Universitat Autònoma de Barcelona

DECONSTRUYENDO LAS TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES
Desprotección en los Estados Unidos de América y el entorno asiático

D. Albert Castellanos Rodríguez

Universitat Autònoma de Barcelona

TESIS DOCTORAL

DECONSTRUYENDO LAS TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES

Desprotección en los Estados Unidos de América y el entorno asiático.

D. Albert Castellanos Rodríguez

Tesis depositada en cumplimiento de los requisitos para el programa de Doctor en Derecho

Universitat Autònoma de Barcelona
Facultad de Derecho
Departamento de Derecho Público y Ciencias Histórico-jurídicas

Director: Dr. D. Josep Cañabate-Pérez

Septiembre de 2021

A mis padres, Pedro y Montse, por apoyarme siempre por adversas que fueran las circunstancias y recordarme la importancia de la vida y sus valores.

A Clara, que con su paciencia y con su comprensión infinita, ha contribuido significativamente a alcanzar lo pretendido.

ÍNDICE

AGRADECIMIENTOS

La elaboración de esta tesis doctoral, pese a ser una decisión personal, no hubiera visto la luz sin la inestimable ayuda de mi círculo familiar más cercano. A pesar de haber sido realizada a tiempo parcial, el soporte recibido ha sido fundamental en los momentos más complicados, pues al estar compaginada con mi desarrollo profesional, éstos no han sido pocos. Por lo que aquí, quiero expresar mi más sentido agradecimiento a todas y cada una de esas personas que han contribuido a hacer posible el presente trabajo de investigación, aunque sea de manera anonimizada —vista la materia que se pretende analizar—.

De manera especial, por un lado, quiero agradecer sinceramente el apoyo recibido por parte de mi madre. Sin ella, la redacción de esta tesis doctoral no hubiera sido posible. Por todo ello, se merece el más profundo de los agradecimientos posible.

Y, por otro lado, también quisiera agradecer a Clara su apoyo y comprensión, por haberme acompañado durante esta etapa vital. Su ayuda ha sido profunda y valiosa.

Particularmente, y bajo la obtención de su respectivo consentimiento, procedo a dar las gracias a Josep Cañabate, mi tutor y director de tesis, pero antes que nada, amigo y guía espiritual. Sus conocimientos, valores y cercanía han sido parte esencial de que este trabajo pudiera finalizarse. Su influencia ha ido más allá de lo profesional, demostrando que la humildad y la excelencia pueden conjugarse en una única persona.

Finalmente, aprovecho para mostrar mi agradecimiento a la Universidad Autónoma de Barcelona, así como a todas aquellas personas que han aportado su pequeño granito de arena propiciando la redacción de este trabajo.

ABREVIATURAS

- AEPD: Agencia Española de Protección de Datos.
- API: *Advanced Passenger Information*
- APN: Asamblea Popular Nacional de China
- APPI: *Act on the Protection of Personal Information of Japan*
- CCT: Cláusulas Contractuales Tipo.
- CDFUE: Carta de Derechos Fundamentales de la Unión Europea.
- CE: Constitución española de 1978.
- CEDH: Convenio Europeo de Derechos Humanos.
- CEPD: Comité Europeo de Protección de Datos.
- CGPJ: Consejo General del Poder Judicial
- Convenio 108: Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal
- Directiva PNR: Directiva relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.
- EE.MM.: Estados Miembros integrantes de la Unión Europea
- EEE: Espacio Económico Europeo.
- EFTA: Asociación Europea de Libre Comercio
- ENISA: Agencia Europea de Ciberseguridad
- EO 12333: *Executive Order 12333* de 1981
- FAQ: Preguntas frecuentes.
- FISA: *Foreign Intelligence Surveillance Act*

- FISC: *Foreign Intelligence Surveillance Court*
- FTC: *Federal Trade Commission*.
- GT29: Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE.
- ICO: *Information Commissioner's Office*
- LIBE: Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo
- LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- LORTAD: Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.
- NCV: Normas Corporativas Vinculantes
- NSA: *National Security Agency*
- OCDE: Organización para la Cooperación y el Desarrollo Económico.
- PDPAS: *Personal Data Protection Act of Singapur*
- PDPAT: *Personal Data Protection Act of Taiwán*
- PNR: Registro de nombres de los pasajeros.
- PPC: Comisión de Protección de Información Personal de Japón
- PPD-28: *Presidential Policy Directive 28*
- RGPD: Reglamento General de Protección de Datos.
- RLOPD: Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- Schrems I: Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 6 de octubre de 2015, en el asunto C- 362/14
- Schrems II: Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 16 de julio de 2020, en el asunto C-311/18
- Sentencia DRI: Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 8 de abril de 2014, en los asuntos acumulados C-293/12 y C-594/12
- SEPD: Supervisor Europeo de Protección de Datos.
- SIS: Sistema de Información de Schengen.
- TC: Tribunal Constitucional de España.
- TEDH: Tribunal Europeo de Derechos Humanos.
- TFUE: Tratado de Funcionamiento de la Unión Europea
- TJUE: Tribunal de Justicia de la Unión Europea.
- TS: Tribunal Supremo de España.
- TUE: Tratado de la Unión Europea
- UIP: Unidad de Información sobre los Pasajeros

INTRODUCCIÓN

SUMARIO: 1. Planteamiento del problema; 2. Objeto de la investigación; 3. Metodología de investigación; 4. Contenido de la investigación.

