/ Yahoo! de Argentina S.R.L*, donde el Fiscal Federal de la Nación pidió a los buscadores el bloqueo de su nombre y de cualquier tipo de información relativa a su persona, el Tribunal señaló que el estándar de responsabilidad por la difusión de noticias inexactas resulta menos riguroso frente a los funcionarios públicos. Así, a nuestro juicio, la difusión de información relativa a un fiscal general tiene interés público. Tampoco parece razonable prohibir la exhibición de imágenes en *Google*, ya que se refieren a actos públicos de una persona que ocupa un cargo público.

periodísticos en Internet y su accesibilidad indiscriminada e ilimitada en el tiempo a través de los buscadores[283].

El tercer requisito que debe cumplir cualquier limitación del derecho fundamental a la protección de datos personales es el respeto al principio de proporcionalidad, una exigencia que se encuentra en la Carta de los Derechos Fundamentales de la Unión Europea, en el CEDH y en la jurisprudencia constitucional. Así, el art. 52.1 de la Carta de los Derechos Fundamentales de la Unión Europea señala que «cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta debe respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o la necesidad de protección de los derechos y libertades de los demás». Por tanto, no es suficiente que exista una previsión legal o que la limitación al derecho a la protección de datos personales se justifique en una finalidad legítima; debe respetar el equilibro entre derechos, teniendo en cuenta su contenido esencial y el principio de proporcionalidad. Este principio de proporcionalidad aparece claramente en la propuesta de Reglamento[284] que establece que los Estados miembros sólo podrán limitar los principios y derechos de protección de datos «cuando tal limitación constituya una medida necesaria y proporcional *en una sociedad democrática*» –art. 21.1–, una expresión tomada del CEDH[285].

---

283. Esta cuestión la hemos analizado con más profundidad en *La protección de datos personales*, cit. pp. 206-211 y 760-905.

284. Como señala la Exposición de Motivos de la propuesta de Reglamento, el principio de proporcionalidad requiere que «cualquier intervención tenga una finalidad específica y no vaya más allá de lo necesario para alcanzar sus objetivos. Este principio ha servido de guía en la elaboración de la presente propuesta, desde la identificación y evaluación de las opciones políticas alternativas a la redacción de la propuesta legislativa». El dictamen del Comité de Evaluación de Impacto, de 9 de septiembre de 2011, también añadió una sección sobre proporcionalidad.

285. Este principio de proporcionalidad ha sido expresado de manera distinta en los diferentes textos normativos. Así, el CEDH señala que las injerencias deben ser «necesarias en una sociedad democrática». De hecho, todos los artículos del CEDH que fijan límites a los derechos establecen como criterio de justificación que *«sean necesarios para una sociedad democrática»*. En esta dirección, el TEDH ha considerado que no basta para que una intromisión sea legítima que persiga un fin legítimo, como la seguridad nacional o el orden público, y que esté prevista en una ley. Deben existir razones graves que justifiquen que las injerencias «son necesarias en una sociedad democrática». El juicio de si una injerencia es «necesaria para una sociedad democrática» se realiza a través del principio de proporcionalidad. Este principio, si bien no se recoge en ninguna disposición del CEDH, ha sido utilizado por el TEDH, aunque con una aproximación distinta. El TEDH no lleva a cabo una diferenciación del principio de proporcionalidad en tres juicios o tres subprincipios sino que lo hace en dos momentos: en primer término, determina la necesidad de la medida en una sociedad democrática –que coincidiría con los subprincipios de necesidad y de adecuación–; y, en segundo lugar, tiene en cuenta la proporcionalidad en sentido estricto de la medida, ponderando los medios empleados y los fines perseguidos –que coincidiría con el subprincipio de la proporcionalidad en sentido estricto–. Para el TEDH una medida es *necesaria* cuando existe «una exigencia social imperiosa». Debe existir un motivo

El principio de proporcionalidad implica la realización de varios juicios donde se valora conjuntamente el límite al derecho fundamental –la injerencia en la protección de datos personales– y el fin que se pretende –la finalidad legítima antes analizada–. Así, el principio de proporcionalidad es concebido en el Derecho Público Europeo –especialmente en el Derecho Alemán– y se ha trasladado al Derecho de la Unión Europea y a la propia jurisprudencia constitucional como un principio que se subdivide en tres subprincipios: el de racionalidad, el de necesidad y el de proporcionalidad en sentido estricto[286]. De esta forma, para que una intromisión supere el juicio de proporcionalidad debe pasar a la vez tres juicios: el juicio de racionalidad, el juicio de necesidad y el juicio de proporcionalidad en sentido estricto[287]. Así, en primer lugar, la intromisión en el derecho fundamental a la protección de datos personales tiene que superar el juicio de racionalidad o de adecuación de los medios a los fines, de forma

justo, pertinente y suficiente que lleve al Estado a limitar un derecho fundamental. Si no existen motivos suficientes la medida no será necesaria y, por lo tanto, no estará justificada. En segundo lugar, la medida debe ser necesaria *en una sociedad democrática* lo que significa que debe ser necesaria de acuerdo con un valor común europeo que es la garantía de los derechos fundamentales. Por tanto, para valorar si una injerencia es legítima el TEDH comprueba si la medida adoptada por los poderes públicos es «necesaria para una sociedad democrática». Utilizando el principio de proporcionalidad se comprueba si existe una «exigencia social imperiosa» y, sobre todo, si la medida adoptada es proporcionada en sentido estricto al fin legítimo perseguido. El Tribunal de Estrasburgo entendió que los Estados disponen de un cierto margen de apreciación pero le corresponde al Tribunal la última palabra si estas limitaciones son compatibles con el CEDH. Así, en el caso *Silver* (1983) el TEDH resumió los principios que se derivaban del requisito de una «necesidad democrática». El Tribunal de Estrasburgo entendió que la frase «necesario en una sociedad democrática« significaba que la injerencia se debía corresponder con una «urgente necesidad social» o «necesidad social imperiosa» y ser proporcionada al fin legítimo perseguido; mantuvo que la expresión «necesario» no era sinónimo de «indispensable», ni tenía la misma flexibilidad que las expresiones «admisible», «ordinario», «útil», «razonable» o «deseable»; además, señaló que los artículos del CEDH que permitiesen límites al derecho garantizado tenían que ser interpretados de forma restrictiva. Cfr. ARENAS RAMIRO, M., *op. cit*. pp. 119-122 y 143-144.

286. Cfr. MEDINA GERRERO, M., «El principio de proporcionalidad y el legislador de los Derechos Fundamentales», *Cuadernos de Derecho Público*, núm. 5, 1998, pp. 119-141 y GONZÁLEZ BEILFUSS, M., *–El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional*, Aranzadi, Pamplona, 2003– analiza cómo el Tribunal Constitucional tiene en cuenta las alegaciones de los recurrentes y del Ministerio Fiscal para valorar las posibles medidas alternativas que podrían suponer un menor nivel de injerencia y, por tanto, el cumplimiento o no del principio de proporcionalidad.

287. Como señala la STC 207/1996, de 16 de diciembre, «[p]ara comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)». Cfr. también las SSTC 66/1995, de 5 de mayo, 134/1999, de 15 de julio, y 70/2009, de 23 de marzo.

que la limitación es considerada desproporcionada si no sirve para alcanzar el fin legítimo. En segundo lugar, la intromisión debe superar el juicio de necesidad, que obliga a buscar siempre la medida más moderada para alcanzar la finalidad con la misma eficacia, de forma que si se opta por una limitación al derecho fundamental a la protección de datos personales, existiendo otros medios menos gravosos con este derecho para alcanzar el mismo fin, se entiende que la limitación es desproporcionada porque no es necesaria –no pasa el juicio de necesidad–. En tercer lugar, la intromisión en el derecho a la protección de datos debe superar el juicio de proporcionalidad en sentido estricto que exige que la medida adoptada –la injerencia en el derecho fundamental a la protección de datos personales– sea proporcional al fin que se persigue, teniendo en cuenta la naturaleza del derecho lesionado, la intensidad de la injerencia y el bien o valor constitucional que se persigue. No basta con que la limitación a la protección de datos personales sea adecuada para alcanzar un fin ni que sea una medida necesaria –no haya ninguna medida menos gravosa para alcanzar el mismo fin–. Es necesario, además, que exista una proporcionalidad entre la medida adoptada –la injerencia en el derecho fundamental a la protección de datos personales– y el fin que se persigue. Se trata de una ponderación entre dos bienes constitucionales –el derecho fundamental a la protección de datos personales, que va a ser limitado, y otro bien o valor constitucional que se pretende alcanzar con el tratamiento de datos personales–. Lógicamente, debe tratarse de dos bienes o valores constitucionales con semejante garantía. Se lleva a cabo un *balancing* –una ponderación– entre dos derechos fundamentales, un análisis de coste-beneficio acerca de si el coste de la limitación del derecho fundamental a la protección de datos personales es proporcionado en sentido estricto con el fin legítimo –con el beneficio– que se pretende conseguir. La injerencia respeta el principio de proporcionalidad en sentido estricto cuando la medida es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto. Se entiende que la medida no pasa el juicio de proporcionalidad en sentido estricto si el fin que se pretende es menos importante que la limitación al derecho fundamental a la protección de datos personales.

Por tanto, el principio de proporcionalidad en sentido estricto conlleva una ponderación de los límites al derecho fundamental a la protección de datos personales y los bienes o valores constitucionales que se pretenden alcanzar, de forma que el esfuerzo para alcanzar un fin no implique un coste excesivo o desproporcionado. Para determinar si la intromisión es desproporcionada, es necesario tener en cuenta cuál es el tipo de lesión que se va imponer al derecho fundamental –limitación al principio de información, de consentimiento, a la cancelación de los datos, al derecho de acceso, etc.–, que tipo de datos van a ser objeto de tratamiento –si van a tratarse datos de especial protección– y qué garantías se han previsto para asegurar el respeto al derecho fundamental. También hay que valorar si el fin que se pretende es un bien o valor constitucional relevante. Por último, habrá que tener en cuenta el interés individual de las

personas a las que se limita el derecho fundamental y la existencia o no de un interés general.

