RPD
REVISTA DEL POSGRADO EN DERECHO DE LA UNAM
NUEVA ÉPOCA, NÚM. 8, ENERO-JUNIO 2018

La revisión del régimen jurídico de la privacidad en la Unión Europea

Luis Ángel Ballesteros Moffa[1]

Resumen: Es conocido el momento de madurez que atraviesa el instituto de protección de datos personales en la Unión Europea, con una ambiciosa renovación de su régimen común, que obligará a revisar la regulación interna de los Estados miembros. La Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, tiene los días contados merced a la aprobación del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016. El cual obedece a los nuevos retos tecnológicos y de globalización, unidos a la necesidad de una regulación homogénea directamente aplicable que evite las divergencias en la ejecución y aplicación de la Directiva, aunque no será aplicable hasta el 25 de mayo de 2018. Renovación que, también en forma de Reglamento europeo de directa aplicación, se hace extensiva a los particulares riesgos que las comunicaciones electrónicas, y, sobre todo, Internet, representan para la información personal. A la vez que se hace más exigente desde esta perspectiva la lucha común contra la delincuencia organizada y el terrorismo, según evidencian la Directiva (UE) 2016/680 de policía y la Directiva (UE) 2016/681 de transferencia de datos PNR.

Palabras clave: *privacidad, Reglamento general de protección de datos, comunicaciones electrónicas, seguridad.*

Abstract: The right to personal data protection is going through a maturity period in the European Union, with an ambitious reform of its legal system, forcing Member States to reform their regulations. The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, will be replaced by Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016. This

[1] Doctor en Derecho y Profesor Titular de Derecho Administrativo (acred. Catedrático) Universidad de León (España).

Regulation is attributable to the emerging challenges of technology and globalisation, together with the need for homogeneous and directly applicable regulation that will avoid divergences in the implementation and application of the Directive, although it shall not come into effect until 25 May 2018. Reform, also in the form of a European Regulation with direct application, is extended to the specific risks of electronic communications, and in particular the internet, for the personal information. At a time of renewal of the data protection legal framework from the perspective of common fight against organised crime and terrorism, as evidenced by the Directive 2016/680 for data protection in the police and criminal justice sectors, and the Directive 2016/681 on the use of PNR data.

KEYWORDS: *privacy, General Data Protection Regulatio, electronic communications, security.*

SUMARIO: I. El reglamento (UE) 2016/679, del parlamento europeo y del consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos: un punto de inflexión en la tutela jurídica de los datos personales; II. La adaptación de la protección de la información personal a los distintos ciclos tecnológicos: un reglamento europeo sobre privacidad y comunicaciones electrónicas; III. Los límites al derecho de protección de datos personales; IV. Bibliografía.

I. EL REGLAMENTO (UE) 2016/679, DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 27 DE ABRIL DE 2016, RELATIVO A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS: UN PUNTO DE INFLEXIÓN EN LA TUTELA JURÍDICA DE LOS DATOS PERSONALES

1. El art. 8 De la Carta de Derechos Fundamentales de la Unión Europea, de 7 de diciembre de 2000

A nadie se le oculta que el instituto de protección de datos personales constituye una de las respuestas más enérgicas del Derecho al carácter potencialmente lesivo de las tec-

nologías de la información y comunicación. Aunque no faltan voces que consideran sobredimensionada la última revolución tecnológica,[2] cuanto mayores son los avances y posibilidades técnicas mayor y más preciso es el papel asumido por los ordenamientos en la conjura de las patologías de la sociedad de la información.[3] El "lado oscuro de internet"[4] como principal fuente de desafíos, que también en lo jurídico exige de una consideración interdisciplinar a partir de los contextos internacional y europeo. Sin dejar de profundizar en la ventana administrativa abierta de la intimidad informática o autodeterminación informativa, en concurso con el sector de las comunicaciones electrónicas, tanto en su dimensión externa de tutela administrativa a los ciudadanos como interna de servicios y ficheros administrativos.

Decisivos hitos que evidencian la consolidación jurídica de la protección de datos personales, frustrando –aquí sí– cualquier "utopía digital". En particular, interesa reparar en los que han dado lugar a sus líneas maestras, europeas e internas, constitucionales y administrativas. Y en la traducción de sus facultades negativas y positivas a los específicos riesgos de las comunicaciones electrónicas, en permanente adaptación a la deriva tecnológica. Lo que permite dibujar sin dificultad una premisa de sólidas raíces y renovadas ramificaciones jurídicas, que ponen al día la institución.

En el frontispicio del régimen jurídico, la salvaguarda de la información personal se erige en un derecho fundamental con sustantividad propia, a tenor del art. 8 de la Carta de Derechos Fundamentales de la Unión Europea, de 7 de diciembre de 2000, adaptada el 12 de diciembre de 2007. "Toda persona tiene derecho a la protección

---

[2] Gordon, R. J., *The Rise and Fall of American Growth. The U.S. Standard of Living Since the Civil War*, s.c., Princeton University, 2016.

[3] Lyon, D., *El ojo electrónico. El auge de la sociedad de la vigilancia*, Madrid, Alianza Editorial, 1995.

[4] Morozov, E., *El desengaño de internet. Los mitos de la libertad en la red*, Barcelona, Destino, 2012; y *La locura del solucionismo tecnológico*, Madrid, Katz, 2015.

de los datos de carácter personal que la conciernan [...]", reza este precepto jurídicamente vinculante, con independencia del respeto a la vida privada y familiar del art. 7;[5] junto con los arts. 39 del Tratado de la Unión Europea y 16 del Tratado de Funcionamiento de la Unión, que reclaman normas tuitivas frente a tratamientos comunitarios y estatales, también en el ámbito de la política exterior y seguridad común, y sobre la libre circulación de estos datos.

Por lo que se refiere al ordenamiento español, tras excluir la naturaleza interna de derecho de estricta configuración legal por la mera remisión del art. 18.4 de la Constitución, se suma su incardinación como derecho fundamental en el sistema constitucional de protección de los arts. 53, 81 y 149.1.1.ª –con otros preceptos menores, como el art. 47.1.a) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que considera nulos de pleno derecho aquellos actos administrativos lesivos de derechos susceptibles de amparo constitucional–.[6] Encontrando este acomodo constitucional a través del

[5] Tal y como aconsejó el Grupo de Protección de las Personas, como órgano consultivo independiente de la Unión Europea creado en virtud del art. 29 de la Directiva 95/46/CE, en virtud de su Recomendación 4/99, Inclusión del derecho fundamental a la protección de datos en el Catálogo europeo de derechos fundamentales, aprobada el 7 de septiembre de 1999 (ref. 5066/00, WP 26).