1. Planteamiento del problema

Los datos se han convertido en una infraestructura vital o incluso en la nueva "luz del sol", dado que se encuentran en todas partes y lo sustentan todo, tal y como ha tenido la oportunidad de afirmar el diario británico *The Economist*[1]. Las organizaciones cada vez más están reuniendo grandes volúmenes de datos sin apenas restricciones, con la intención de someterlos a una serie de tratamientos de análisis de patrones y perfilados avanzados para hacer posible la obtención de un rédito económico a partir de su explotación. Según datos publicados por la OCDE, dichas actividades generaban en 2017 alrededor de sesenta mil millones de dólares en ganancias para los Estados Unidos. Respectivamente, al otro lado del Atlántico, las cifras alcanzaban los cincuenta mil millones de euros en el contexto de la Unión Europea.

Adicionalmente, la globalización ha tenido también una influencia trascendental en el ámbito de la tecnología y la gestión de la información. Ha comportado que cantidades masivas de datos se muevan de un lado a otro del globo en apenas cuestión de segundos. Este intercambio de datos no se produce únicamente entre instituciones, organizaciones o entes públicos, sino que los propios ciudadanos lo favorecen a través de las publicaciones que efectúan en sus propias redes sociales, las cuáles ostentan un papel esencial dentro de este complejo escenario. En la mayoría de las ocasiones, estos movimientos de datos se realizan fuera del ámbito de la Unión Europea, poniendo en jaque los derechos y libertades de los afectados, esto es, los titulares del bien jurídico protegido.

[1] *Vid*. KER, D. y MAZZINI, E., *Perspectives on the value of data and data flows*, Paris: OECD Digital Economy Papers, No. 299, OECD Publishing, 2020. Consultado el 05.05.2021 desde: https://doi.org/10.1787/a2216bc1-en

En este sentido, se podría afirmar en términos generales que las transferencias internacionales de datos personales se han consolidado en los últimos años como un mecanismo imprescindible para el favorecimiento de la evolución de la sociedad tecnológica y la globalización. De dicho fenómeno se han percatado los distintos actores del tejido empresarial y económico, pudiendo observar que —motivada por la alta competitividad de los mercados— se ha producido una tendencia al alza en la obtención de datos de los ciudadanos. Cuestiones relacionadas con su vida privada, comportamiento, hábitos de consumo, salud, orientación social, sexual y/o política, entre muchas otras, constituyen en la actualidad un producto básico para mejorar la rentabilidad de las organizaciones.

De hecho, el "ARPU", cuyas siglas en inglés se corresponden con el "Promedio de Ingresos por Usuario", no ha parado de crecer desde el inicio del pasado siglo XX. Según datos facilitados por ENISA[2] —organismo europeo en materia de ciberseguridad—, en 2017 alcanzó los 59 dólares por persona en publicidad digital, sector controlado principalmente por Google y Facebook. Por lo que, si multiplicamos este número por un promedio aproximado de 3.800 millones de usuarios activos de Internet, podríamos alcanzar una estimación sobre las elevadas cifras económicas que podría llegar a generar este negocio.

Así pues, el uso de la tecnología parece haberse convertido en el mejor aliado de empresas e instituciones, aportando innumerables beneficios cualitativos y cuantitativos para su eficiencia y transformación digital. Estas contribuciones —como se subraya al inicio de este apartado— no se han realizado sin repercusiones, sino que es una realidad palpable que en la actualidad se producen movimientos internacionales de datos sin restricciones ni salvaguardas de ningún tipo , que comportan un tratamiento de los datos personales sin las suficientes garantías. Dicha tesitura juega directamente en contra de la tutela de los derechos y libertades de los afectados que intenta preservar el derecho fundamental a la protección de los datos personales.

La situación anterior produce una dicotomía que resulta palpable directamente en el ámbito del estudio que aquí nos ocupa. Las reglas del juego se han estructurado de tal manera que los afectados por la recogida de datos personales disponen de una serie de

[2] *Vid*. ENISA, "The Value of Personal Online Data", 23 de abril de 2018. Consultado el 22.08.2019 desde: https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data.

derechos y garantías que velan por el tratamiento lícito de estos. Al mismo tiempo, los responsables que se encargan de la obtención y el tratamiento de estos datos están supeditados a una serie de deberes y obligaciones. Este escenario se adentra en una dimensión aún más compleja cuando además los datos se remiten a terceros destinos que no disponen de una legislación específica que vele por el cumplimiento del derecho fundamental a su protección.

Por ende, se produce entonces una situación de difícil encaje y regulación. Los intereses que concurren son contrapuestos. Por un lado, encontramos aquellos vinculados a la protección propia y al respeto de los derechos constitucionales relacionados con la libertad de información, la protección de la intimidad y los datos de carácter personal[3]. Y, por otro lado, se advierten los legítimos intereses comerciales de empresas e instituciones en utilizar los datos personales para la obtención de beneficios económicos o comerciales.