El principio de proporcionalidad es clave a la hora de analizar la legitimidad de la publicación de información personal por la Administración, donde es necesario buscar un equilibrio entre el interés público que justifica el acceso a información administrativa y el derecho fundamental a la protección de datos[288]. Se trata de llevar a cabo una ponderación que tenga en cuenta el tipo de interés público que demanda la transparencia administrativa y el nivel de injerencia en el derecho fundamental a la protección de datos personales[289]. Existe, muchas veces, un claro interés público .vinculado, por ejemplo, a la libertad de información, a la participación política, al control de la actividad administrativa o a la igualdad en las relaciones con la Administraciónl, que prevalece sobre el derecho fundamental a la protección de datos personales y que justifica el acceso a información personal. En otras ocasiones, el interés público no justifica el acceso o una difusión generalizada de datos personales. *La clave es tratar de alcanzar este interés público Lque justifica el acceso a información administrativaq con el menor nivel de injerencia, con la menor restricción posible del derecho fundamental a la protección de datos personales*. Esto obliga a analizar en cada uno de los supuestos de hecho el interés público presente, el nivel de publicidad, el plazo de cancelación y la tipología de datos personales sobre la que se quiere realizar el acceso[290]. Inicialmente, esta valoración debe ser realizada por el legis-

---

288. En la misma dirección, es necesario reformar la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15.3.2006, sobre conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes de comunicaciones, teniendo en cuenta el principio de proporcionalidad, en relación con el plazo de conservación de los datos, las personas que pueden acceder a los mismos y los fines que lo justifican.

289. Sobre la necesidad de una conciliación entre el derecho de acceso a documentos administrativos y la protección de datos personales, cfr. los Dictámenes del Grupo de Trabajo del Artículo 29 5/2001, de 17 de mayo, en relación a un Informe Especial del Defensor del Pueblo Europeo, y 3/1999, de 3 de mayo, relativo a la «Información del sector público y protección de los datos personales, cit.; cfr. también la Recomendación del Consejo de Europa núm. R (91) 10, de 9 de septiembre, sobre la comunicación a terceros de datos de carácter personal en poder de organismos públicos.

290. Esta es una cuestión que hemos analizado en *La protección de datos personales*, cit. pp. 760-797 Es más fácilmente aplicable el principio de calidad a la publicidad de la actividad administrativa en Internet que a los tratamientos de datos que llevan a cabo los medios de comunicación porque la Administración no ostenta ningún derecho fundamental sino desarrolla competencias en virtud del principio de legalidad, salvo algunos supuestos donde sí estaría actuando como un medio de comunicación en ejercicio de la libertad de información como en la publicación en los canales institucionales en Internet de las Administraciones Públicas de vídeos e imágenes de actos públicos, destinados tanto a las propias empresas informativas como al público en general y donde existe un interés público vinculado al principio democrático. En este supuesto, la publicación de datos personales npor ejemplo, de imágenes de los asistentesp sin su consentimiento se encontraría habilitada por el art. 20 CE y por el art. 9 de la Directiva 95/46/CE.

Los criterios que hemos expuesto en otro momento para aplicar el principio de proporcionalidad al acceso a información administrativa y a la publicación de datos perso-

lador, ya que los límites a los derechos fundamentales están sometidos a reserva de ley. Esta legislación no elude que el órgano administrativo lleve a cabo un análisis concreto para garantizar que el acceso a información administrativa respeta el principio de calidad y de proporcionalidad[291].

F) Las autoridades independientes de control y los mecanismos de coherencia.

---

nales por parte de la Administración no se pueden trasladar acríticamente a los medios de comunicación. Así, no es aplicable a los medios de comunicación lo relativo a los niveles de acceso –no se puede afirmar que el comunicador debe optar por el medio que facilitando la información al ciudadano y cumpliendo el interés público suponga la menor intromisión en el derecho fundamental a la protección de datos personales–. Tampoco es aplicable a los tratamientos de datos personales que llevan a cabo los medios de comunicación el principio de finalidad y, en especial, la obligación del mantenimiento de la finalidad original. De la teoría que hemos expuesto en otro momento para el ámbito de la transparencia administrativa sólo puede aplicarse a la publicación por los medios de comunicación lo referido a la tipología de datos, la disociación de la información, la cancelación y el bloqueo, el derecho de rectificación, el de oposición y el *balancing* entre la injerencia en la protección de datos personales y la existencia o no de un interés público

291. Hemos aplicado el principio de proporcionalidad a la hora de analizar la legitimidad de algunos tratamientos de datos personales que suponen injerencias en este derecho fundamental, como es el caso de los tratamientos de datos biométricos –*ibídem* pp. 215-243–. Muchas limitaciones de los derechos a la privacidad personal –a la intimidad personal y familiar– y a la integridad física han sido resueltas teniendo en cuenta el principio de proporcionalidad. Así, en el caso de la intimidad corporal, el Tribunal Constitucional entendió que el corte de pelo y tonsura de axilas de un sospechoso en un proceso judicial sobre delitos contra la salud pública no superara el test de proporcionalidad y que, por tanto, lesionaba su derecho a la integridad física –STC 207/1996, de 16 de diciembre–. En la STC 98/2000, de 10 de abril –caso *«Micrófonos en el casino de La Toja»*–, el Tribunal constitucional entendió que la grabación permanente de las conversaciones de un trabajador a lo largo de su jornada laboral no era proporcional a la finalidad perseguida, que era garantizar la seguridad –no respetaba el criterio del mínimo sacrificio posible de los derechos fundamentales–. En cambio, en la STC 186/2000, de 10 de julio, el Tribunal entendió que la instalación de cámaras en las cajas registradoras del economato de ENSIDESA era una medida proporcional ante las irregularidades detectadas en las mismas –era una medida idónea, era necesaria y era equilibrada porque se ciño a una zona de la caja de la empresa y por un espacio de tiempo limitado–. El mismo principio de proporcionalidad debe aplicarse al control del correo electrónico dentro de la relación laboral. Cfr. CARRILLO, M, , *op. cit*. pp. 108-109 y 135-139 y GOÑI SEIN, J., *La videovigilancia empresarial y la protección de datos personales*, Civitas, Cizur Menor, 2007, pp. 106-142. El Tribunal Constitucional ha señalado que cualquier medida que suponga un límite al derecho a la intimidad de las personas y al derecho a la integridad física en el ámbito penal debe respetar el principio de proporcionalidad –SSTC 37/1989, de 15 de febrero; 85/1994, de 14 de marzo; y 54/1996, de 26 de marzo–. Así, como señala la Sentencia del Tribunal Constitucional 207/1996, de 16 de diciembre, «una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad».

El establecimiento en los Estados miembros de autoridades de control que ejerzan sus funciones con plena independencia constituye para la propuesta de Reglamento un *elemento esencial* para la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal –Considerando 92–. Por ello, la propuesta de Reglamento refuerza la independencia de estas autoridades de control –arts. 46-50–[292], algo que se encontraba brevemente mencionado en la Directiva pero que recibe ahora un amplio desarrollo, tanto en lo relativo a las garantías formales de independencia –incompatibilidad e inamovilidad, autonomía de personal, presupuestaria y de medios materiales– como a las garantías sustanciales de independencia –ausencia de órdenes e instrucciones–[293], teniendo en cuenta la jurisprudencia del TJUE[294]. Muchas de estas cuestiones se encuentran ya bien resueltas en la legislación española pero no tanto en la del resto de Estados de la Unión –como ha sido el caso de Alemania–, por lo que la propuesta de Reglamento exige que cada Estado miembro incorpore estas garantías por Ley. Al mismo tiempo, la propuesta de Reglamento respeta el principio de autonomía institucional, ya que establece que cada Estado miembro dispondrá de una o de varias autoridades públicas que se encarguen de ejecutar la normativa de protección de datos personales –lógicamente,

292. Buena muestra de la importancia de independencia de las autoridades de control es que tanto la Carta de los Derechos Fundamentales de la Unión Europea –art. 8.3– como el malogrado proyecto de Constitución Europea –I-51.3– establecían que el respeto a las normas de protección de datos personales debe estar sujeto al control de una autoridad independiente. En la misma dirección, la Comisión ya señalaba en el *Segundo Informe de aplicación de la Directiva*, cit. que «una preocupación es el respeto por el requisito de que las autoridades supervisoras de protección de datos actúen con total independencia y tengan poder y recursos suficientes para llevar a cabo sus tareas» –p. 6–. Así, en el caso *Rotaru*, de 4 de mayo de 2000, el TEDH consideró que la inexistencia de un procedimiento que asegure los derechos del interesado y controle la actividad de la Administración supone una vulneración de la legislación de protección de datos

293. Llama la atención la referencia a que los miembros de las autoridades de control deben ser elegidos entre personas que ofrezcan «absolutas garantías de independencia y que posean experiencia y aptitudes acreditadas para el ejercicio de sus funciones, en particular, en el ámbito de la protección de datos personales» y que tras la finalización de su mandato, los miembros de la autoridad de control actuarán con integridad y discreción en lo que respecta a la aceptación de cargos y beneficios, una referencia genérica que trata de evitar la captura de las autoridades por intereses privados, cuestiones que no estaban recogidas ni en la Directiva ni en la LOPD. La propuesta de Reglamento admite la posibilidad de que la autoridad esté sujeta a control financiero, sin que ello afecte a su independencia –art. 47–, una cuestión que hemos defendido en otro momento en relación con el control de legalidad del gasto y la fiscalización previa por parte de la Intervención –cfr. *La protección de datos personales*, cit. pp. 1.723-1.827, esp. 1748-1765–.

294. Sentencia, de 9 de marzo de 2010, Comisión/Alemania (C-518/07, Rec. 2010, p. I-1885). La propuesta de Reglamento incorpora también las garantías de independencia –especialmente en lo relativo a las condiciones generales de los miembros de la autoridad de control del art. 48– previstas en el Reglamento (CE) núm. 45/2001, ya citado, sobre 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.

consecuencia de un modelo de Estado más o menos centralizado y de la existencia de entidades subnacionales o Comunidades Autónomas que hayan asumido estas competencias-[295] y que los miembros de la autoridad de control pueden ser nombrados tanto por el Parlamento como por su Gobierno –art. 48–.