[6] El Tribunal Constitucional acepta su naturaleza de derecho constitucional aunque de configuración legal, es decir, de verdadero derecho constitucional que requiere de *interpositio legislatoris* para la definitiva fijación de su contenido y desarrollo, y consiguiente plena eficacia. Con la importante precisión de que incluso este tipo de derechos constitucionales de configuración legal gozan de un contenido esencial mínimo garantizado directamente por el texto constitucional, capaz de hacerse valer con anterioridad a su desarrollo legal, y susceptible de servir de pauta de constitucionalidad de esta regulación legal *ex* art. 53.1 Constitución, referente al respeto del contenido esencial de los derechos constitucionales por parte de su regulación legal. Con lo que nuestro máximo intérprete constitucional no solo ha compatibilizado el fundamento constitucional del derecho con la remisión legal del art. 18.4, sino también con el art. 53.1. Considerando en concreto incluidas en este contenido esencial mínimo de configuración constitucional tanto la vertiente negativa de exclusión como las propias facultades de disposición y control de la

reconocimiento de un derecho fundamental autónomo, respecto de otros clásicos derechos como el de la intimidad,[7] sin perjuicio de su intrínseca relación, como evidenciara la postura un tanto ecléctica de la STC 292/2000, de 30 de noviembre,[8] según la cual, la vertiente negativa del derecho que se refiere a datos personales íntimos corresponde tanto al derecho a la intimidad como al derecho autónomo de protección de datos, mientras que la vertiente negativa de datos personales no íntimos, más la vertiente positiva de cualquier tipo de dato personal, corresponde exclusivamente al derecho autónomo de protección de datos del art. 18.4 de la Constitución.[9]

---

vertiente positiva, habiendo defendido no obstante la exclusiva inclusión de la vertiente negativa dentro de este núcleo de configuración constitucional previo al desarrollo legal, el Voto Particular a la STC 254/1993, de 20 de julio, formulado por el Magistrado y entonces Presidente del Tribunal Constitucional Rodríguez-Piñero y Bravo-Ferrer.

[7] Que, en el caso del Voto Particular a la STC 290/2000, de 30 de noviembre, formulado por el Magistrado Jiménez de Parga y Cabrera, y al que prestó su adhesión el Magistrado De Mendizábal Allende, se asentaba en un derecho atípico o no escrito de creación jurisprudencial como una de las funciones del Tribunal Constitucional.

[8] Estimatoria del recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra determinadas previsiones limitativas de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por no cumplir la doctrina de límites a los derechos fundamentales. En concreto, esta STC 292/2000 declaró inconstitucionales y nulos determinados incisos de sus arts. 21.1 y 24.1 y 2, por los que se reconocían límites o excepciones genéricas e indeterminadas a las facetas positivas de la libertad informática en favor de las Administraciones (en concreto, a los derechos de cesión de datos bajo consentimiento u *ope legis*, información, acceso, rectificación y cancelación), por no cumplir con el requisito del art. 53.1 de la Constitución de reserva de ley, ni tampoco con el respeto al contenido esencial del derecho fundamental limitado, exigido asimismo por el mencionado precepto constitucional.

[9] Véanse Verdier Hernández, S., Comentarios sobre la STC 292/2000, de 30 de noviembre, relativa a la inconstitucionalidad de determinados preceptos de la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, *El Consultor de los Ayuntamientos y de los Juzgados*, núm. 17, septiembre 2001, pp. 2865-2876; De La Torre Trinidad, S., "Creación de un derecho fundamental

2. La directiva 95/46/ce, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, y el reglamento (ue) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016

Es la naturaleza de derecho fundamental precisamente la que ha dejado en manos del legislador orgánico estatal en España las competencias legislativas en la materia, sin perjuicio naturalmente de la legislación autonómica y conexa en la medida en que la reserva de ley orgánica del art. 81.1 de la Constitución[10] se vincula restrictivamente al desarrollo general y directo de los derechos fundamentales, sin menoscabo de la numerosa legislación específica con incidencia en privacidad, como su traslación a las comunicaciones electrónicas o en el marco de la transparencia pública. Si la primera Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD) bebía directamente del art. 18.4 de la Constitución y del Convenio núm. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal,

---

a la protección de datos", *El Consultor de los Ayuntamientos y de los Juzgados*, núm. 19, octubre 2001, pp. 3193-3194; Jiménez Rius, P., "Estudio de la Sentencia del Tribunal Constitucional 292/2000, por la que se declaran inconstitucionales determinados artículos de la Ley Orgánica 15/1999, de Protección de Datos Personales", *Al Día*, núm. 22, noviembre 2001, pp. 1-4; Serrano Pérez, M.ª M., *El derecho fundamental a la protección de datos. Derecho español y comparado*, Thomson-Civitas, Navarra, 2003, pp. 171 y ss.; Campuzano Laguillo, A. B., "Algunas consideraciones sobre la libertad informática y el derecho a la protección de datos de carácter personal en la jurisprudencia constitucional", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 1, 2003, pp. 99 y ss.; Rebollo Delgado, L., *Derechos fundamentales y protección de datos*, Madrid, Dykinson, 2004.

[10] Frente a las reservas de ley establecidas tanto en el art. 18.4 de la Constitución –respecto a la protección de datos– como en el art. 53.1 de la Constitución –en relación a todos los derechos constitucionales del Capítulo segundo del Título primero–, asépticas a la hora de asignar la competencia a uno u otro legislador.

hecho en Estrasburgo el 28 de enero de 1981,[11] la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) transpone la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Instrumento de armonización que cumple con dos de las ambiciones más antiguas del proyecto de integración europea, ocupando desde entonces un lugar destacado en el Derecho de la Unión: la realización del mercado interior (libre circulación de datos personales) y la protección de los derechos fundamentales. Cuya transposición ha completado el Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD), además del anterior Estatuto de la Agencia Española de Protección

[11] Si los primigenios documentos centrados en la incidencia de los avances tecnológicos sobre los derechos humanos vieron la luz en el seno de Naciones Unidas y Consejo de Europa, muy pronto esa misma preocupación se extendería a otros foros, como las propias Comunidades Europeas o la OCDE. Ha sido de hecho bajo los auspicios de estas cuatro Organizaciones desde donde han surgido los documentos maestros en la materia, como ejes vertebradores de su armonización internacional. Entre ellos, la Resolución de la ONU 2450 (XXIII), de 19 de diciembre de 1968, donde se reconoce la necesidad de fijar límites a las aplicaciones de la electrónica por su incidencia en los derechos de la persona, siendo el punto de partida de ulteriores informes y trabajos; la Recomendación de la OCDE, de 23 de septiembre de 1980, referente a las líneas directrices tendentes a regular la protección de la vida privada y los flujos transfronterizos de datos de carácter personal, así como su Recomendación de 26 de noviembre de 1992, sobre la seguridad de los sistemas de información; y el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, firmado en Estrasburgo el 28 de enero de 1981. Véanse Frosini, V., "La convenzione europea sulla protezione dei dati", *Rivista di Diritto Europeo*, núm. 24, 1984, pp. 3-18; Ausems, E. J., "La protección de las personas frente al tratamiento automatizado de los datos personales en el marco del Convenio 108 del Consejo de Europa", en *Jornadas sobre informática judicial y protección de datos personales*, Vitoria-Gasteiz, 1994, pp. 15-27.

de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo, declarado vigente por la disposición transitoria tercera de la LOPD.