Esta dicotomía ha producido que en nuestra historia reciente se hayan cosechado algunos escándalos que reflejan la dificultad de buscar un equilibrio jurídico entre los distintos intereses contrapuestos. Uno de ellos puede advertirse en el caso "Cambridge Analytica", estrechamente vinculado a la campaña política de Trump y, en última instancia, al resultado de las elecciones celebradas en 2016 en los Estados Unidos de América. En este caso, se analizaron aproximadamente hasta 5.000 puntos de datos por persona sobre una población de más de 230 millones de ciudadanos norteamericanos, utilizando más de cien variables de datos y algoritmos que moldeaban grupos de audiencia objetivo para predecir su comportamiento y determinar así su intención de voto[4].

Otro supuesto similar podríamos encontrarlo con lo sucedido sobre la situación del "*Brexit*" y el papel que jugó la compañía canadiense de análisis de datos "Aggregate IQ Data Services, Ltd.". Al respecto, existen ciertas manifestaciones efectuadas por parte de la Autoridad de Protección de Datos del Reino Unido que aluden al papel fundamental que desempeñó dicha empresa en el referéndum europeo que se celebró sobre la cuestión.

---

[3] *Vid*. ESTADELLA YUSTE, O., "La transmisión internacional de datos personales y su control", en *Jornadas sobre Derecho Español de Protección de Datos Personales*, Madrid: Ed. Agencia de Protección de Datos, 1996, p. 195.

[4] *Vid*. CADWALLADR, C. y GRAHAM-HARRISON, E., "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", en *The Guardian*, 17 de marzo de 2018. Consultado el 22.08.2019 desde: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Dicha organización habría participado analizando toda una serie de datos personales para finalidades estrictamente políticas que de algún modo podrían haber influido en la intención de voto de los electores británicos[5].

Ni siquiera en España hemos sido ajenos a esta tipología de escándalos. Podemos encontrar un supuesto similar en los efectos producidos por la modificación del artículo 58 bis de la Ley Electoral General a través de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, durante su tramitación parlamentaria. Al no encontrarse dicha cuestión prevista en el Anteproyecto de Ley inicial remitido por el Gobierno a la Agencia Española de Protección de Datos, no pudo ser objeto de informe preceptivo por parte de la referida autoridad de control. No obstante, dicho articulado pasó posteriormente su examen de legalidad al ser declarado inconstitucional por parte del Tribunal Constitucional[6].

Teniendo en cuenta lo anterior, resulta conveniente advertir de los riesgos y amenazas que supone el tratamiento internacional e indiscriminado de los datos de carácter personal sin que medien unas salvaguardas adecuadas. La pérdida de garantías en el ejercicio de los derechos y libertades de los ciudadanos se ha constatado como una realidad, convirtiéndose en uno de los mayores quebraderos de cabeza para las sociedades democráticas en los últimos años. Más ejemplos de lo apuntado podríamos encontrarlos también en las revelaciones efectuadas por Edward Snowden, a través del periódico británico *The Guardian*, en junio de 2013[7], así como con la sucesión de numerosas brechas de seguridad que se han producido en los últimos años, entre las que podemos

[5] *Vid*. ICO. "Investigation into the use of data analytics in political campaigns", 11 de julio de 2018. Consultado el 24.08.2019 desde: https://ico.org.uk/media/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf.

[6] *Vid*. TC. " Nota informativa nº 74/2019", 22 de mayo de 2019. Consultado el 24.08.2019 desde: https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_074/NOTA%20INFORMATIVA%20N%C2%BA%2074-2019.pdf.

[7] *Vid*. MACASKILL, E. y DANCE, G., "NSA Files: Decoded. What the revelations mean for you", en *The Guardian*, 1 de noviembre de 2011. Consultado el 22.08.2019 desde: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

mencionar, entre otras, la relativa a Uber[8] o FedEx[9] en 2016 y 2017, respectivamente, o, más recientemente, la de Marriot[10], constituyen en su conjunto una pequeña muestra de lo apuntado.

En consecuencia, la expectativa de privacidad del ciudadano se ha visto mermada en gran parte, siendo la transmisión de información personal de éste a terceros el coste para poder acceder a determinados servicios o productos supuestamente gratuitos. La búsqueda de un equilibrio ha resultado convertirse en un auténtico reto. Las últimas iniciativas legislativas comunitarias toman cuenta de ello, otorgándole al afectado la posición de consumidor que le hubiera correspondido desde hace algunas décadas. En particular, con esta aseveración se alude a la Directiva (UE) 2019/770, del Parlamento Europeo y del Consejo de 20 de mayo de 2019, que incluye en su ámbito de aplicación, aquellos contratos en los que el empresario suministra o se compromete a suministrar contenidos o servicios digitales al consumidor a cambio de que este facilite o se comprometa a facilitar sus datos personales, tal y como se establece en la Exposición de Motivos del Real Decreto-ley 7/2021, de 27 de abril[11].