Uno de los ámbitos donde se produce una mayor disparidad entre los Estados miembros es en la capacidad coercitiva de las autoridades de control. El art. 25 de la Directiva ya establecía que los Estados miembros deben disponer de autoridades de control que «vigilen» su aplicación. 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, el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso la posibilidad de prohibir provisional o definitivamente un tratamiento, 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 Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial[296]. Estas decisiones de la autoridad de control podrán ser objeto de recurso jurisdiccional. Sin embargo, la Comisión ha señalado como una de las causas del bajo cumplimiento de la Directiva –y de las divergencias entre los Estados miembros– la reducida capacidad coercitiva de las autoridades de control de algunos Estados. Así, la Comisión ha señalado que las autoridades de control tienen una amplia variedad de cometidos entre los que las acciones coercitivas tienen poca prioridad; además, como hemos señalado anteriormente, este esfuerzo coercitivo se encuentra dotado con recursos insuficientes[297]. Todas las autoridades de protección de datos, de una manera o de otra, tienen la responsabilidad de investigar las posibles vulneraciones de la normativa de protección de datos dentro de su ámbito competencial, investigación que puede ser consecuencia de una propuesta de trata-

295. Lógicamente, se prevé que exista un solo interlocutor a nivel de cada Estado miembro en el Consejo Europeo y que todas las autoridades subnacionales deban cumplir las normas relativas al mecanismo de coherencia –art. 46–.

296. El Considerando 63 de la Directiva señala que las autoridades de control deben disponer de los medios necesarios para cumplir su función como son los poderes de investigación o de intervención, en particular en aquellos supuestos de reclamaciones presentadas a la autoridad, o la capacidad de comparecer en juicio. Igualmente se establece que los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido –art. 23–. También se señala que los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de la Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento –art. 24–.

297. Cfr. el *Primer informe sobre la aplicación de la Directiva*. cit.. Cfr. también el apartado de *Investigative powers* del *Analysis and impact study on the implementation of Directive*. cit..

miento notificado a la Agencia o de una queja del titular de los datos. La propia Comisión es consciente de que, a excepción de España, donde se llevan a cabo cientos de actuaciones de inspección cada año, la mayoría de las autoridades de control desarrollan pocas inspecciones, aunque cuando éstas se realizan, son detalladas y en profundidad[298]. Una especial divergencia se encuentra en el régimen sancionador. Así, si bien la mayoría de los países atribuyen formalmente a las autoridades de control la posibilidad de imponer sanciones económicas, en la práctica, esto sólo se utiliza como último recurso, con la excepción de España y Portugal que lo hacen habitualmente. Por tanto, existe una importante divergencia tanto en la actividad inspectora de las Autoridades de Control como en la gravedad de las sanciones que éstas pueden imponer[299]. Las divergencias también proceden de una diferente voluntad de ejercer los instrumentos coercitivos –o en palabras de la Comisión Europea, una parte del problema se debe a una aplicación incompleta de las reglas–[300].

298. En ocasiones, algunas autoridades de protección de datos llevan a cabo puntualmente inspecciones sectoriales durante un periodo concreto de tiempo. En Holanda la autoridad de control realiza unas detalladas *privacy audits* sobre determinados responsables de ficheros para asegurar que todas las cuestiones son estrechamente analizadas. En la mayoría de los países las autoridades de control tienen atribuidas un amplio poder para acceder a los ficheros y a los sistemas de información empleados para el tratamiento de los datos. Sin embargo, la autoridad de protección de datos de Gran Bretaña sólo puede llevar a cabo inspecciones con el consentimiento del responsable del fichero o con autorización judicial.

299. Como señalamos tempranamente, «la mayoría de las Autoridades de Control de los países de la Unión Europea –a excepción de España y de Portugal– suelen tener un nivel de teorización bastante elevado sobre el derecho fundamental a la protección de datos personales –especialmente la Autoridad francesa y la italiana–, que no se ve refrendado ni por el contenido de las legislaciones de estos países, ni por las potestades que éstas atribuyen a las Autoridades de Control, ni por la actividad de inspección y sanción, que no llevan a cabo en realidad. Y aunque tengan estos poderes, no los ejercen por sus tradiciones jurídicas. La Autoridad alemana, además de estar encuadrada en el Ministerio del Interior, no desarrolla una labor real de inspección. La Autoridad italiana elige los temas que investiga y sólo lleva a cabo inspecciones puntuales. La Autoridad francesa hace básicamente deliberaciones, pero tampoco lleva a cabo inspecciones realmente. No obstante, la Comisión francesa tiene un importante poder político al ser sus miembros diputados. La Agencia de Gran Bretaña tiene que pedir permiso para hacer una inspección al responsable del fichero –orden de *enforcement*–. Si el responsable se niega, sólo le queda ir a los Tribunales. La Agencia irlandesa ha hecho una sola inspección en los últimos cinco años. Sólo Portugal y Grecia atribuyen poderes reales de inspección en materia de protección de datos, lo que no es decir mucho. En pocos ámbitos se ve tanta incongruencia entre lo que se predica en los foros internacionales y lo que efectivamente se lleva a cabo en los respectivos países. No existe realmente una tutela efectiva del derecho fundamental a la protección de datos personales en el ámbito europeo» –«La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional», *Cuadernos de Derecho Público*, núm. 19-20, 2003, pp. 314-315.

300. No obstante, esta situación estaba cambiando en los últimos años ya que las Autoridades de Protección de Datos Personales de la Unión Europea están descubriendo progresivamente la importancia del *enforcement*, cuestión ésta que fue abordada dentro de la *London Iniciative*. Así, recientemente ha sido modificada la legislación británica

La propuesta de Reglamento va directamente dirigida a resolver estos problemas, con una extensa regulación de las funciones y poderes de las autoridades de control –art. 52-54–, tratando de superar las deficiencias en las legislaciones de los Estados miembros –no en la española– en lo que hace referencia a los poderes de investigación y de sanción[301]. Además, lleva a cabo una intensa regulación de los recursos, responsabilidad y sanciones –arts. 73-79–, mejorando los instrumentos de reacción de los países de la Unión Europea[302]. El derecho a presentar una reclamación a la autoridad del control no es sólo del interesado sino también de toda organización o asociación que tenga por objeto la protección de los datos personales[303]. La propuesta de Reglamento aclara que las Agencias de Protección de Datos no serán competentes para controlar las operaciones de tratamiento efectuadas por los órganos jurisdiccionales en el ejercicio de su función jurisdiccional[304]. Cabe destacar especialmente que las

---

para dotar a la autoridad de aquel país de la capacidad de imponer importantes sanciones económicas.

301. Como señala el Considerando 9 de la propuesta de Reglamento, «la protección efectiva de los datos personales en la Unión no solo requiere que se refuercen y detallen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, sino también que se otorguen poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y se impongan sanciones equivalentes a los infractores en los Estados miembros». Hay que señalar que entre las funciones de las autoridades de control del art. 52 no se incluye sólo la investigación de las reclamaciones sino también fomentar el conocimiento de los ciudadanos en materia de riesgos, normas garantías y derechos. También se establece la obligación de las autoridades de control de elaborar informes anuales de actividad, algo que supone una obligación de transparencia hacia la sociedad y que tiene su antecedente en la publicación de un informe anual previsto en el art. 28.5 de la Directiva –lo que se materializa entre nosotros en la publicación de una memoria anual –art. 37.k)–.

302. También dentro del Capítulo dedicado al responsable y encargado del tratamiento se incluye una obligación de cooperación de éstos con la autoridad de control, facilitando la información, el acceso y la respuesta dentro del plazo razonable fijado por ésta –art. 29–.

303. Si bien el desempeño de las funciones de la autoridad de control es gratuito para el interesado, se incorpora una importante excepción cuando las solicitudes sean manifiestamente excesivas, en particular por su carácter repetitivo, lo que permitiría a la autoridad de control la posibilidad de exigir el pago de una tasa o decidir no adoptar las medidas solicitadas por el interesado, recayendo la carga de la prueba del carácter manifiestamente excesivo de la solicitud en la autoridad de control.

304. El Considerando 99 aclara que el Reglamento se aplica a las actividades de los órganos jurisdiccionales, si bien la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los primeros actúen en ejercicio de su función jurisdiccional, con el fin de garantizar la independencia de los jueces en el desempeño de sus funciones. No obstante, esta excepción debe limitarse estrictamente a verdaderas actividades judiciales en juicios y no debe aplicarse a otras actividades en las que puedan estar implicados los jueces, de conformidad con el Derecho nacional. Sin embargo, recientemente, la STS, de 2 de diciembre de 2011, ha señalado que la competencia para controlar el cumplimiento de la legislación de protección de datos personales tanto de los ficheros jurisdiccionales como de los gubernativos o no jurisdiccionales no le corresponde a la Agencia de Protección de Datos sino al CGPJ. Esta es una cuestión de gran complejidad, que abordaremos en otro momento.