Una Directiva que tiene los días contados merced a la aprobación del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la misma. Pues, aunque sus objetivos y principios siguen siendo válidos, el Reglamento, que será aplicable –con efecto de su derogación– a partir del 25 de mayo de 2018, obedece a los nuevos retos tecnológicos y de globalización, que requieren un marco más sólido, coherente y simplificado en la Unión Europea, capaz de combinar la apertura a los flujos internacionales de datos con el máximo grado de protección de las personas físicas.[12] Unido a la necesidad de una regulación homogénea directamente aplicable que evite las divergencias en la ejecución y aplicación de la Directiva, garantizando poderes equivalentes en los veintiocho Estados para supervisar y garantizar el cumplimiento de las reglas de protección bajo sanciones equivalentes.[13] Sin que la normativa única paneuropea, por otra parte, excluya la regulación de los Estados, al disponer de cierto margen de maniobra para trasladar y especificar aquella, lo que exigirá la reforma de nuestra LOPD y resto de normativa interna.

---

[12] Establece el marco estratégico de la Comisión con respecto a las decisiones de adecuación, así como otros mecanismos de transferencia de datos e instrumentos internacionales de protección de datos, en el contexto de facilitar su circulación mediante el fomento de la convergencia de los ordenamientos jurídicos, la Comunicación de la Comisión al Parlamento Europeo y Consejo, "Intercambio y protección de los datos personales en un mundo globalizado", COM (2017) 7, de 15 de febrero de 2017.

[13] Por todos, Piñar Mañas, J. L. (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2017; López Calvo, J., *Comentarios al Reglamento europeo de protección de datos*, Madrid, Sepín, 2017; Plaza Penadés, J., "Implementado el nuevo Reglamento europeo de protección de datos", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 43, 2017.

A la vez que se refuerzan y especifican los derechos de los interesados y las obligaciones de los responsables de los tratamientos. Como meridianamente se deriva de la nueva definición de consentimiento de los arts. 4.11) y 7 del Reglamento, los cuales, frente a la ambigüedad y disparidad de la actual terminología, como una de sus carencias más clamorosas, exigen una acción positiva como consentimiento expreso. De forma que, "cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales". Con la importante precisión, además, de que "al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato".[14] Bajo la convicción, según el considerando trigésimo segundo, de que "el consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, 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

[14] En este sentido, el considerando decimoctavo de la Propuesta de Reglamento sobre privacidad y comunicaciones electrónicas, que más adelante se analizará, afirma que "el consentimiento para el tratamiento de datos derivados del uso de internet o de comunicaciones de voz no será válido si el interesado no goza de verdadera libertad de elección o no puede denegar o retirar su consentimiento sin verse perjudicado.

silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento [...].[15]

3. Competencias y organización administrativa

Pero tan importante o más que la consagración teórica de los distintos derechos que forman parte de la protección de datos, es la articulación legal de instrumentos y organismos de ejecución, control y tutela administrativa, en aras de hacer verdaderamente efectiva la protección. "Garantía institucional que se traduce en capítulos tan importantes como la inscripción, tutela, inspección y sanción, en respuesta a reclamaciones de los interesados ante la denegación de sus derechos por parte de los responsables de los tratamientos, o denuncias de cualquier ciudadano a efectos sancionadores; amén de la tutela judicial y, en particular, del derecho a indemnización conforme al sistema de responsabilidad patrimonial administrativa (en ficheros públicos) o Jurisdicción ordinaria (en ficheros privados). Como quiera que los arts. 28 de la Directiva 95/46/CE y 51 y ss. del Reglamento (UE) 2016/679 exigen a los Estados miembros disponer de una o más autoridades públicas independientes y que, junto con la Agencia Española de Protección de Datos, tienen la consideración de autoridades de control también aquellos órganos o instituciones que pueden crear las Comunidades Autónomas, se hace preciso el reparto interno de estas competencias ejecutivas, máxime cuando ni la Constitución ni los Estatutos de Autonomía las contemplan entre las materias objeto de reparto competencial.[16]

[15] Martínez-Rojas, A., "Principales aspectos del consentimiento en el Reglamento general de protección de datos de la Unión Europea, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 42, 2016, pp. 59-82; Adsuara Varela, B., "El consentimiento, en Piñar Mañas, J. L. (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus, 2017, pp. 151-169.

[16] Prueba de la controversia son los sendos recursos de inconstitucionalidad interpuestos por el Consejo Ejecutivo de la Generalidad de Cataluña y el Parlamento de Cataluña contra determinados preceptos de la antigua LORTAD

Mientras el art. 40 LORTAD reconocía de tutela autonómica exclusivamente los ficheros creados o gestionados por las Comunidades Autónomas, el art. 41 LOPD extendió dicha ejecución autonómica a aquellos otros ficheros pertenecientes a las distintas Administraciones locales del ámbito territorial autonómico,[17] siendo legitimada la competencia estatal respecto de todos los ficheros de titularidad privada –también, por tanto, radicados en territorio autonómico y creados en ámbitos competenciales descentralizados– por la STC 290/2000, de 30 de noviembre, con base en la proyección institucional del art. 149.1.1.ª de la Constitución.

En la actualidad, amén de la Agencia Española de Protección de Datos, como Entidad institucional pública del sector público estatal, con naturaleza de Autoridad administrativa independiente de los arts. 109 y 110 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, actúan como instituciones autonómicas independientes: la Autoridad Catalana de Protección de Datos (Ley 32/2010, de 1 de octubre, derogatoria de la Ley 5/2002, de 19 de abril; y Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos), la Agencia Vasca de Protección de Datos (Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia; y Decretos 308/2005, de 18 de octubre, de desarrollo de esta Ley y 309/2005, de 18 de octubre, por el que se aprueba el Estatuto de la Agencia) y el Consejo de Transparencia y Protección de Datos de Andalucía (Ley 1/2014, de 24 de junio, de Transparencia

por presunta infracción del orden constitucional de competencias entre el Estado y las Comunidades Autónomas en materia de ejecución administrativa de dicha Ley; recursos que, tras subsistir a la aprobación de la LOPD y consiguiente derogación de aquella, fueron desestimados por la STC 290/2000, de 30 de noviembre.

[17] Sin perjuicio siempre de la notificación de la creación, modificación o cancelación de todo fichero a la Agencia Española de Protección de Datos para su inscripción en el Registro General de Protección de Datos, que puede consultarse a través de su página web: <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/otros_derechos/consulta_RGPD-ides-idphp.php>.

Pública de Andalucía; y Decreto 434/2015, de 29 de septiembre, por el que se aprueban los Estatutos del Consejo).[18] La independencia de estas autoridades de control es enfatizada por los arts. 52 y 53 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Organización administrativa interna que se completa con la previsión de otros organismos a nivel comunitario, como el Grupo de protección de las personas en lo que respecta al tratamiento de los datos personales *ex* art. 29 de la Directiva 95/46/CE o Comité europeo de protección de datos *ex* arts. 68 y ss. del Reglamento (UE) 2016/679, compuestos por los Directores de las autoridades nacionales y el Supervisor Europeo de Protección de Datos o sus representantes.