Este nuevo escenario influenciado por la aparición de nuevas tecnologías propició que, durante la segunda mitad del siglo XX hasta la actualidad, se haya gestado la aparición de un nuevo derecho de corte constitucional y fundamental, vinculado a la protección de los datos de carácter personal. Sus primeras apariciones se circunscriben territorialmente a los Estados Unidos de América a finales del siglo XIX, de la mano del juez Thomas Cooley cuando expresaba la aseveración *"the right to be let alone"* —el

---

[8] *Vid*. UBER. "Información sobre el incidente de seguridad de datos de 2016". CONSULTADO el 22.08.2019 desde: https://help.uber.com/riders/article/informaci%C3%B3n-sobre-el-incidente-de-seguridad-de-datos-de-2016?nodeId=12c1e9d1-4042-4231-a3ec-3605779b8815.

[9] *Vid*. SHABAN, H. "FedEx delivery unit hit by worldwide cyberattack", en *The Washington Post*, 28 de junio de 2017. Consultado el 22.08.2019 desde: https://www.washingtonpost.com/news/the-switch/wp/2017/06/28/fedex-delivery-unit-hit-by-worldwide-cyberattack/?noredirect=on.

[10] *Vid*. ICO. "Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach", 9 de julio de 2019. Consultado el 24.08.2019 desde: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.

[11] España. Real Decreto-ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores. Consultado el 05.05.2021 desde: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-6872

derecho a no ser molestado— mediante una de sus obras más representativas. Posteriormente serían las teorías formuladas por dos de los juristas más influyentes de dicho sistema jurídico en relación con la materia que nos ocupa, Samuel Warren y Louis Brandeis, quienes desarrollarían primigeniamente la expectativa de privacidad como manifestación propia vinculada al derecho a la intimidad.

Estos planteamientos doctrinales servirían de fundamento teórico para articular lo que posteriormente vendrá a convertirse en un derecho fundamental en el ámbito europeo y en un auténtico derecho propio a la autodeterminación informativa en el ordenamiento jurídico estadounidense, cuyo soporte se articulará mediante el respeto de la dignidad de la persona y el libre desarrollo de su personalidad. No obstante, ha resultado extremadamente dificultoso regular en tiempo real los desarrollos tecnológicos que se han ido sucediendo por parte de los poderes legislativos estatales. Esta circunstancia ha desencadenado que, por más esfuerzos que se realicen para mitigar el riesgo de descontrol existente en lo relativo a la supervisión en la utilización de los datos e información personal por parte de los afectados, siempre exista un amplio margen de mejora. Incluso, en ocasiones, pese a la complejidad de la situación, nos encontramos adicionalmente con operadores económicos y entes privados que aúnan fuerzas en torpedear aún más esta difícil coyuntura.

Así pues, el derecho a la protección de los datos de carácter personal o a la autodeterminación informativa ha ido evolucionando para intentar adecuarse a todas estas nuevas realidades, para así convertirse en un mecanismo de salvaguarda efectivo de protección respecto a los derechos y libertades de los afectados frente a la recopilación y el tratamiento de sus datos personales. Su cometido no se centra exclusivamente en perseguir el uso indiscriminado y extensivo efectuado por parte de organizaciones privadas, sino también en perseguir las actuaciones efectuadas por parte de autoridades públicas, que en muchas ocasiones abanderan motivos relacionados con la protección de la seguridad nacional para realizar prácticas abusivas respecto al tratamiento de información personal.

Sin perjuicio de lo anterior, cabe mencionar que en el ordenamiento jurídico estadounidense se parte de una perspectiva histórica diferente a la europea, donde ha existido un mayor consenso en considerar el derecho a la protección de datos de carácter personal con rango fundamental. En el contexto norteamericano, la visión de la privacidad en sus orígenes viene marcada por su vinculación expresa al derecho a la intimidad y al

respeto de la propiedad privada. Su desarrollo posterior estará vertebrado a partir de las disciplinas jurídicas vinculadas al derecho constitucional y mercantil. Por ende, su eje básico se centrará en diferenciar la protección de la intimidad y la privacidad frente a las actuaciones realizadas por parte de las autoridades gubernamentales, así como respecto a ciertas organizaciones del sector privado.

Teniendo en cuenta esta aproximación, puede afirmarse que no existe una relación pacífica entre las autoridades europeas y norteamericanas en lo relativo a la materia que nos ocupa, y especialmente, en relación con las transferencias internacionales de datos personales. Desde la entrada en vigor de la anterior Directiva 95/46/CE, se iniciaron una serie de negociaciones entre la Comisión Europea y el Departamento de Comercio de los Estados Unidos, con la intención de encontrar un marco jurídico adecuado que permitiera un flujo de datos personales entre ambos territorios sin escollos. En ningún caso se trataba de unas intenciones desinteresadas, sino que su cometido principal radicaba en articular un escenario plausible que permitiera aprovechar los beneficios económicos resultantes del tratamiento masivo de los datos personales mediante el uso de nuevas tecnologías.