autoridades de control tienen en virtud de la propuesta de Reglamento la facultad de imponer sanciones económicas muy elevadas. Si la legislación de nuestro país había sido cuestionada reiteradamente por las empresas por ser la más exigente a nivel europeo por la cuantía elevada de las sanciones económicas y la propia Ley 2/2011, de 4 de marzo, de Economía Sostenible las había revisado ligeramente a la baja[305], la propuesta de Reglamento va justo en la dirección contraria, incidiendo en la importancia en este ámbito de la existencia de sanciones económicas auténticamente disuasorias[306], estableciendo multas de hasta 250.000 euros o de hasta el 0,5% del volumen de negocios anual a nivel mundial, por ejemplo, cuando al empresa no responda al ejercicio de los derechos de los interesados; multas de hasta 500.000 o de hasta el 1% del volumen de negocios, por ejemplo, cuando no facilite información de manera suficientemente transparente al interesado; y multas de hasta 1 millón de euros o de hasta el 2% de su volumen de negocios –téngase en cuenta que el máximo de la sanción muy grave en la legislación española es de 600.000 euros–, por ejemplo, cuando se tratan datos sin base jurídica suficiente, aunque no sea de forma deliberada sino por negligencia. En todo caso, la propuesta de Reglamento recoge un adecuado equilibrio y tiene en cuenta que el tratamiento de datos personales se haga sin interés comercial o que sea una organización de menos de doscientas cincuenta personas que trate datos como actividad auxiliar de su actividad principal –lo que el art. 45.4 de la LOPD llama la vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal– para permitir que la autoridad de control opte por una advertencia escrita y no imponga sanción económica alguna[307]. Se trata de ser más exigentes con quien tiene los tratamientos de datos personales como actividad principal de carácter comercial –valorando también su volumen de negocios a nivel mundial, como hacía la LOPD que incluía referencias al volumen de los tratamientos o al volumen de negocio–, siendo más flexibles con la mayoría de las pequeñas

305. La Disposición Adicional Quincuagésimo Sexta de la Ley 2/2011, de 4 de marzo, de Economía Sostenible, modificó el art. 45.1 LOPD, y rebajó el mínimo de la multa a los responsables de ficheros privados por infracciones graves desde 60.101 000 euros a los 40.000, elevando las sanciones leves –que quedaron entre 900 a 40.000 euros– y dejando las infracciones muy graves como estaban –entre 300.001 euros y los 600.000 euros–, si bien algunas infracciones leves se convirtieron en infracciones graves. Cfr. ASIS ROIG, A. E. y GONZÁLEZ ESPADAS, F. J., «El art. 44 LOPD. Tipo de infracciones», en *Comentario*, cit. pp. 2041-2134,

306. El considerando 119 incide en que los Estados miembros deben asegurarse de que las sanciones sean efectivas, proporcionadas y disuasorias y deben tomar todas las medidas para su aplicación.

307. La Ley 2/2011, de 4 de marzo, introdujo en el art. 45.6 LOPD la posibilidad de la autoridad de control de sustituir la sanción por un apercibimiento al sujeto responsable –con el consiguiente archivo– cuando los hechos fueran constitutivos de infracción leve o grave siempre que exista una concurrencia significativa de elementos atenuantes y el infractor no hubiera sido sancionado con anterioridad, una posibilidad que no contemplaba hasta ese momento la legislación española, poco dada a las vías intermedias entre la Resolución de infracción con la correspondiente sanción económica y el archivo.

y medianas empresas que no llevan a cabo tratamientos de datos personales como actividad principal y para las que la normativa de protección de datos –y, un eventual incumplimiento– ha supuesto un problema económico para la continuidad de la propia actividad empresarial –y, por tanto, para el mantenimiento del empleo–. La propuesta de Reglamento incluye algunos elementos para favorecer la proporcionalidad de la sanción –naturaleza, gravedad, duración, intencionalidad o negligencia, grado de responsabilidad de la persona, anteriores infracciones, medidas de protección de datos por defecto y en el diseño o grado de cooperación con la autoridad de control para reparar la infracción–. Muchos de estos elementos estaban ya presentes como circunstancias atenuantes tanto en el texto inicial de la LOPD, como a través de la reforma operada en ella en virtud de la Ley 2/2011, de 4 de marzo, de Economía Sostenible[308], que tenía en cuenta la doctrina ya consolidada en esta materia por la Agencia Española de Protección de Datos y por la Sala de lo Contencioso Administrativo de la Audiencia Nacional. No podía ser de otro modo ya que sólo nuestro país contaba con una experiencia dilatada en relación con el ejercicio de la potestad sancionadora en el ámbito de la protección de datos, que no disponía ni la Comisión ni las autoridades de control de otros países. En general, la propuesta de Reglamento dedica su parte más extensa –treinta y tres artículos– a reforzar a las autoridades de protección de datos y equiparar sus poderes en todos los Estados miembros, lo que incluye la imposición de sanciones económicas sobre la base de un régimen sancionador que también se armoniza para toda la Unión[309]. De esta forma, elimina las diferencias normativas

308. Esta Ley también introdujo en la LOPD criterios más objetivos para ponderar las multas y para apreciar circunstancias atenuantes tanto para la graduación de las sanciones como para la rebaja del grado, limitando la discrecionalidad en este punto de la Agencia Española de Protección de Datos a la hora de aplicar el art. 45. En todo caso, la legislación española sigue siendo más precisa que la propuesta de Reglamento en la descripción de estos elementos. Se echa en falta una referencia a otros elementos: los beneficios obtenidos como consecuencia de la comisión de la infracción; la acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad tenía implantados procedimientos adecuados, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor; la apreciación de que la conducta del afectado haya podido influir en la comisión de la infracción; o que se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente. Este último elemento, que proviene de la Ley 2/2011, de 4 de marzo, trata de favorecer los procesos de fusión para lograr una «economía sostenible», teniendo en cuenta, además, las dificultades que tiene la entidad absorbente para conocer y evaluar económicamente las infracciones cometidas por la entidad absorbida antes de la fusión. Se trata de paliar en lo posible las consecuencias gravosas de las infracciones cometidas por la entidad absorbida de las que la absorbente no tuvo conocimiento, teniendo en cuenta, además, que en estos supuestos no está presente el elemento subjetivo para poder apreciar la culpabilidad y ni siquiera puede hablarse de una simple inobservancia por quien no ha intervenido materialmente en la comisión de los hechos (la absorbente) –sobre esta última cuestión ha profundizado González Espadas, F. J, *in voce*-.

309. Buena muestra de la importancia que la Comisión atribuye a reforzar las funciones y los poderes de las autoridades de control es que los «Indicadores de resultados e

existentes que indudablemente perjudicaban a las empresas sometidas en algunos Estados a un más intenso control y régimen sancionador, suprimiendo así una de las disfunciones principales que existían para un correcto funcionamiento del mercado interior[310].

Los tratamientos de datos personales, como hemos señalado antes, tienen un carácter transnacional. Por este motivo, por una parte, la propuesta de Reglamento aclara cuestiones de competencia y jurisdicción cuando el tratamiento de datos personales sea llevado a cabo por un responsable o encargado en varios Estados miembros, siendo competente la autoridad donde esté situado el establecimiento principal[311]. Por otra, trata de fortalecer, al menos, la cooperación y la coherencia entre autoridades de control de la Unión Europea entre sí y con la Comisión, una cuestión a la que dedica todo el Capítulo VII –arts. 55-72–

---

incidencia» –1.4.4– que se introducen en la Ficha financiera Legislativa de la propuesta de Reglamento elaborada por la Comisión y que van a servir para evaluar su eficacia sean las multas impuestas a los responsables de tratamiento por infracciones de protección de datos, el número de reclamaciones formuladas por los interesados e indemnizaciones recibidas por éstos, el número de casos que dan lugar a enjuiciamiento de los responsables o los recursos asignados a las autoridades de protección de datos.

310. De hecho, el mecanismo de coherencia, que después analizaremos también puede emplearse para cubrir las divergencias entre Estados en la aplicación de las sanciones administrativas –Considerando 120–.

311. Esta solución es calificada por la Exposición de Motivos de la propuesta de Reglamento como «principio de ventanilla única», con la finalidad de velar por una aplicación uniforme. Este criterio favorece el funcionamiento de las Corporaciones Internacionales que prestan servicios en varios países de la Unión Europea, que no pueden estar al criterio cambiante de varias autoridades de protección de datos y, que, por tanto, estarán sometidos al control de la autoridad del país donde tenga el establecimiento principal, debiendo el resto de los países respetar el criterio de esta autoridad. El modelo de una *one stop shop* obliga al ciudadano a interponer la denuncia ante la autoridad de control del Estado miembro donde la corporación tenga su establecimiento principal, si bien puede presentar la denuncia en la autoridad de control de su país. Hay que señalar que el Dictamen 8/2010, sobre Derecho Aplicable elaborado por el Grupo de Trabajo del art. 29 ya señalaba en relación con el artículo 4.1.a) de la Directiva 95/46/CE que la referencia a «un» establecimiento significa que la aplicabilidad del Derecho de un Estado miembro se desencadenará por la ubicación de un establecimiento del responsable del tratamiento en dicho Estado miembro, mientras que la de los Derechos de otros Estados miembros podría desencadenarse por la ubicación de otros establecimientos de ese responsable del tratamiento en dichos Estados miembros. Para que se desencadene la aplicación del Derecho nacional, es decisiva la noción de «marco de las actividades» de un establecimiento. Esto supone que el *establecimiento* del responsable del tratamiento está implicado en *actividades* que entrañan el tratamiento de datos personales, habida cuenta de su grado de implicación en las actividades de tratamiento, la naturaleza de las actividades y la necesidad de garantizar una protección de los datos efectiva. El Dictamen 8/2010 ya anticipaba que «*simplificar las normas que determinan el Derecho aplicable supondría una vuelta al principio del país de origen: todos los establecimientos de un responsable del tratamiento dentro de la UE aplicarían el mismo Derecho, el del establecimiento principal, con independencia del territorio en que estén ubicados. Sin embargo, esto solo sería aceptable si se logra una armonización más completa entre las legislaciones nacionales, incluida la armonización de las obligaciones de seguridad*» –lo que se alcanza con la propuesta de Reglamento–.