4. La administración electrónica

Sirva asimismo el blindaje de la privacidad ante el desarrollo del capítulo interno y europeo de la Administración electrónica. Con el reconocimiento explícito, entre los derechos de los ciudadanos en sus relaciones con las Administraciones, más allá del régimen ponderado de acceso a la información pública, "a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas [art. 13.h) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas]. Articulado frente a las ciberamenazas, además de por las medidas de seguridad del RLOPD, por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de

[18] La Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal de la Comunidad de Madrid y el Decreto 40/2004, de 18 de marzo, por el que se aprobó el Estatuto de la Agencia de Protección de Datos de la Comunidad de Madrid, fueron derogados por la Ley 8/2012, de 28 de diciembre, de Medidas Fiscales y Administrativas, cuyo art. 61 extinguió dicha Agencia territorial siendo reintegradas sus competencias a la Agencia Española de Protección de Datos.

Seguridad en el ámbito de la Administración Electrónica –actualizado por el Real Decreto 951/2015, de 23 de octubre–, a fin de asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen las Administraciones públicas en el ejercicio de sus competencias.[19] Y, en cuanto a la Administración comunitaria, a partir de una Propuesta de la Comisión Europea, de 10 de enero de 2017, de nuevo Reglamento para la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión Europea y sobre la libre circulación de estos datos [COM (2017) 8]. El cual derogará el actual Reglamento (CE) 45/2001, del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, así como la Decisión 1247/2002/CE, para garantizar una protección equiparable a la exigida a los Estados en virtud de las normas más rigurosas del Reglamento general (UE) 2016/679.

II. La adaptación de la protección de la información personal a los distintos ciclos tecnológicos: un reglamento europeo sobre privacidad y comunicaciones electrónicas

1. Las directivas 97/66/CE, del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, y 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002

El potencial de las comunicaciones electrónicas y, en particular, de Internet viene representando un punto de inflexión en la protección

[19] Fondevila Antolín, J., "Seguridad en la utilización de medios electrónicos. El esquema nacional de seguridad, en Gamero Casado, E. (dir.), *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público*, Valencia, Tirant lo Blanch, 2017, vol. I, pp. 597-674.

de la privacidad, en la medida en que no solo acentúa los riesgos generales, sino que genera además riesgos específicos a través de fórmulas de acceso, almacenamiento y uso electrónico de la información con el común denominador de resultar "invisibles para su titular. Son estos riesgos específicos a los que pretende dar respuesta la regulación de la privacidad electrónica, en una suerte de interacción entre los sectores de protección de datos y telecomunicaciones, implementando instrumentos precisos y actualizados como complemento a la regulación general a partir de sus mismos principios. En el bien entendido de que la Directiva 95/46/CE o el Reglamento (UE) 2016/679 siguen respondiendo a los problemas genéricos de privacidad, presentes con especial agresividad en la transmisión electrónica y servicios vinculados.[20]

Puede afirmarse que el derecho a la protección de datos ha tenido que ir adaptándose a los distintos ciclos en aras de proporcionar una respuesta integral a la sociedad tecnológica que cubra todos los focos de vulnerabilidad de la información personal, en una secuencia marcada por los distintos estadios complementarios de protección:[21] siempre por detrás de la tecnología, de los ficheros informatizados, incluso no automatizados, a los rastros en la red de los servicios de comunicaciones electrónicas, pasando por las tradicionales telecomunicaciones, hasta los servicios de transmisión libre *over-the-top* (OTT).

---

[20] Según el décimo considerando de la Directiva 2002/58/CE sobre privacidad y comunicaciones electrónicas, "en el sector de las comunicaciones electrónicas es de aplicación la Directiva 95/46/CE, en particular para todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales que no están cubiertas de forma específica por las disposiciones de la presente Directiva, incluidas las obligaciones del responsable del tratamiento de los datos y los derechos de las personas, aplicándose asimismo "a los servicios de comunicaciones electrónicas que no sean de carácter público.

[21] Ballesteros Moffa, L. A., "La adecuación del instituto de protección de datos a los distintos ciclos tecnológicos, *Actualidad Jurídica Aranzadi*, núm. 690, noviembre 2005, pp. 1, 10 y 11.

En el punto de partida de esta secuencia, como marco general ante el impacto informático sin perjuicio de su extensión a ficheros no automatizados, se sitúa la Directiva 95/46/CE, que, como se ha dicho, será derogada por el Reglamento (UE) 2016/679. La primera Directiva específica en orden a traducir sus principios para el campo de las tradicionales telecomunicaciones, en especial en su salto digital, fue la Directiva 97/66/CE, del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones;[22] que fue transpuesta al ordenamiento español por la antigua Ley 11/1998, de 24 de abril, General de Telecomunicaciones y su Reglamento de desarrollo, aprobado por Real Decreto 1736/1998, de 31 de julio. Directiva que, por su sobrevenido anacronismo con la realidad de las comunicaciones electrónicas, especialmente de internet y servicios convergentes, no tardaría en ser sustituida por la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas;[23] siendo incorporada

[22] Fernández Esteban, M.ª L.ª, *Nuevas tecnologías, internet y derechos fundamentales*, Madrid, McGraw Hill, 1998, pp. 139 y ss.; Suñé Llinás, E., "La protección de la intimidad en el sector de las telecomunicaciones, en Davara Rodríguez, M. A. (coord.), *Encuentros sobre Informática y Derecho (1998-1999)*, Navarra, Universidad Pontificia Comillas, Aranzadi, 1999, pp. 79-90; Corripio Gil-Delgado, M.ª R. y Marroig Pol, L., *El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones*, Madrid, Agencia Española de Protección de Datos, 2001; Campuzano Tomé, H., *Vida privada y datos personales. Su protección jurídica frente a la sociedad de la información*, Madrid, Tecnos, 2000, pp. 131 y ss.

[23] Esta Directiva fue adoptada con ocasión de la revisión de las antiguas Directivas de telecomunicaciones, conforme al nuevo marco regulador de redes y servicios de comunicaciones electrónicas cristalizado en el año 2002 como consolidación del modelo liberalizador a partir de la Directiva marco 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo. Siendo modificada por las Directivas 2009/136/CE, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009; y 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso

en España por la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones –hoy derogada por la Ley 9/2014, de 9 de mayo–, la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico –modificada por la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información–, y el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril, al cual se remite el art. 31 del Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas.[24]

2. La propuesta por la Comisión Europea, de 10 de enero de 2017, de un reglamento relativo al respeto de la vida privada y a la protección de los datos personales en el ámbito de las comunicaciones electrónicas [COM (2017) 10]

Secuencia que se cierra de momento con la Propuesta por la Comisión Europea, de 10 de enero de 2017, de un Reglamento relativo

público o de redes públicas de comunicaciones. Véanse Davara Rodríguez, M. A., *La protección de datos personales en el sector de las comunicaciones electrónicas*, Madrid, Universidad Pontificia Comillas, 2003; Prieto Andrés, A., "La nueva Directiva europea sobre el tratamiento de datos personales y la protección de la intimidad en el sector de las telecomunicaciones, *Diario La Ley*, núm. 5620, septiembre 2002; Cimas, M., "Protección de datos y telecomunicaciones. Regulación actual y exigencias de la nueva Directiva, en Villar Uríbarri, J. M. (dir.), *La nueva regulación de las telecomunicaciones, la televisión e Internet*, Navarra, Thomson-Aranzadi, 2003, pp. 289-309; guerrero picó, M.ª C., *El impacto de internet en el derecho fundamental a la protección de datos de carácter personal*, Navarra, Thomson-Civitas, 2006.