Finalmente, el 26 de julio del año 2000, se adoptó la Decisión 2000/520/CE. La referida norma amparaba un mecanismo que posibilitaba las transferencias de datos personales de ciudadanos europeos a empresas que tenían su sede en Estados Unidos. Dichas organizaciones, para poder ser destinatarias de la información, debían haber aceptado con carácter previo el respeto de los principios de salvaguarda y protección de la privacidad incluidos en el propio Acuerdo, que paradójicamente pasaría a denominarse "Puerto Seguro". Con posterioridad, quedaría constatado que su contenido no ofrecería ningún tipo de protección y salvaguarda sobre los derechos y libertades de los afectados.

A tenor de la evolución de la sociedad y de la proliferación de nuevas realidades y paradigmas digitales, se suscitaron numerosas cuestiones que vendrían a poner en jaque definitivamente la efectividad de la Decisión de la Comisión 2000/520/CE. Entre ellas, puede destacarse, en primer lugar, el aumento exponencial de la cantidad de organizaciones estadounidenses que decidieron adherirse al Acuerdo de Puerto Seguro. Según datos expresados por parte de la propia Comisión Europea[12], durante el período

[12] *Vid*. Comunicación de la Comisión Europea al Parlamento Europeo y al Consejo, sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la Unión Europea y las empresas establecidas en la misma, de fecha 27 de noviembre de 2013 (COM [2013] 847 final). Consultado el 22.08.2019 desde:

que comprende las anualidades de 2004 hasta 2013 se pasó de 400 en ese primer año a 3.246 en la última de las fechas indicadas.

En segundo lugar, podríamos aducir que las revelaciones desencadenadas por Edward Snowden a través del periódico británico *The Guardian*, en junio de 2013[13], acerca de las operaciones de vigilancia masiva e indiscriminada llevadas a cabo por el Gobierno de los Estados Unidos a través de su Agencia de Seguridad Nacional (en adelante, NSA[14]), pondrían nuevamente de manifiesto las deficiencias normativas existentes en el marco que regulaba las transferencias internacionales de datos personales a territorio estadounidense. Adicionalmente, al mismo tiempo que las organizaciones que habían participado en las actividades de vigilancia masiva aducían sus alegatos de defensa, se sucedieron simultáneamente demandas que abogaban por la suspensión automática y la posterior revocación del Acuerdo de Puerto Seguro. Dichas solicitudes provenían tanto de determinados sectores sociales como de las propias autoridades de control de algunos Estados miembros[15].

En tercer lugar, y siguiendo con lo expuesto, en fecha 6 de octubre de 2015, el Tribunal de Justicia de la Unión Europea, en el marco del asunto C-362/14 (Schrems), hizo público su pronunciamiento, declarando la invalidez de la Decisión de la Comisión, de fecha 26 de julio de 2000. El fundamento jurídico básico que propiciaría tal conclusión radicaba en que las estipulaciones que se contenían en el Acuerdo de Puerto Seguro no garantizaban un nivel de protección suficientemente robusto respecto de los datos personales transferidos desde la Unión Europea a las diferentes compañías sitas en los Estados Unidos de América.

---

http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com(2013)0847_es.pdf.

[13] *Vid*. MACASKILL, E. y DANCE, G., "NSA Files: Decoded…", cit.

[14] La National Security Agency, se podría definir como un órgano de inteligencia creado por parte del gobierno de los Estados Unidos de América, dependiente del Departamento de Defensa, que tiene como principal objetivo el análisis masivo de las comunicaciones, entendido el concepto en un sentido extensivo, con la intención de garantizar la protección y salvaguarda de los intereses gubernamentales.

[15] *Vid*. Resolución del Parlamento Europeo nº 2016/C075/14, de fecha 4 de julio de 2013, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los Estados Unidos, los organismos de vigilancia en varios Estados miembros y su impacto en la vida privada de los ciudadanos de la Unión Europea (2013/2682 [RSP]). Consultado el 28.08.2019 desde: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2013/2682(RSP).

A principios de 2016, concretamente el 29 de febrero de ese mismo año, y transcurridos más de dos años desde el inicio de las negociaciones con el Departamento de Comercio. La Comisión hizo público el proyecto de decisión sobre el nuevo marco regulador de las transferencias internacionales entre ambos territorios, el cual fue acuñado bajo la denominación "*EU-U.S. Privacy Shield framework*"[16]. En fecha 12 de julio de 2016, la Comisión Europea, mediante nota de prensa[17], hizo pública la adopción del Acuerdo sobre el Escudo de Privacidad UE-EE. UU., que constituía el marco normativo que volvía a posibilitar las transferencias internacionales de datos personales de ciudadanos europeos hacia el mencionado territorio.

Dicho Acuerdo gozaría de una escasa vigencia, pues los mismos motivos que motivaron la anulación de la Decisión de la Comisión 2000/520/CE cuatro años atrás, propiciarían que el 16 de julio de 2020 el Tribunal de Justicia de la Unión Europea (Gran Sala), en el asunto C-311/18, volviera a determinar la invalidez del Acuerdo sobre el Escudo de Privacidad UE-EE. UU. La incertidumbre sobre los flujos transatlánticos de datos personales entre los dos territorios volvió a ceñirse sobre las organizaciones, obligando a que las autoridades de control sobre la materia se pronunciaran para intentar disminuir la inseguridad jurídica producida, pero que en la actualidad, a fecha de este trabajo, aún no ha conseguido solventarse.