que contiene una regulación muy novedosa que no se existía en la Directiva[312] y que supone un gran paso adelante, desarrollando la cooperación como misión de las autoridades de control[313]. La propuesta materializa la cooperación entre autoridades de control en un conjunto de deberes de asistencia mutua –como facilitarse información útil– y medidas de control como solicitudes de autorización y consulta previa, inspecciones, comunicación rápida de información sobre la apertura de expedientes, lo que incluye medidas represivas para que se proceda al cese o a la prohibición de las operaciones de tratamiento, todo ello dentro de plazos concretos y prohibiendo la negativa a las solicitudes de asistencia. De esta forma, se introducen normas explícitas sobre asistencia recíproca obligatoria, que incluyen las consecuencias del incumplimiento de la solicitud de otra autoridad de control –art. 55–. También se prevén operaciones conjuntas –investigaciones, medidas represivas– en las que participen autoridades de control de distintos Estados miembros, estableciendo una interesante regulación sobre la relación entre las autoridades de control del país de origen y del país de acogida, especialmente en relación con la presencia del personal de la primera autoridad, sus inspecciones y la responsabilidad sobre sus actos –art. 56-[314]. La propuesta de Reglamento no se queda en la cooperación sino que fija un marco de mecanismos de coherencia, que tratan de facilitar la libre circulación de datos personales en el territorio de la Unión al mismo tiempo que se respeta la protección de datos personales, estableciendo herramientas que aproximen las divergencias entre autoridades de control. Este mecanismo prevé un Dictamen del Consejo Europeo de Protección de Datos, que está compuesto por los Directores de las Autoridades del control y por el Supervisor Europeo de Protección de Datos. De esta forma, se sustituye el Grupo de trabajo descrito en el art. 29 de la Directiva –más conocido por el Grupo del Art. 29–, que era un órgano de cooperación de las autoridades de control, por un Consejo Europeo de Protección de Datos –art. 64-72–, que es un órgano independiente que va a velar por la aplicación coherente de la normativa de protección de datos a nivel europeo y que interviene activamente en el sistema, especialmente a través de su participación en el mecanismo de coherencia antes descrito[315].

---

312. El art. 28.6 de la Directiva 95/46/CE se limitaba a prever la cooperación entre autoridades de control para el cumplimiento de sus funciones, en especial mediante el intercambio de información útil.

313. Hay que señalar que la regulación de las transferencias internacionales incluye una previsión sobre cooperación internacional en el ámbito de la protección de datos personales entre la Comisión y las autoridades de control de terceros países, especialmente aquellas que se consideran que ofrecen un nivel de protección adecuado –art. 45–, que tiene en cuenta la Recomendación de la OCDE para la cooperación transfronteriza en la ejecución de leyes que protegen la privacidad, de 16 de junio de 2007.

314. Las normas sobre operaciones conjuntas incluido el derecho de las autoridades de control a participar en estas decisiones se inspira en el art. 17 de la Decisión 2008/615/JAI, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza –DO L 210 de 6 de agosto de 2008–.

315. La Comisión no es miembro del Consejo Europeo de Protección de Datos, aunque tenga derecho a participar en sus actividades y a estar representada. No obstante, hay que mencionar la importancia que la Comisión se ha dado a sí misma en el Consejo

La propuesta de Reglamento establece un derecho a un recurso judicial contra una autoridad de control, también cuando ésta no informe al interesado en el plazo de tres meses desde la presentación de una reclamación –art. 74-[316]. Igualmente se establece un derecho a un recurso judicial contra un responsable o encargado cuando el interesado considere vulnerado su derecho a la protección de datos, acción que puede ejercitarse alternativamente ante los órganos jurisdiccionales del estado miembro en el que el responsable o encargado tenga su residencia o en los que el interesado tenga su residencia habitual, debiendo los Estados miembros ejecutar las resoluciones definitivas de los órganos jurisdiccionales –art. 75–. La propuesta de Reglamento incluye mecanismos de coordinación entre órganos jurisdiccionales, de manera que si un órgano jurisdiccional competente de un Estado miembro tenga motivos razonables para creer que se están llevando procedimientos judiciales paralelos en otro Estado miembro, se ponga en contacto con el órgano jurisdiccional competente y pueda suspender el procedimiento –art. 76–[317].

VI. REFLEXIÓN FINAL

La Comisión Europea ha presentado una Propuesta de Reglamento General

---

Europeo de Protección de Datos, reservándose para el Supervisor Europeo de Protección de Datos una de las dos Vicepresidencia del Consejo, salvo que haya sido elegido Presidente –art. 69– y la Secretaría del mismo, que incluye la preparación y seguimiento de las reuniones del Consejo Europeo y las comunicaciones con otras instituciones y con el público –art. 71–. Se trata de un poder excesivo, consecuencia, sin duda, del peso en la redacción de la propuesta de Reglamento de los actuales Supervisor y Supervisor Adjunto, Peter Hustinx y Giovanni Buttarelli. De hecho, el reforzamiento de la figura del Supervisor Europeo se manifiesta en que la Ficha financiera legislativa que acompaña a la propuesta reconoce que la principal incidencia presupuestaria del Reglamento atañe a las nuevas tareas confiadas al Supervisor Europeo de Protección de Datos.

316. Si bien las acciones legales contra una autoridad de control deberán ejercitarse ante los órganos jurisdiccionales del Estado miembro en que esté establecida, si el interesado tiene su residencia habitual en otro Estado miembro puede solicitar a su autoridad de control que ejercite en su nombre la acción contra la autoridad de control competente en el otro Estado miembro. Esta es la principal novedad en relación con el recurso judicial porque el Capítulo III de la Directiva, relativo a los recursos judiciales, responsabilidad y sanciones, establece también en el art. 22 que, sin perjuicio del recurso administrativo que pueda interponerse ante la autoridad de control antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos establecidos en la legislación nacional de protección de datos personales. Cfr. también los arts. 32 y 33 del Reglamento de la UE 45/2001.

317. Como señala la Exposición de Motivos, esta previsión se establece sobre la base del art. 5.1 de la Decisión Marco 2009/948/JAI del Consejo, de 30 de noviembre de 2009, sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales, DO L 328 de 15 de diciembre de 2009; y el art. 13.1 del Reglamento (CE) nº 1/2003 del Consejo, de 16 de diciembre de 2002, relativo a la aplicación de las normas sobre competencia previstas en los artículos 81 y 82 del Tratado, DO L 1 de 4 de enero de 2003. La obligación de los Estados de garantizar la celeridad de las actuaciones judiciales se establece sobre la base del art. 18.1 de la Directiva 2000/31/

de Protección de Datos, que derogará la actual Directiva 95/46/CE y desplazará las leyes de los Estados miembros, y que junto a la propuesta de Directiva para el ámbito policial y judicial, va a configurar un nuevo marco normativo para la protección de datos personales en la Unión Europea Las propuestas de Reglamento y de Directiva son posiblemente el proyecto estrella para este mandato de la Vicepresidenta de la Comisión Viviane Reding. Se abre ahora un intenso periodo de negociación en el Consejo y en el Parlamento, un proceso que tienen su horizonte puesto en el 2014, año en el que finaliza el mandato de esta Comisión y de este Parlamento Europeo –sin perjuicio de que una Comisión renovada pueda continuar impulsando estas propuestas–. La iniciativa normativa de la Unión Europea se une a la impulsada en el Consejo de Europa para negociar un nuevo Tratado internacional que reforme y actualice el Convenio 108. Llama la atención que se estén reformando a la vez dos instrumentos internacionales de protección de datos y que esté presente en ambos la vocación y la preocupación por ser compatibles y en ningún caso contradictorios.

La necesidad de un nuevo marco jurídico europeo es consecuencia de los profundos cambios que han experimentado las tecnologías de la información y la comunicación en los últimos años, en una evolución que va desde los clásicos ficheros de datos personales al desarrollo de Internet, de los motores de búsqueda, de las redes sociales, de la computación en nube y de los *smart phones*. A ello hay que añadir la aprobación del Tratado de Lisboa, que refuerza la base jurídica en la Unión Europea para aprobar una normativa en virtud del reconocimiento de un derecho fundamental a la protección de datos personales en el art. 8 de la Carta, y permite extender la vigencia del derecho europeo de protección de datos personales al ámbito del antiguo tercer pilar, que se movía antes en los terrenos de la cooperación y no de la integración. Además, la protección de datos personales es un elemento esencial para la construcción europea y para hacer viable la libre circulación de personas que tiene como presupuesto que los países europeos tengan un modelo de protección de datos personales homogéneo que permita el intercambio de información. Sin embargo, las divergencias en la protección de los datos personales en los Estados miembros son todavía demasiado grandes. Esto es consecuencia, por una parte, de una inadecuada transposición de la Directiva 95/46/CE por la propia legislación de los Estados miembros. El margen de maniobra que dejaba la Directiva como derecho derivado institucional y sus abundantes cláusulas abiertas –*open-ended principles*– que admitían una transposición diferente en la legislación de los distintos Estados han sido utilizados en ocasiones para el incumplimiento de las exigencias de la Directiva y para sobrepasar sus límites. Hay que tener en cuenta que la Directiva no se limitaba a una armonización mínima –no era una Directiva de mínimos– sino que constituía, en principio, una armonización completa que operaba como norma de máximos y que impedía que el legislador

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, DO L 178 de 17 de enero de 2000.

nacional introdujera una protección más rigurosa o que estableciera exigencias adicionales. Recientemente, la STJUE, de 24 de noviembre de 2011, ha afirmado la incorrecta transposición de la Directiva por parte de la legislación española, que no incluyó como supuesto de legitimación del tratamiento la satisfacción de un interés legítimo del responsable, sino que impuso obligaciones adicionales y no estableció la necesaria ponderación con los derechos del interesado en las circunstancias concretas del caso particular. A estas divergencias en la protección de datos personales en la Unión Europea ha contribuido también la disparidad en la capacidad coercitiva de las autoridades de control –o una distinta voluntad de ejercer los instrumentos coercitivos– y la deficiente interpretación y aplicación que llevan a cabo las autoridades de control y los órganos jurisdiccionales en los diferentes Estados de los mismos principios y derechos recogidos en la Directiva ante similares supuestos de hecho.