[24] Este último Real Decreto transpone la la Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, en materia de servicio universal y derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, con la derogación del Título VI del Reglamento de servicio universal y derechos de los usuarios del Real Decreto 424/2005, de 15 de abril.

al respeto de la vida privada y a la protección de los datos personales en el ámbito de las comunicaciones electrónicas, por la que se derogará la Directiva 2002/58/CE [COM (2017) 10]. Norma de directa aplicación con la que se pretende completar un marco jurídico actualizado de privacidad en Europa, reforzando la confianza y seguridad en el mercado único digital. Para una mayor protección a abonados y usuarios, dimanante en buena medida de la asunción del Reglamento general (UE) 2016/679, sin que ello merme las oportunidades comerciales de innovación. Pero, sobre todo, de su adaptación a la coyuntura económica y tecnológica de las comunicaciones electrónicas, donde los consumidores y empresas recurren cada vez más a nuevos servicios basados en internet que permiten comunicaciones interpersonales, como los servicios de comunicaciones *over-the-top* (OTT), en los que no media control alguno ni gestión específica por parte de los operadores de red. Extendiendo su aplicación así a los nuevos proveedores de servicios de comunicaciones electrónicas (WhatsApp, Facebook Messenger, Skype, Gmail, iMessage o Viber) desde la remisión al concepto más avanzado de las mismas de la Propuesta de Directiva, de 12 de diciembre de 2016, por la que se establece el Código Europeo de las Comunicaciones Electrónicas [COM (2016) 590].[25]

Lo cual se suma al ya amplio objeto de aplicación de la Directiva 2002/58/CE, que incluye, más allá de la regla general de su art. 3 ("la presente Directiva se aplicará al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Comunidad […]"), algunas reglas específicas de protección respecto de los servicios de la sociedad de la información, en cuanto servicios prestados normalmente a cambio

[25] La protección de estos servicios de comunicación electrónica funcionalmente equivalentes es reclamada por el Dictamen 3/2016, de 19 de julio, del Grupo Europeo de Protección de Datos sobre "la evaluación y revisión de la Directiva de privacidad electrónica (2002/58/CE) (ref. 16, WP 240).

de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios [Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, sobre el comercio electrónico y Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información]. Con obligaciones, por tanto, no solo para operadores de redes y proveedores de servicios de comunicaciones electrónicas, sino también para prestadores de la amplia gama de servicios de transmisión o contenido en internet. Lo que explica su transposición, no sin alguna disfunción, tanto por la Ley General de Telecomunicaciones como por la Ley de Servicios de la Sociedad de la Información.[26]

Entre los capítulos específicos de privacidad electrónica en favor de abonados o usuarios, sean personas físicas o jurídicas en esta ocasión, se encuentra el tratamiento de los datos de conexión de las comunicaciones electrónicas, objeto del presente estudio desde la perspectiva de la seguridad. Además de toda una batería de potenciales vulnerabilidades de la información personal en la transmisión electrónica y particularmente en el ciberespacio: interceptación ilegal de comunicaciones, *cookies* y demás dispositivos de almacenamiento y recuperación de información en el terminal del usuario, guías públicas impresas o electrónicas de abonados, comunicacio-

---

[26] Féral-Schuhl, C., *Cyberdroit. Le droit à l'épreuve de l'internet*, Dunod, Paris, 2000; Fenoll-Trousseau, M.-P. y Haas, G., *Internet et protection des données personnelles*, Litec, Paris, 2000; Del Peso Navarro, E., *Servicios de la sociedad de la información. Comercio electrónico y protección de datos*, Madrid, Díaz de Santos, 2003; Oliver Lalana, D., "El derecho fundamental "virtual" a la protección de datos. Tecnología transparente y normas privadas, *Diario La Ley*, núm. 5592, julio 2002; Villar Uríbarri, J. M. (dir.), *La nueva regulación de las telecomunicaciones, la televisión e Internet*, Navarra, Thomson-Aranzadi, 2003; Aparicio Vaquero, J. P., "El nuevo régimen de prestación de servicios de la sociedad de la información, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 2, 2003, pp. 87-111.

nes comerciales no solicitadas o *spam*, servicios avanzados de telefonía… A las que las precitadas normas trasladan específicamente los principios rectores de seguridad, cancelación y oposición, y sobre todo información y consentimiento, bien en su versión de *opt out* o consentimiento tácito que no precisa acto formal alguno, bien de *opt in* o consentimiento expreso que exige acto formal de aceptación.[27]

Disyuntiva que parece declinarse definitivamente hacia la segunda en atención al Reglamento general (UE) 2016/679, aun cuando su art. 95 establece que el mismo no impondrá obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación de la Unión en ámbitos en los que estén sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE. O, en cualquier caso, a la luz de la Propuesta de Reglamento sobre privacidad y comunicaciones electrónicas, cuyo art. 9 se remite al consentimiento expreso del Reglamento general (UE) 2016/679, sin perjuicio de conservar los supuestos de consentimiento tácito en el *spam* menos agresivo de las llamadas de telefonía con intervención humana o que traiga causa de una relación comercial preexistente, y ampliar incluso los tratamientos legales de metadatos por razones de calidad, seguridad técnica o para detectar el uso fraudulento o abusivo de servicios, con exclusión también del consentimiento para algunas *cookies*, por ejemplo, cuando sean necesarias para medir la audiencia en la *web*.

---

[27] Ballesteros Moffa, L. A., *La privacidad electrónica. Internet en el centro de protección*, Valencia, Tirant lo Blanch, 2005.

III. Los límites al derecho de protección de datos personales

1. El difícil equilibrio entre privacidad y otros derechos; en particular, la seguridad

Pese al arraigo y transformación jurídica de la privacidad, también en el específico escenario de las comunicaciones electrónicas, en modo alguno se concibe en términos absolutos, debiendo cohonestarse con otras exigencias y prioridades, como la seguridad y preservación del orden jurídico.[28] Tal y como reconoce el considerando cuarto del Reglamento (UE) 2016/679, "[…] el derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. Lo cual entronca con la jurisprudencia constitucional sobre los límites a los derechos fundamentales a partir del art. 53.1 de la Constitución, aplicada en esta materia en la citada STC 292/2000, de 30 de noviembre, a partir de la quíntuple exigencia cumulativa de que sea una ley la que los restrinja; que el límite legal se encuentre justificado por algún otro interés o bien constitucionalmente protegido; que responda al principio de necesidad y proporcionalidad; que respete, en todo caso, el contenido esencial del derecho fundamental limitado; y que resulte preferente el bien constitucional justificativo sobre el propio derecho limitado".