Entendemos que este trabajo de investigación se fundamenta en la constatación de que los esfuerzos que todavía deben realizarse en relación con la protección de los datos personales pueden calificarse como considerables, a pesar de la existencia de un precedente histórico de evolución favorable en pro de la protección de los derechos y libertades de los afectados. No obstante, el análisis de la institución de las transferencias internacionales de datos resulta uno de los supuestos más flagrantes que ponen de manifiesto la necesidad de buscar una proporcionalidad y un equilibrio entre los intereses en juego. Por un lado, el relativo a las autoridades gubernamentales y organizaciones

[16] *Vid*. Decisión de ejecución (UE), nº 2016/1250, de la Comisión, de fecha, 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. [notificada con el número C-(2016) 4176]. Consultado el 28.08.2019 desde: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D1250&from=EN.

[17] *Vid*. Nota de prensa efectuada por la Comisión Europea, en fecha 12 de julio 2016, sobre la adopción del Acuerdo sobre Escudo de Privacidad UE-EE. UU. Consultado el 28.08.2019 desde: http://europa.eu/rapid/press-release_IP-16-2461_es.htm.

privadas que centran sus esfuerzos en el tratamiento de los datos personales para el cumplimiento de sus fines y la obtención de un rédito comercial o económico. Y, por otro lado, la salvaguarda del bien jurídico protegido por el derecho fundamental a la protección de dichos datos de carácter personal.

A pesar de lo anterior, si bien es cierto que puede constatarse que aquellos países que disponen de una sociedad democrática que ha alcanzado un mayor grado de madurez, han sido capaces de acoger con mayor soltura y rapidez como propias las distintas legislaciones que se han ido sucediendo en materia de protección de datos de carácter personal en el contexto de la Unión. Al mismo tiempo, la situación generada ha tenido un efecto expansivo al irradiar otros sistemas jurídicos con su contenido, como es el caso de los Estados Unidos y del propio continente asiático analizados respectivamente en este trabajo. Dicha casuística se ha venido a denominar como el *"Brussels effect"*[18], esto es, la capacidad significativa de la que dispone la normativa comunitaria de incidir en la políticas legislativas de terceros estados, según los intereses que ésta pretenda consolidar, que en este caso redundarían en la protección de la intimidad y los datos de carácter personal de los ciudadanos.

2. Objeto de la investigación

El objetivo general que pretende alcanzar el presente trabajo de investigación radica en realizar un análisis crítico sobre el régimen jurídico relativo a las transferencias internacionales de datos de carácter personal. Por cuestiones derivadas de la propia naturaleza de la institución, dicho análisis no puede realizarse en abstracto, sino que debe de efectuarse a partir de casuísticas específicas. Para ello se estudiará el ordenamiento jurídico de los Estados Unidos, así como el propio de las economías más avanzadas de Asia Oriental. Adicionalmente, la hipótesis que interesa plantear se centra en la desprotección de los afectados frente a las vulneraciones flagrantes y sistemáticas que se producen en relación con sus respectivos derechos y libertades reconocidos en materia de protección de datos de carácter personal.

[18] El concepto fue acuñado originariamente por parte de la profesora de Derecho de Columbia, Anu Bradford, que sostiene la gran influencia que ejerce a nivel regulatorio la Unión Europea, elevando los estándares internacionales a nivel mundial en diversas materias, como la que aquí nos ocupa, así como en otros ámbitos como la salud, la seguridad jurídica del consumidor, la protección del medio ambiente y ciertas prácticas abusivas en materia de competencia.

Los objetivos específicos que se pretenden conseguir con la consecución de este estudio, son: analizar el origen y evolución del derecho a la protección de datos de carácter personal en el ordenamiento jurídico comunitario y español; contextualizar y estudiar la institución jurídica de las transferencias internacionales de datos desde la perspectiva comunitaria y sus posibles efectos en terceros estados; observar la efectividad de las decisiones de adecuación que se emiten por parte de la Comisión Europea sobre terceros estados que disponen de un nivel de protección adecuado; analizar el origen y evolución del derecho a la intimidad y privacidad en el sistema jurídico estadounidense desde el prisma del derecho comparado; estudiar el ordenamiento jurídico de los Estados Unidos y revisar los esfuerzos realizados en materia de protección de datos de carácter personal; determinar si el país norteamericano puede considerarse como un territorio que ofrece un nivel de protección adecuado desde el punto de vista de la legislación comunitaria; contextualizar la prevalencia de la protección de la seguridad nacional en los Estados Unidos frente a la tutela del derecho fundamental a la protección de datos de carácter personal; analizar la legalidad de los movimientos de datos personales que realiza la Unión Europea en el marco de sus actuaciones de prevención, detección, investigación y enjuiciamiento de los delitos vinculados al terrorismo y a la delincuencia grave respecto los datos del registro de nombres de los pasajeros; discernir el régimen jurídico de aquellas economías más avanzadas de Asia Oriental que disponen de un marco normativo en materia de protección de datos de carácter personal; demostrar si el sistema de derechos y libertades instaurado en las economías asiáticas analizadas puede llegar a considerarse más garantista que el instaurado en el ámbito comunitario; y, constatar si efectivamente se ha producido una estandarización internacional en materia de protección de datos a raíz de las actuaciones legislativas realizadas por parte de la Unión Europea.