Las diferencias en la protección de los datos personales entre los Estados miembros obstaculizan el mercado interior, dificultando el ejercicio de actividades económicas a escala comunitaria y falseando la competencia; además, la ausencia de protección equivalente afecta también a la eficacia del derecho fundamental a la protección de datos personales de los ciudadanos europeos. La propuesta de un Reglamento General de protección de Datos es, para la Comisión, un marco jurídico coherente y homogéneo de protección de datos que suprime las incongruencias entre los Estados miembros y reduce el margen de elección tanto de los legisladores nacionales como de las autoridades de control, desplazando la mayor parte de la legislación de los Estados y facilitando una política más integradora en la Unión Europea en este ámbito. La Comisión justifica el valor añadido de la intervención de la Unión Europea a través de la aprobación de un Reglamento en que los objetivos perseguidos de facilitar el funcionamiento del mercado interior y garantizar la protección de los datos personales de los ciudadanos europeos no pueden ser alcanzados de manera suficiente por los Estados miembros. Estos, por sí solos, no pueden mitigar los problemas de libre circulación de datos en las fronteras internas de la Unión Europea que plantea la situación actual de fragmentación de las legislaciones nacionales, lo que obliga a hacerlo a escala de la Unión, como exige el principio de subsidiariedad –art. 5.3 TUE–. Al mismo tiempo, la propuesta de Reglamento permite una protección más efectiva de los ciudadanos europeos frente a los tratamientos de datos a escala internacional, que puede lograrse mejor a nivel de la Unión.

La propuesta de Reglamento aborda con precisión cuestiones como el ámbito de aplicación territorial, resolviendo la problemática de jurisdicción y de ley aplicable que plantean las corporaciones internacionales que ofrecen servicios de tratamiento de datos –redes sociales virtuales, motores de búsqueda, servicios de computación en nube– y que tienen su sede fuera de la Unión Europea. Además introduce nuevas obligaciones del responsable del tratamiento como la evaluación de impacto, el nombramiento de un delegado de protección de datos, la conservación de la documentación o el cumplimiento de requisitos

en materia de autorización y consulta previas. Regula con precisión la licitud de los tratamientos –decantándose por el consentimiento explícito–, la transparencia de la información y el derecho al olvido en Internet –el deseo de «borrar el rastro en Internet»–, haciendo recaer la responsabilidad de garantizarlo en quien haya publicado los datos personales y no en los buscadores, e incorporando limites al derecho a la protección de datos personales para garantizar la libertad de información y de expresión. Por último, fortalece a las autoridades de control, tanto en sus funciones como en la posibilidad de imponer importantes sanciones económicas, de manera que puedan ser eficaces en la supervisión y la aplicación de la protección de datos, unificando su capacidad coercitiva y estableciendo mecanismos que faciliten la coherencia en la aplicación de la protección de datos personales en la Unión. La propuesta de Reglamento de la Comisión supone, de alguna manera, un reconocimiento implícito del modelo español de protección de datos personales y de la actividad de supervisión y control que ha desempeñado la Agencia Española de Protección de Datos en las últimas dos décadas. Por todo ello, la propuesta de Reglamento tiene que ser bienvenida *desde la perspectiva de las personas* porque le da más instrumentos para el control sobre su información personal. El incremento de los tratamientos de datos personales derivado del proceso tecnológico –Internet de las cosas, video vigilancia, biometría, nanotecnología, historia clínica electrónica en la nube, RFID– eleva el nivel de riesgo para la privacidad, por lo que este proceso debe ir acompañado de un fortalecimiento de las garantías de las personas en la era de Internet.

Desde *la perspectiva de los países*, la propuesta de Reglamento no se aleja del objetivo –no alcanzado– de la Directiva de tratar de mantener un equilibrio entre la libre circulación de la información personal y la tutela del derecho a la protección de datos personales en la Unión Europea. El texto equipara el nivel de protección de los datos personales en todos los Estados miembros, suprimiendo las divergencias graves que existían entre países para asegurar un alto nivel de protección de datos personales. Esto en la práctica supone un endurecimiento del régimen jurídico para aquellos países que presentaban un menor nivel de exigencia –basta poner el ejemplo de la incorporación de una normativa que establece muy graves sanciones económicas por incumplimientos en ordenamientos nacionales que no contemplaban ninguna o la supresión del consentimiento tácito–, sin que pueda afirmarse que la propuesta conduce al mismo tiempo a España a una disminución del nivel de protección. La aplicación del criterio del interés legítimo del responsable como legitimación para el tratamiento sin consentimiento –también en virtud de la STJUE, de 24 de noviembre de 2011, que ha atribuido un efecto directo a este supuesto ya previsto en la Directiva– o la desaparición del régimen específico para las cesiones de datos, va a introducir al ordenamiento jurídico de nuestro país instrumentos que permitan la ponderación entre derechos e intereses legítimos y le va a restar rigideces, especialmente aquellas que aportó la STC 292/2000, de 30 de noviembre, que incorporó al contenido esencial del derecho fundamental elementos que justamente estaban absoluta y completamente fuera de la noción admitida por

los juristas de lo que el derecho a la protección de los datos personales significaba. Posiblemente habrá quien piense que puede existir un eventual conflicto entre el Reglamento y la Constitución –o por decirlo más exactamente, entre Reglamento y jurisprudencia constitucional–, que, además, no puede ser resuelto por el Tribunal Constitucional, que no controla la constitucionalidad del derecho derivado institucional. El Reglamento tiene como parámetro el Derecho de la Unión y al Tribunal de Justicia como único juez competente para juzgar su validez. Las instituciones europeas están obligadas a respetar las tradiciones constitucionales que sean *comunes* y que forman parte también del Derecho que debe garantizar el Tribunal de Justicia. Lógicamente los actos nacionales de ejecución del Derecho de la Unión que lesionen un derecho fundamental son controlables por el Tribunal Constitucional.

Indudablemente –y todavía *desde la perspectiva de los países*–, la aprobación de la propuesta de Reglamento, una norma de Derecho derivado institucional obligatoria en todos sus elementos, va a dejar muy poco margen de maniobra a los Estados, correspondiéndole sobre todo a la Comisión la aclaración de algunos conceptos jurídicos indeterminados a través de la aprobación de actos delegados. No obstante, cuando avance el proceso negociador y crezca en los Gobiernos la preocupación por la pérdida neta de soberanía –o, al menos, la perciban– en un punto que afecta al desarrollo legislativo de un derecho fundamental, posiblemente la propuesta de Reglamento comience a incluir más habilitaciones a los Estados, concediéndoles a éstos un mayor margen de apreciación, de manera que se pase de una Directiva que permitía una flexibilidad formal a un Reglamento que sea flexible en lo material[318] En todo caso, cualquiera que sea la mayor o menor flexibilidad material del Reglamento, lo que está claro es que su aprobación va a reducir la libertad del legislador nacional en el desarrollo de un derecho fundamental y afecta al principio democrático. No nos referimos ahora a la escasa intervención del Parlamento en la ejecución futura de un Reglamento, que presenta un alto nivel de detalle y de especificación, que supone también una subordinación y limita en gran medida la amplitud del debate. No se trata sólo de reincidir en la débil implicación de los Parlamentos nacionales en el proceso europeo de toma de decisiones, que las Cortes Generales no ejerciten ningún mecanismo de control sobre la acción normativa que el Gobierno desempeña en el Consejo o de la escasa presencia en la determinación de la política europea de la Comisión Mixta Congreso-Senado para la Unión Europea[319]. Sin negar el reforzamiento del Parlamento

318. El Gobierno Británico ya ha anunciado su voluntad de presionar para eliminar muchos de los poderes de la Comisión Europea para hacer actos delegados y de ejecución, especialmente cuando estos tienen el potencial de hacer una gran diferencia en los principios fundamentales –por ejemplo, en los intereses legítimos que los responsables pueden alegar para la legitimación de su tratamiento–.

319. Cfr. PÉREZ TREMPS, P, «La débil Parlamentarización de la integración en España», en *La encrucijada constitucional en la Unión Europea*, Civitas, Madrid, 2002, pp. 401-416. TAJADURA TEJADA, J., *El futuro de Europa: luces y sombras del Tratado de Lisboa*, Comares, Granada, 2010.

Europeo y la garantía que esto supone para al principio democrático, queremos incidir sobre todo en la ausencia de un debate político sobre el nuevo marco europeo de protección de datos –que va a desplazar todas las leyes de los Estados–, que llegue también a la opinión pública y a los medios de comunicación y que facilite la reconducibilidad –*zurück geführt*– de las decisiones al pueblo, titular de la soberanía[320]. Esta ausencia de debate se manifiesta especialmente cuando lo comparamos con el que hubo para la aprobación de la LORTAD o de la LOPD o actualmente en relación con la tramitación del proyecto de ley de transparencia administrativa, tanto en el Parlamento como en los medios de comunicación y en la opinión pública. Se van a desplazar leyes estatales aprobadas tras una acalorada discusión pública y que fueron impugnadas y que exigió un pronunciamiento del Tribunal Constitucional, por un reglamento general de protección de datos personales aprobado sin debate político alguno que llegue a la opinión pública –lo que ocurre ordinariamente con los que celebra el Parlamento Europeo–. La tramitación del marco normativo europeo de protección de datos evidencia, de nuevo, los déficits constitucionales que presenta la integración europea. El déficit democrático se hace visible por la prevalencia de los criterios técnicos sobre los políticos en el proceso de negociación del marco normativo europeo de protección de datos personales, algo que comienza a hacerse consustancial a la aprobación del derecho derivado institucional –y que se extiende a la política europea y a la de los propios gobiernos nacionales–. Esta es una cuestión que ha de tenerse en cuenta, sobre todo, si los documentos iniciales provienen de instituciones y grupos que carecen de legitimidad democrática directa o indirecta y no están sometidos a controles políticos. No nos referimos únicamente a la participación decisiva de autoridades administrativas independientes –supervisor europeo, grupo del artículo 29 y agencias de protección de datos– en la elaboración de los primeros documentos previos a los borradores y en la orientación de las posiciones de los Gobiernos, algo razonable habida cuenta de que son las autoridades de control las que mejor conocen mejor la realidad y los efectos de adoptar una decisión u otra. Las instituciones de la Unión Europea como los Gobiernos están siguiendo fundamentalmente los criterios de técnicos en ausencia de criterio político alguno al respecto. La propuesta de Reglamento es un texto técnico que nace de la Comisión, en el que se ha hecho ostensible una depreciación de la política, a la vez que la opinión pública se mantiene al margen en una materia que no interesa tampoco a los medios de comunicación. Déficit de debate político y adopción de decisiones sólo en virtud de criterios técnicos sin trascendencia pública alguna que es el hábitat preferido por la industria para poder, al menos, presionar, orientando hacia una u otra postura, con consecuencias claramente económicas bajo la cobertura de razones técnicas. Además, el hecho de que el debate político en la

320. El principio democrático exige que toda decisión política, libre en fines, de un poder público tenga que ser reconducible al titular de la soberanía. Cfr. BÖCKENFÖRDE, E.–W., "Demokratie als Verfassungsprinzip" *Staat, Verfassung, Demokratie. Studien zur Verfassungstheorie und zum Verfassungsrecht*, Suhrkamp, Frankfurt am Main, 1991, pp. 289-378.