En realidad, el baluarte jurídico de los datos personales en sí mismo es un ejercicio de equilibrio entre este derecho y otros fronterizos, ya sea desde la perspectiva de su propio régimen u otras instituciones. Regímenes que se baten entre el reconocimiento de

---

[28] López Calvo, J., *Comentarios al Reglamento europeo de protección de datos*, *op. cit.*, pp. 41 y ss.

las distintas facultades de protección de datos y las excepciones a las mismas, fruto de funciones de índole administrativa, sanitaria, judicial, científica, estadística o comercial, o de implicación antagónica de otras libertades, como la de expresión e información. Y del derecho a saber cuando el acceso a la información pública contiene datos personales, para el que rige el principio de consentimiento expreso del afectado para datos especialmente protegidos, y de previa ponderación suficientemente razonada entre el interés público en la divulgación de cualquier otra información personal y los derechos de los afectados cuyos datos aparezcan en la información solicitada (art. 15 de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno).

Haciéndose presentes asimismo estas tensiones en las soluciones adoptadas por la regulación específica de privacidad en las comunicaciones electrónicas, por el valor estratégico comercial de algunas *cookies* que ha llevado a ampliar los supuestos en que no se exige consentimiento expreso; el de aquellas comunicaciones comerciales no solicitadas que por su menor lesividad siguen vinculadas a consentimiento tácito; por el interés público de divulgación de las guías –impresas o electrónicas– de abonados, que no obstante está cediendo en favor de la salvaguarda de sus datos personales; por la necesaria ponderación entre el mismo derecho al olvido y el de recibir acceso a la información por los usuarios, no procediendo aquel cuando esta sea de interés para el público por su naturaleza o afecta a una figura pública;[29] o a la luz del régimen de privacidad dispensado frente a los servicios avanzados de telefonía de facturación desglosada, desvío automático de llamadas e identificación de la línea telefónica de origen y conectada. Pero, sobre todo, cuando la seguridad, la lucha contra el crimen u otros motivos de interés ge-

[29] Por todos, Álvarez Caro, M.ª, "El derecho a la supresión o al olvido, en Piñar Mañas, J. L. (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus, 2017, pp. 241-256; López Calvo, J., *Comentarios al Reglamento europeo de protección de datos*, *op. cit.*, pp. 140 y ss.

neral avalan la interceptación legal de comunicaciones, frente a la garantía de secreto del art. 18.3 de la Constitución española, cuya violación en el ámbito de las comunicaciones electrónicas cuenta con el Reglamento (UE) 611/2013, de la Comisión, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas.[30] Y cuando los mismos fines de investigación y represión penal, por lo que atañe al presente trabajo, justifican las obligaciones de conservación temporal y cesión de los datos de tráfico y localización de las comunicaciones electrónicas, como limitación al régimen de protección de una información que, sin consentimiento, solo debe ser tratada para llevar a cabo la conducción de la comunicación, su facturación o los pagos de interconexiones.

Precisamente para que la información personal se proteja al tiempo que se previene y combate el terrorismo, el crimen organizado y otros actos criminales, son la seguridad del Estado, la defensa, la seguridad pública y la prevención, investigación, descubrimiento y persecución de delitos, las necesidades de mayor intensidad que pueden encauzar medidas comunitarias o estatales

[30] Se trata de un procedimiento de notificación a la autoridad nacional competente, y en algunos casos a los abonados y particulares afectados, por parte de los proveedores de servicios de comunicaciones electrónicas, obligados según el art. 4 de la Directiva 2002/58/CE, con el fin principalmente de que la autoridad sea informada de la forma más rápida y exhaustiva posible, sin que ello entorpezca los esfuerzos del proveedor por investigar el caso y tomar las medidas necesarias para limitarlo y remediar sus consecuencias. Se considera violación de datos personales, de acuerdo con la Directiva 2002/58/CE, "toda violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público en la Unión. Esta notificación en el sistema general de protección de datos se contempla en los arts. 33 y 34 del Reglamento (UE) 2016/679.

limitativas del alcance de las obligaciones y derechos de protección de datos.[31] El art. 23.1 del Reglamento (UE) 2016/679, como en términos más lacónicos el art. 13 de la Directiva 95/46/CE, establece que "el Derecho de la Unión o de los Estados miembros […] podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención; e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social; f) la protección de la independencia judicial y de los procedimientos judiciales; g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas; h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g); i) la protección del interesado o de los derechos y libertades de otros; j) la ejecución de

[31] Cole, D. D.; Fabbrini, F. y Schulhofer, S. (ed.), *Surveillance, Privacy and Trans-Atlantic Relations*, Oxford, Hart Publishing, 2017; De Asís Roig, A., "Secreto, protección de datos y seguridad e integridad en las telecomunicaciones, en Parejo Alfonso, L. y Vida Fernández, J. (coord.), *Los retos del Estado y la Administración en el siglo XXI. Libro homenaje al Profesor Tomás de la Quadra-Salcedo Fernández del Castillo*, Valencia, Tirant lo Blanch, 2017, pp. 2105-2141.

demandas civiles".[32] Añadiendo el apartado 2, a diferencia de la Directiva 95/46/CE, que cualquiera de estas medidas legislativas habrá de contener disposiciones específicas sobre la finalidad del tratamiento, las categorías de datos, el alcance de las limitaciones, las garantías para evitar accesos o transferencias ilícitos o abusivos, los responsables, los plazos de conservación, los riesgos y el derecho a información. Limitaciones que de forma análoga son reiteradas para los capítulos específicos de privacidad electrónica en los arts. 15.1 de la Directiva 2002/58/CE y 11.1 de la Propuesta de Reglamento sobre privacidad y comunicaciones electrónicas, los cuales se remiten respectivamente a aquellos preceptos generales. En concreto, según la Propuesta, el Derecho de la Unión o de un Estado miembro podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y los derechos previstos en los artículos 5 a 8, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria, adecuada y proporcionada en una sociedad democrática para salvaguardar uno o varios de los intereses públicos generales contemplados en el artículo 23, apartado 1, letras a) a e), del Reglamento (UE) 2016/679 o una función de control, inspección o reglamentación vinculada al ejercicio de la autoridad pública en aras de tales intereses.