3. Metodología de investigación

Una vez que se ha procedido a la exposición del objeto de estudio sobre el que versa el presente trabajo, así como se han presentado los objetivos e hipótesis que se pretenden alcanzar, resulta preciso mencionar que la metodología de investigación utilizada no se ha limitado exclusivamente a analizar el derecho positivo actual, sino que se ha extendido a analizar su contexto, pues la particularidad de la temática escogida así lo exigía. Para el correcto entendimiento de esta disciplina, no ha sido suficiente con entender los aspectos jurídicos, sino que los tecnológicos también juegan un papel

transcendental, dado que intervienen durante todo el ciclo de vida del tratamiento de los datos personales.

En sentido contrario con lo que puede suceder con otras disciplinas jurídicas, en las que el propio conocimiento de la actividad diaria puede servir de base para que los operadores jurídicos puedan aplicar la norma y que esta pueda desplegar sus efectos, en el ámbito del derecho tecnológico o relativo a las nuevas tecnologías el escenario o paradigma resulta un tanto diferente. Nos encontramos con que el conocimiento actualizado de las realidades tecnológicas resulta imprescindible para poder comprender lo dispuesto en la legislación aplicable y que los juristas puedan aplicarla con todos sus plenos efectos jurídicos. Se trata de una metodología que viene aplicándose en materia de protección de datos personales desde sus propios orígenes.

En cualquier caso, la temática principal que centra este trabajo ostenta cierto carácter historiográfico. No obstante, no resultaría favorable limitar únicamente el análisis a la evolución y al desarrollo de este derecho fundamental, dado que se trata de una casuística global que se dirime más allá de las fronteras geográficas entre territorios. Por lo que, por razones obvias, ha resultado preciso realizar un ejercicio de derecho comparado con los ordenamientos jurídicos existentes en otros territorios para ser capaces de identificar y dirimir las principales cuestiones que inciden en la desprotección de los derechos y libertades de los afectados como bien jurídico protegido por la norma.

Dicho lo anterior, se ha partido de una metodología basada en tres niveles de análisis. El primero centrado en el análisis y estudio de material bibliográfico, compuesto por legislación, jurisprudencia, dictámenes emitidos por parte de los organismos y autoridades con competencias sobre la materia, así como de aquellos documentos doctrinales que se han considerado de mayor relevancia para el objeto de la presente tesis doctoral. Un factor determinante ha sido la lectura de los principales pronunciamientos efectuados por parte del Tribunal Europeo de Derechos Humanos, el Tribunal de Justicia de la Unión Europea y el Tribunal Constitucional alemán y español.

El segundo nivel se ha sustentado en realizar un análisis histórico-jurídico de la evolución del derecho a la privacidad o a la protección de datos de carácter personal, así como de la propia institución jurídica relativa a las transferencias internacionales de datos. El tercer nivel se ha ocupado de implementar una metodología de análisis basada en el derecho comparado. Para ello, han resultado fundamentales las obras elaboradas por

Daniel J. Solove y Graham Greenleaf en aras de poder estudiar los respectivos ordenamientos jurídicos estadounidense y asiático desde dicha perspectiva basada en el derecho comparado.

Asimismo, para la elaboración de la bibliografía, se ha partido de una configuración clásica para su ordenación, fundamentada en la siguiente estructura: monografías y obras compuestas; revistas, referencias normativas —diferenciadas entre las fuentes internacionales, comunitarias y nacionales—; y, las referencias jurisprudenciales —diferenciando nuevamente entre fuentes internacionales, comunitarias y nacionales—.

Por último, se cree oportuno dejar constancia de la necesidad de recurrir a la consulta de fuentes escritas en lengua inglesa, por tratarse de una casuística complicada dentro de la materia que aquí nos ocupa, que apenas ha sido tratada en lengua castellana. Adicionalmente, se entiende conveniente manifestar que, en un futuro no demasiado lejano, se pretende articular una nueva línea de investigación centrada en analizar pormenorizadamente, a través de un ejercicio de derecho comparado, la protección que se ofrece en materia de protección de datos en el ámbito norteamericano y europeo, más allá del análisis pormenorizado de una institución, que es la intención que en parte, se ha intentado conseguir como resultado de esta investigación.

4. Contenido de la investigación

El presente trabajo se divide en tres capítulos claramente diferenciados. El primero de ellos se dedica a analizar la construcción histórica del derecho fundamental a la protección de los datos de carácter personal en el ámbito comunitario y español, para que una vez se haya entendido su origen, evolución y contexto, puedan comprenderse los entresijos de la institución jurídica de las transferencias internacionales de datos personales y sus correspondientes efectos, pues se trata de una casuística especialmente compleja de movimientos transnacionales de datos personales.