Unión Europea y en los distintos países se encuentre casi monopolizado por las cuestiones económicas plantea el interrogante de si un contexto de crisis económica grave es el mejor momento para acometer una revolución sustancial del marco de protección de datos que desplace las leyes de los Estados. Si en la década pasada los atentados terroristas de Nueva York, Londres o Madrid pusieron en la agenda de los gobiernos –también de sus opiniones públicas– la preocupación por la seguridad en detrimento de la privacidad, lo que implicó un mayor grado de injerencia en el derecho a la protección de datos personales –retención de datos de tráfico, cesión de datos de pasajeros a EEUU–, la preocupación por los problemas económicos en el contexto actual puede llevar al traste durante la negociación los buenos propósitos iniciales de la Comisión y la aprobación del nuevo Reglamento puede ser visto sólo como una oportunidad para fortalecer el mercado interior en un contexto de crisis económica en detrimento de la privacidad. Por ello, la modificación de la Directiva es una operación no exenta de riesgos, sobre todo, si la armonización finalmente se encamina a descender el nivel de protección para acercarse a los países que presentan un menor nivel de exigencia. De ahí la opinión de quienes mantienen que las principales divergencias entre Estados pueden resolverse sin modificar la Directiva pues existe aún un amplio margen para mejorar su aplicación, a través del desplazamiento o la modificación de la legislación nacional que incumple la Directiva, una mayor armonización de la interpretación que teniendo como base la argumentación jurídica pueda llegar a criterios comunes entre los distintos órganos que tienen que aplicar el derecho fundamental a la protección de datos, una mayor cooperación entre las autoridades que supere las prácticas divergentes y un incremento de la actividad de control que evite el déficit de *enforcement*.

Desde la *perspectiva de la industria y los mercados*, el Reglamento es visto con una cierta reticencia. Por una parte, existe una valoración positiva hacia la superación de la actual fragmentación de la legislación que dificulta comercializar productos y servicios y hacer políticas de privacidad paneuropeas y que representa un límite a la competencia e incrementa los costes. La simplificación normativa del Reglamento y la supresión o flexibilización de algunas exigencias de las leyes nacionales que los mercados consideraban burocráticas, como la notificación de los tratamientos o los trámites para las transferencias internacionales de datos han merecido también un juicio positivo. De hecho, uno de los objetivos del Reglamento es hacer sencilla la protección de datos, reduciendo la carga administrativa, pero incrementando al mismo tiempo la *accountability*. No obstante, el Reglamento incorpora nuevas obligaciones para el responsable –hacer evaluaciones de impacto en la privacidad, designar un delegado de protección de datos, documentar los tratamientos, notificar las brechas de seguridad, hacer *privacy by design*–, sin que aparentemente para la industria su cumplimiento les exima de nada, manteniendo algunos requerimientos para las pequeñas y medianas empresas que éstas consideran todavía excesivos. La propuesta trae más obligaciones para las empresas y, por tanto, más posibilidades de sanciones económicas por incumplimientos, que, aunque deban ser aplicadas

con ponderación y regirse por el principio de proporcionalidad, pueden ser potencialmente muy elevadas si se tiene en cuenta el volumen de negocio. Así, el Gobierno Británico ha cuantificado los costes y los beneficios que va a suponer para la economía británica la implantación del nuevo marco normativo europeo y se ha comprometido a apoyar un instrumento que no sobrecargue –*not overburden*– a las organizaciones y que permita el desarrollo y la innovación, marcando, de esta forma, las líneas rojas de la posición británica en el proceso negociador[321].

Es innecesario decir que la vía que le interesa a la industria para la protección de los datos personales es la autorregulación. Y esta es, sin duda, una herramienta aprovechable. De hecho, la propuesta de Reglamento incorpora instrumentos propios de ese ámbito como la privacidad en el diseño –que la privacidad esté presente en el momento del diseño del sistema de información, por ejemplo, en la elaboración de las especificaciones técnicas y en el desarrollo de los programas o sistemas operativos–, la privacidad por defecto –que las configuraciones por defecto respeten la privacidad–, las certificaciones y sellos de protección de datos, los códigos de conducta o las tecnologías de protección de la privacidad, avanzando en este camino más allá de lo que lo hacía la Directiva. La autorregulación es, por ello, una respuesta ágil cuando falte una regulación jurídica en el ámbito nacional o internacional, ante situaciones de gran complejidad técnica o ante la imposibilidad de llegar a todos los ámbitos a través de una actividad administrativa de inspección y control, pudiendo contribuir a la protección de los derechos del usuario. Es imprescindible que las instituciones públicas eviten las posiciones frentistas en relación con las empresas y sean capaces de generar entornos de colaboración, lo que no significa ceder ante la industria –que no deja de ser un *stakeholder*– sino de alcanzar un diálogo que permita una mayor protección de los datos personales. Frente a

321. La Comisión Europea ha señalado que el ahorro estimado que se deriva de la armonización regulatoria y de la desaparición de las tasas de notificación era de 2.3 billones de euros al año. Sin embargo, el Ministerio de Justicia Británico ha discrepado de las cifras resultantes de esa evaluación de impacto de la Comisión porque no ha cuantificado correctamente los costes de las nuevas obligaciones del responsable del tratamiento y ha sobreestimado los beneficios del fortalecimiento del derecho de acceso y del derecho al olvido. Así, por ejemplo, no comparte la propuesta de que el derecho de acceso se ejercite sin coste alguno y plantea reticencias sobre la propuesta de «derecho al olvido» en relación con sus aspectos prácticos, sus costes y la posibilidad de confusión que esta regulación puede ocasionar en las personas y en las organizaciones. Igualmente rechaza las nuevas obligaciones del responsable de hacer evaluaciones de impacto, la previa autorización de la autoridad de control, la designación obligatoria de delegados de protección de datos, a las que considera nuevas cargas burocráticas y potencialmente costosas para las organizaciones que, además, no parece que vayan a ofrecer una mayor protección a las personas; pone reticencias también a las comunicaciones de las brechas de seguridad en las infracciones menores, e incide en la necesidad de impulsar una mayor proporcionalidad en la aplicación de las multas máximas. Cfr. *Call for Evidence on Proposed EU Data Protection Legislative Framework. Summary of Responses*, 28 de junio de 2012, Ministry of Justice, pp. 11 y 37-38, en *www.justice.gov.uk*.

una cierta prevalencia de una imagen negativa de la protección de datos personales –con mensajes como el de que nadie cumple esta legislación–, es necesario tratar de poner este derecho fundamental en positivo, involucrando al propio sector. La privacidad se debe mostrar como una oportunidad de negocio, como una ventaja competitiva para las empresas, como algo *sexy* que posiciona mejor y que es un incentivo en el mercado. Por ello, es imprescindible introducir la protección de datos dentro de la responsabilidad empresarial, convirtiendo a las empresas –también al buen funcionamiento de sus propios canales de denuncia– en un elemento estratégico en el sistema de garantías, convenciéndolas de que Internet y la protección de datos es un canal de retorno, que la privacidad es algo demandado por los clientes y cuyas quiebras afectan gravemente a la reputación corporativa –como han comprobado recientemente tanto empresas proveedoras de servicios de redes sociales como las propias Administraciones Públicas–.

Sin embargo, la autorregulación representa únicamente una solución complementaria y no puede ser la garantía principal sobre la que descanse la privacidad de los usuarios. Las empresas se siguen moviendo frecuentemente por lógicas económicas a corto plazo. Las normas jurídicas han surgido, de hecho, como garantía de la privacidad frente a las malas prácticas de las empresas. El cumplimiento de la normativa de protección de datos personales supone, lógicamente, un incremento de costes y la industria tiene una tendencia natural a reducir cargas económicas para ser más competitiva o para obtener más beneficios. Si bien es extremadamente importante en un contexto como el actual incidir en los análisis de impacto económico de cualquier obligación nueva que se imponga a las empresas –siendo también especialmente sensibles y proporcionales en la aplicación de sanciones económicas– para no debilitar el tejido empresarial, también las empresas deben ser conscientes de que tienen que cumplir la normativa de protección de datos, como también cumplen la de prevención de riesgos laborales o la de medio ambiente, porque se trata de respetar un derecho fundamental. Las exigencias privadas a través de la autorregulación no llegan a garantizar con plenitud los derechos de los afectados por lo que hay que aplicar también en este ámbito los instrumentos hererónomos y la regulación y la supervisión desde fuera de la empresa, especialmente en un periodo en el estamos padeciendo las consecuencias económicas de la autorregulación y de la desregulación.