El art. 15.1 de la Directiva 2002/58/CE alberga la previsión general de conservación de los metadatos derivados de las comunicaciones electrónicas, como una de las manifestaciones más claras en el entorno en línea de la pugna entre privacidad y seguridad. Se-

[32] Por su parte, tras reconocer que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia, el art. 8 del Convenio Europeo de Derechos Humanos prescribe de forma análoga que "no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

gún el mismo, "los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado". Disposición que, tras la aprobación de la Directiva específica de conservación de datos, se acompaña de un nuevo apartado 1 bis, introducido por la misma, en el sentido de que "el apartado 1 no se aplicará a los datos que deben conservarse específicamente de conformidad con la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, para los fines recogidos en el artículo 1, apartado 1, de dicha Directiva". Sustrayéndose así esta específica armonización de la posibilidad general contemplada con anterioridad en la Directiva 2002/58/CE. De modo que, una vez declarada la invalidez de la Directiva 2006/24/CE por el Tribunal de Justicia de la Unión Europea (STJUE de 8 de abril de 2014, Digital Rights Ireland/Minister for Communications y otros [asunto C-293/12] y Kärntner Landesregierung y otros [asunto C-594/12]), las normas internas de retención de datos han quedado amparadas exclusivamente por dicha previsión de la Directiva 2002/58/CE. Aunque habrá que valorar, a la luz de la jurisprudencia europea, en qué medida estas obligaciones de los operadores de redes y servicios de comunicaciones electrónicas de conservar determinados datos generados o tratados por ellos para su ulterior disposición por los agentes facultados en el marco de una investigación criminal, siguen encontrando fundamento en el Derecho europeo. Teniendo en cuenta que la Propuesta de Reglamento en privacidad y comunicaciones electrónicas no incluye ya ninguna previsión en este sentido, lo que, más allá de las limitaciones genéricas, dejaría huérfanas a las normas internas de conservación vigentes, aprobadas en transposición de la Directiva específica.

2. La directiva (ue) 2016/680 de policía

Regresando a la interacción entre el régimen general de privacidad y la seguridad, y de acuerdo con la exclusión de los arts. 3.2 y 2.2.d) de la Directiva 95/46/CE y del Reglamento (UE) 2016/679 respectivamente, la provisión y tratamiento de datos personales con fines penales cuenta con su particular norma europea para la protección de los mismos, y sobre todo para que esta protección no enerve el intercambio de datos personales por parte de las autoridades competentes en el interior de la Unión. Es la Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Directiva de policía, cuyo plazo de transposición concluye el 6 de mayo de 2018, con la que se busca conciliar en la lucha contra las actividades delictivas un nivel uniforme y elevado de protección de los datos personales y su intercambio entre los Estados miembros, sin perjuicio de la transmisión también a terceros países u organizaciones internacionales. La armonización de estas normas, incluidas las relativas a las transferencias internacionales, representa una contribución fundamental a la Agenda Europea de Seguridad,[33] al facilitar la cooperación transfronteriza entre las autoridades policiales y judiciales, tanto dentro de la Unión Europea como con los socios internacionales, propiciando una mayor eficacia en la represión de la delincuencia. Según los considerandos décimo y undécimo, en la Declaración núm. 21 relativa a la protección de

[33] Comunicación de la Comisión al Parlamento Europeo, Consejo, Comité Económico y Social Europeo y Comité de las Regiones, "Agenda Europea de Seguridad", COM (2015) 185, de 28 de abril de 2015.

datos de carácter personal en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial, aneja al acta final de la Conferencia Intergubernamental que adoptó el Tratado de Lisboa, la Conferencia reconoció que podrían requerirse normas específicas sobre protección de datos personales y libre circulación de los mismos en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial basada en el artículo 16 del Tratado de Funcionamiento de la Unión Europea, en razón de la naturaleza específica de dichos ámbitos. Conviene por lo tanto que esos ámbitos estén regulados por una Directiva que establezca las normas específicas relativas 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, incluidas la protección y la prevención frente a las amenazas para la seguridad pública. […] Cuando dicho organismo o entidad trate datos personales con fines distintos de los previstos en la presente Directiva, se aplica el Reglamento (UE) 2016/679 […].

3. La directiva (ue) 2016/681 de transferencia de datos pnr

La privacidad se sujeta en particular a las exigencias de seguridad, con independencia del reconocimiento adaptado de sus principios y facultades, en la Directiva (UE) 2016/681, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, con un plazo máximo de transposición de 25 de mayo de 2018. Aparte de la comunicación de información anticipada sobre los pasajeros con objeto de mejorar los controles fronterizos y combatir la inmigración ilegal se-

gún la Directiva 2004/82/CE, del Consejo, de 29 de abril de 2004 (*Advance Passenger Information*-datos API), se regula la obligación de las compañías aéreas que realicen vuelos exteriores de la Unión Europea (pudiéndose ampliar por los Estados a vuelos intracomunitarios, previa notificación a la Comisión) de transferir a las autoridades nacionales todos los datos del registro de nombres de los pasajeros recogidos en sus sistemas de reservas internos, con el fin de prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y delitos graves (*Passenger Name Record*-datos PNR).[34] Información que es objeto de intercambio mutuo entre los Estados miembros y con Europol, e incluso de transferencia a autoridades de terceros países conforme a requisitos adicionales. Lo que viene dando lugar a Acuerdos PNR bilaterales, como los suscritos entre la Unión Europea y los Estados Unidos para la transferencia de información personal desde las compañías aéreas europeas a este socio trasatlántico.[35] Teniendo en cuenta el Acuerdo marco entre Estados Unidos

---

[34] Sobre los métodos técnicos de transferencia (*pull* de acceso o *push* de envío), el considerando decimosexto clarifica que "en la actualidad se dispone de dos métodos de transferencia de datos: el método de extracción, en el que las autoridades competentes del Estado miembro que solicita los datos PNR pueden acceder al sistema de reserva de la compañía aérea y obtener ('extraer') una copia de los datos PNR deseados, y el método de transmisión, en el que las compañías aéreas envían ('transmiten') los datos PNR a la autoridad solicitante, lo que permite a las compañías aéreas mantener el control de los datos suministrados. Se considera que el 'método de transmisión' ofrece un nivel mayor de protección de los datos y que debe ser obligatorio para todas las compañías aéreas".

[35] Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, hecho en Bruselas el 14 de diciembre de 2011, y por el que se sustituye al Acuerdo de 23 y 26 de julio de 2007. Al que se suma el Acuerdo entre la Comunidad Europea y el Gobierno de Canadá sobre el tratamiento de datos procedentes del sistema de información anticipada sobre pasajeros y de los expedientes de pasajeros, de 3 de octubre de 2005. Y el Acuerdo entre la Unión Europea y Australia sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por los transportistas aéreos al Servicio de Aduanas y de Protección de las

y la Unión Europea, de 2 de junio de 2016, sobre protección de datos personales en relación con la prevención, investigación, detección y enjuiciamiento de infracciones penales.[36]

iv. Bibliografía

Adsuara Varela, B., "El consentimiento", en Piñar Mañas, J. L. (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2017.

Álvarez Caro, M.ª, "El derecho a la supresión o al olvido", en Piñar Mañas, J. L. (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2017.

Aparicio Vaquero, J. P., "El nuevo régimen de prestación de servicios de la sociedad de la información", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 2, 2003.

Fronteras de Australia, de 29 de septiembre de 2011. Véase Ballesteros Moffa, L. A., "Hacia un difícil equilibrio entre privacidad y seguridad: la conservación de datos en las comunicaciones electrónicas y la transferencia de datos de pasajeros por las compañías aéreas", *Revista Española de Derecho Administrativo*, núm. 137, enero/marzo 2008, pp. 17 y ss.

[36] Como señala el segundo considerando de la Decisión (UE) 2016/2220, del Consejo, de 2 de diciembre de 2016, relativa a la celebración, en nombre de la Unión Europea, del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la protección de los datos personales en relación con la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales, "el Acuerdo persigue establecer un marco general de principios y salvaguardias de la protección de los datos personales cuando dichos datos se transfieren a efectos policiales y judiciales en materia penal entre los Estados Unidos de América, por una parte, y la Unión Europea y sus Estados miembros, por otra. El objetivo es garantizar un alto nivel de protección de los datos y, de este modo, reforzar la cooperación entre las Partes. Aunque no constituya en sí mismo la base jurídica para todas las transferencias de datos personales a los Estados Unidos, el Acuerdo complementa, en caso necesario, las garantías de protección de datos previstas en los acuerdos en materia de transferencia de datos actuales y futuros o las disposiciones nacionales que autorizan tales transferencias.

AUSEMS, E. J., "La protección de las personas frente al tratamiento automatizado de los datos personales en el marco del Convenio 108 del Consejo de Europa", en *Jornadas sobre informática judicial y protección de datos personales*, Vitoria-Gasteiz, 1994.

BALLESTEROS MOFFA, L. A., *La privacidad electrónica. Internet en el centro de protección*, Valencia, Tirant lo Blanch, 2005.

———, "Hacia un difícil equilibrio entre privacidad y seguridad: la conservación de datos en las comunicaciones electrónicas y la transferencia de datos de pasajeros por las compañías aéreas", *Revista Española de Derecho Administrativo*, núm. 137, enero/marzo 2008.

CAMPUZANO LAGUILLO, A. B., "Algunas consideraciones sobre la libertad informática y el derecho a la protección de datos de carácter personal en la jurisprudencia constitucional", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 1, 2003.

CAMPUZANO TOMÉ, H., *Vida privada y datos personales. Su protección jurídica frente a la sociedad de la información*, Madrid, Tecnos, 2000.

CIMAS, M., "Protección de datos y telecomunicaciones. Regulación actual y exigencias de la nueva Directiva", en VILLAR URÍBARRI, J. M. (dir.), *La nueva regulación de las telecomunicaciones, la televisión e Internet*, Navarra, Thomson-Aranzadi, 2003.

COLE, D. D.; FABBRINI, F. y SCHULHOFER, S. (ed.), *Surveillance, Privacy and Trans-Atlantic Relations*, Oxford,Hart Publishing, 2017.

CORRIPIO GIL-DELGADO, M.ª R. y MARROIG POL, L., *El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones*, Madrid, Agencia Española de Protección de Datos, 2001.

DAVARA RODRÍGUEZ, M. A., *La protección de datos personales en el sector de las comunicaciones electrónicas*, Madrid, Universidad Pontificia Comillas, 2003.

DE ASÍS ROIG, A., "Secreto, protección de datos y seguridad e integridad en las telecomunicaciones", en PAREJO ALFONSO, L. y VIDA FERNÁNDEZ, J. (coord.), *Los retos del Estado y la Administración en el siglo XXI. Libro homenaje al Profesor Tomás de la Quadra-Salcedo Fernández del Castillo*, Valencia, Tirant lo Blanch, 2017.

De La Torre Trinidad, S., "Creación de un derecho fundamental a la protección de datos", *El Consultor de los Ayuntamientos y de los Juzgados*, núm. 19, octubre 2001.

Del Peso Navarro, E., *Servicios de la sociedad de la información. Comercio electrónico y protección de datos*, Madrid, Díaz de Santos, 2003.

Fenoll-Trousseau, M.-P. y Haas, G., *Internet et protection des données personnelles*, Litec, Paris, 2000.

Féral-Schuhl, C., *Cyberdroit. Le droit à l'épreuve de l'internet*, Dunod, Paris, 2000.

Fernández Esteban, M.ª L.ª, *Nuevas tecnologías, internet y derechos fundamentales*, Madrid, McGraw Hill, 1998.

Fondevila Antolín, J., "Seguridad en la utilización de medios electrónicos. El esquema nacional de seguridad", en Gamero Casado, E. (dir.), *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público*, vol. I, Valencia, Tirant lo Blanch, 2017.

Frosini, V., "La convenzione europea sulla protezione dei dati", *Rivista di Diritto Europeo*, núm. 24, 1984.

Gordon, R. J., *The Rise and Fall of American Growth. The U.S. Standard of Living Since the Civil War*, s.c., Princeton University, 2016.

Guerrero Picó, M.ª C., *El impacto de internet en el derecho fundamental a la protección de datos de carácter personal*, Navarra, Thomson-Civitas, 2006.

Jiménez Rius, P., "Estudio de la Sentencia del Tribunal Constitucional 292/2000, por la que se declaran inconstitucionales determinados artículos de la Ley Orgánica 15/1999, de Protección de Datos Personales", *Al Día*, núm. 22, noviembre 2001.

López Calvo, J., *Comentarios al Reglamento europeo de protección de datos*, Madrid, Sepín, 2017.

Lyon, D., *El ojo electrónico. El auge de la sociedad de la vigilancia*, Madrid, Alianza Editorial, 1995.

Martínez-Rojas, A., "Principales aspectos del consentimiento en el Reglamento general de protección de datos de la Unión Europea", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 42, 2016.

Morozov, E., *El desengaño de internet. Los mitos de la libertad en la red*, Barcelona, Destino, 2012.

———, *La locura del solucionismo tecnológico*, Madrid, Katz, 2015.

Oliver Lalana, D., "El derecho fundamental "virtual" a la protección de datos. Tecnología transparente y normas privadas, *Diario La Ley*, núm. 5592, julio 2002.

Piñar Mañas, J. L. (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus, 2017.

Plaza Penadés, J., "Implementado el nuevo Reglamento europeo de protección de datos", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 43, 2017.

Prieto Andrés, A., "La nueva Directiva europea sobre el tratamiento de datos personales y la protección de la intimidad en el sector de las telecomunicaciones", *Diario La Ley*, núm. 5620, septiembre 2002.

Rebollo Delgado, L., *Derechos fundamentales y protección de datos*, Madrid, Dykinson, 2004.

Serrano Pérez, M.ª M., *El derecho fundamental a la protección de datos. Derecho español y comparado*, Navarra, Thomson-Civitas, 2003.

Suñé Llinás, E., "La protección de la intimidad en el sector de las telecomunicaciones", en Davara Rodríguez, M. A. (coord.), *Encuentros sobre Informática y Derecho (1998-1999)*, Navarra, Universidad Pontificia Comillas, Aranzadi, 1999.

Verdier Hernández, S., "Comentarios sobre la STC 292/2000, de 30 de noviembre, relativa a la inconstitucionalidad de determinados preceptos de la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal", *El Consultor de los Ayuntamientos y de los Juzgados*, núm. 17, septiembre 2001.

Villar Uríbarri, J. M. (dir.), *La nueva regulación de las telecomunicaciones, la televisión e Internet*, Navarra, Thomson-Aranzadi, 2003.