Que la autorregulación ha demostrado sus limitaciones –que el mercado tiene sus límites– es algo que se evidencia con el cambio de la posición de EEUU en esta materia. Hasta ahora el modelo americano había hecho descansar la protección de datos en el ámbito del derecho del consumo, del derecho de la competencia y de la autorregulación de las empresas –las empresas tienen que cumplir con sus clientes sus compromisos de privacidad y si no lo hacen se les puede exigir judicialmente su responsabilidad y la correspondiente indemnización–, mientras que el modelo europeo de protección de datos ha apostado por las herramientas normativas heterónomas, de ahí su fuerte asimetría

con el modelo americano. Sin embargo, recientemente el Presidente Obama ha presentado una *Consumer Privacy Bill of Rights*[322], que reconoce derechos a los consumidores y ofrece una orientación clara sobre lo que pueden exigir o deben esperar de quienes manejan su información personal. De hecho, el texto descansa en la autorregulación vinculante y, en el caso de que ésta no se cumpla, apuesta por la regulación. Así, hace un llamamiento a las empresas para comenzar inmediatamente a trabajar por implementar estos principios en códigos de conducta, pero advirtiendo de que «mi gobierno trabajará para promover estos principios y trabajar con el Congreso para llevarlos a la ley»[323]. El texto de la Administración Obama es también la respuesta americana a la propuesta de la Comisión Europea de un nuevo marco normativo de protección de datos, que ha generado, ya de inicio, la modificación de la tradicional posición americana en este ámbito –que había mantenido hasta ahora que sus políticas de privacidad en el medio electrónico eran como mínimo, tan estrictas como las impulsadas por la Unión Europea– y la consiguiente aproximación al modelo europeo, lo que representa, en el fondo, el reconocimiento de un fracaso. Este fracaso se hace si cabe más evidente por el proceso de cambio profundo en la protección de datos personales que está viviendo Iberoamérica en los últimos años, en el que distintos países están afrontando un proceso de aprobación de normas de protección de datos personales, que aproxima su legislación al modelo europeo y la aleja del modelo americano[324]. Se resuelve, de esta forma, el dilema pro-

322. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 23 de febrero de 2012. El Presidente Obama ha calificado este documento como modelo para la privacidad en la era de la información –«as a blueprint for privacy in the information age»–.

323. «I call on these companies to begin immediately working with privacy advocates, consumer protection enforcement agencies, and others to implement these principles in enforceable codes of conduct. My Administration will work to advance these principles and work with Congress to put them into law».

324. Así, se puede citar: en Argentina la Ley 25.326, de 2000 y la puesta en marcha de la Dirección Nacional de Protección de Datos Personales –aunque el caso argentino ha podido dar lugar a una situación paradigmática o inidónea en algunos aspectos–; en Uruguay la Ley 18.331, de 11 de noviembre de 2008, de Protección de Datos Personales y Acción de Habeas Data, y la puesta en marcha de la Unidad Reguladora y de Control de Datos Personales como autoridad administrativa independiente; en Colombia hay que destacar la Sentencia de la Corte Constitucional de Colombia –C-748/11–, de 6 de octubre de 2011, que lleva a cabo el control constitucional al Proyecto de Ley Estatutaria No. 184 de 2010 por la que se dictan disposiciones generales para la protección de datos personales, de forma que la próxima sanción de esta Ley permitirá que Colombia cuente con una ley general de protección de datos personales; en Perú la Ley 29733 de Protección de Datos Personales; en Costa Rica, la Ley nº 8968, de Protección de la Persona Frente al Tratamiento de sus Datos Personales, publicada el 5 de septiembre de 2011 y la puesta en marcha el 5 de marzo de 2012, de la Agencia de Protección de Datos de la República de Costa Rica; en Méjico, la Federal de Transparencia y Acceso a la Información Pública Gubernamental, del 11 de junio de 2002 –donde se reconocía la protección de datos como límite a la transparencia– y recientemente la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 5 de julio de 2010; en Perú, la Ley nº 29733, de Protección de Datos Personales, publicada el 3 de julio de 2011; en Nicaragua la Ley de protección de datos personales 787, del 29 de marzo de 2012, etc.

fundo que tenían ante sí los países iberoamericanos entre el modelo norteamericano o el modelo europeo de protección de datos personales. Esta aproximación de los países iberoamericanos al modelo europeo de protección de datos personales está siendo premiado con la declaración por parte de la Comisión Europea de que estos países garantizan un nivel adecuado de protección, un reconocimiento que ha obtenido hasta ahora Argentina en 2003 y muy recientemente Uruguay en agosto de 2112. Este reconocimiento, que se concede teniendo en cuenta que su legislación reconoce principios y derechos de protección de datos, establece autoridades de control independientes y prevé los necesarios recursos administrativos y jurisdiccionales, permite las transferencias internacionales de datos sin autorización, lo que abre la posibilidad de que los países iberoamericanos se conviertan en un espacio donde sean posibles inversiones y actividades empresariales que impliquen transferencias de datos personales, convirtiendo esa región en un espacio más competitivo para el ámbito de las TIC. En todo caso, la aprobación de normas de protección de datos personales en Iberoamérica se hace a distinto ritmo por parte de los Estados y sin la existencia de un instrumento que obligue en el ámbito del Derecho Internacional Público[325].

Lógicamente, detrás del cambio de posición en el continente americano en materia de protección de datos personales también se encuentra la preocupación por la necesidad de incrementar los intercambios comerciales transatlánticos, algo especialmente importante en un contexto de crisis económica. La cooperación entre América y Europa en el ámbito de la protección de datos refuerza la confianza de los consumidores y facilita el crecimiento de la economía global de Internet y el mercado digital. Esto pone también sobre la mesa la necesidad de establecer marcos normativos de protección de la privacidad que permitan el flujo de datos y la interoperabilidad sin discriminación, también con el área Asia-Pacífico –China, Japón, India, Corea del Sur, Australia–. Durante los últimos años se ha hecho si cabe cada vez más patente la necesidad de garantizar la privacidad en un mundo sin fronteras, cada vez más globalizado e interconectado, especialmente desde la aparición de Internet, y caracterizado por las transferencias internacionales. No nos referimos únicamente al intercambio transfronterizo de datos derivado del incremento de las relaciones económicas y comerciales con otros países, especialmente del área Asia-Pacífico sino a los tratamientos de la propia esfera personal o doméstica –motores de búsqueda, redes sociales, computación en nube– que se desarrollan por Internet a través de redes internacionales cuyos usuarios y proveedores de servicios se encuentran

325. Desde la perspectiva política, hay que citar la Declaración de Santa Cruz de la Sierra, del 15 de noviembre del 2003, donde los jefes de Estado y de Gobierno de 21 países iberoamericanos manifestaron que «la protección de datos personales es un derecho fundamental de las personas» –núm. 45–. Recientemente la Asamblea General de la OEA, en su sesión ordinaria en San Salvador realizada del 5 al 7 de junio del 2011, recalcó la creciente importancia de la privacidad y la protección de datos personales, así como la necesidad de fomentar y proteger el flujo transfronterizo de información en las Américas y estudió un proyecto de principios y recomendaciones preliminares sobre la protección de datos personales.

ubicados en países diferentes y donde el servidor informático se encuentra también en un tercer país. Estos tratamientos de datos personales implican la existencia de constantes flujos de información personal para los que no es efectiva la normativa regional. Cada vez es más complicado determinar la jurisdicción competente –cuál es la legislación aplicable y la autoridad para resolver las disputas– y quien es el responsable del tratamiento. Por ello, la protección de datos personales en un entorno globalizado sólo es posible si se consensuan unas exigencias homogéneas de privacidad, que superen las discrepancias existentes –por no decir los desequilibrios– entre la Unión Europea, Estados Unidos y el ámbito Asia-Pacífico y ofrezcan seguridad jurídica a todos los agentes. Esta preocupación por la necesidad de una normativa internacional le ha correspondido no sólo a las Agencias de Protección de Datos –conscientes cada vez más de las limitaciones de la actual regulación y sistema de control– sino también a la sociedad civil –sabedora de que los derechos no son reales y efectivos con la mera aplicación de la normativa regional– y también a la propia industria y a las corporaciones internacionales que no pueden impulsar productos y servicios a nivel global sobre la base de una variada y cambiante legislación. Aparece, así, de manera clara que la protección de los datos personales tiene una dimensión internacional de la que carecen otros derechos fundamentales y su tutela efectiva exige una normativa internacional[326]. La aprobación de un Tratado internacional –del que la Resolución de Madrid de Estándares Internacionales sobre Protección de Datos Personales y Privacidad de 2009 fue un primer paso– que establezca una normativa de protección de datos personales y unas instituciones de supervisión a nivel internacional es algo imprescindible, lo que requiere alcanzar un equilibro entre las diferentes visiones sobre la protección de datos personales en los distintos continentes, que se plasme en un documento nacido del diálogo y de la búsqueda del consenso que trata de integrar las sensibilidades de los distintos continentes. Lógicamente, lo que se esconde detrás es el debate de fondo sobre el papel regulador –principal o subsidiario– de los Gobiernos en Internet –una cuestión que fue abordada por la Cumbre del G-8 dedicada a Internet, en mayo de 2011–, la necesidad de establecer un marco jurídico eficaz, no para frenar Internet, sino para asegurarse de que prospera sobre la base del respeto a la privacidad, a la propiedad y a los derechos de las personas. Si bien la tecnología puede ser neutra, no lo son los usos y no debe permitirse que la revolución digital afecte negativamente a los derechos fundamentales. Si bien las revoluciones de la primavera árabe han mostrado que Internet no pertenece a los Estados, en esta tercera mundialización de la historia no puede marginarse a los Estados democráticos. Olvidarse que son los representantes de la voluntad popular y que tienen la legitimidad para imponer normas y establecer un control judicial sería apostar por un riesgo claro, la anarquía. Internet no puede ser un universo paralelo, liberado del imperio de la ley, sin moral y sin los principios fundamentales que gobiernan la vida social en

326. El Convenio 108 del Consejo de Europa, si bien es un documento básicamente eurocéntrico, está jugando un importante papel en ausencia de un instrumento internacional, habiendo solicitado recientemente la adhesión Uruguay (2011) y Méjico (2012).

los países democráticos. Al final, los Estados y las entidades internacionales y supranacionales son los últimos garantes del interés público y de los derechos de las personas y no deben renunciar a la regulación y a la supervisión en Internet y a la protección de la privacidad. Como ha señalado recientemente el Presidente Obama, *«one thing should be clear, even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever»*[327].

327. «Presentación» a *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 23 de febrero de 2012.