El segundo capítulo se centra en primera instancia en examinar el origen del concepto "*privacy*" en el ámbito del derecho anglosajón, repasando las teorías formuladas por dos de los juristas más influyentes de dicho sistema jurídico en relación con la materia que nos ocupa, Samuel Warren y Louis Brandeis, hasta analizar en síntesis la protección jurídica que ofrece el ordenamiento norteamericano sobre los derechos de la intimidad y la privacidad, históricamente conectados. En segunda instancia, se aborda el

ordenamiento jurídico de los Estados Unidos y su posible consideración como un país de un nivel de protección adecuado en materia de protección de datos personales. Para ello, se examinan los diferentes acuerdos suscitados entre las instituciones comunitarias y norteamericanas que han intentado garantizar el flujo de datos personales entre ambos territorios.

El tercer capítulo se destina a abordar de manera crítica dos casuísticas especiales englobadas dentro del alcance de la institución jurídica de las transferencias internacionales de datos que se ha venido a examinar. En primer lugar, se ha optado por analizar una de las principales medidas adoptadas para la lucha contra las amenazas antiterroristas que tiene su fundamento en el intercambio masivo de datos personales de pasajeros entre las distintas compañías aéreas y las respectivas autoridades gubernamentales en el contexto de la Unión Europea, e incluso, en ocasiones, hacia los Estados Unidos de América.

Para ello, se analizará el contenido establecido en la Directiva relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave (en adelante, Directiva PNR). Cuya entrada en vigor se produciría el 24 de mayo de 2016 —en la misma fecha que lo hizo el Reglamento (UE) 2016/679—, colisionando directamente con los fundamentos intrínsecos de la cultura jurídica de protección de datos existente en la Unión Europea.

Y, en segundo lugar, se examinará otra de las casuísticas especiales a las que se enfrenta la Unión Europea en el momento de habilitar el flujo de datos personales hacia terceros países que no ostentan un nivel de protección adecuado. En concreto, el análisis se delimitará a discernir el régimen jurídico de aquellas economías más avanzadas de Asia Oriental que disponen de un marco normativo en materia de protección de datos de carácter personal, en aras de demostrar si los mismos dan cobertura suficiente a la protección de la privacidad y los datos de carácter personal. Planteándose incluso, si dicho sistema de derechos y libertades puede llegar a considerarse más garantista —o incluso equiparable— al instaurado en el ámbito comunitario.

CAPÍTULO I – TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES DESDE LA UNIÓN EUROPEA

SUMARIO: 1. Perspectiva histórica del derecho a la protección de datos en Europa; 2. Perspectiva histórica del derecho a la protección de datos en España; 3. Transferencias internaciones de datos. Fundamentación de una institución jurídica; 4. Régimen jurídico de las transferencias internacionales de datos de carácter personal bajo el acervo de la Directiva 45/96/CE. Mención a la LORTAD, a la LOPD y al RLOPD; 5. Enfoque de las transferencias internacionales de datos de carácter personal bajo el acervo del Reglamento (UE) 2016/679, General de Protección de Datos. Mención a la Ley Orgánica 3/2018.

Introducción

El proceso de construcción y consolidación de este derecho de moderna creación ha sido convulso. Sus orígenes fueron duramente cuestionados en relación con su ámbito de autonomía y sus posibles efectos en relación con otros derechos fundamentales. Dichas aseveraciones se verán constatadas en las siguientes líneas de este estudio, cuando se analice su proceso de configuración histórica vinculado al desarrollo gradual del derecho a la intimidad. Sus primeras manifestaciones se consagran como una reacción a los avances tecnológicos sucedidos a finales del siglo XIX y las intromisiones ilegítimas que se efectuaban mediante la toma de imágenes fotográficas sin la debida autorización de los retratados.

Puede apreciarse entonces como la interpretación clásica del derecho a la intimidad vinculado al concepto de la propiedad pasa a evolucionar hacia una vertiente más vinculada a la protección de la dignidad humana y al libre desarrollo de la personalidad. Posteriormente, dichas concepciones serán adaptadas y reformuladas mediante un proceso de configuración jurisprudencial que permitirá regular y hacer frente a las nuevas amenazas y riesgos derivados de la evolución de las nuevas tecnologías. La protección se articulará a través de la formulación de un derecho fundamental que

permitirá a los afectados tutelar, salvaguardar y controlar el tratamiento de sus respectivos datos personales[19].

En este nuevo escenario, las instituciones sitas en el viejo continente europeo jugarán un papel esencial en el fortalecimiento de este nuevo derecho, acogiendo las tesis desarrolladas en el continente norteamericano para profundizar sobre su contenido y vertebrar una estructura uniforme que permitiese su aplicación en distintos países. Principalmente, la labor será desarrollada de manera pionera por el Consejo de Europa hasta conseguir su consagración definitiva como un auténtico derecho fundamental en la Carta de Derechos Fundamentales de la Unión Europea.

Sin perjuicio de lo anterior, no debemos olvidarnos del principal instrumento jurídico que guiará su aplicación práctica hasta el 25 de mayo de 2018, esto es, 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. Pues, a partir de entonces, vendrá a ser sustituida por 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.

Tanto la Directiva como el posterior Reglamento se aplicaron y se aplican respectivamente en el ámbito de la Unión Europea, tanto en organizaciones y entidades públicas como privadas, erigiéndose con el principal cometido de garantizar la protección de los datos personales de los ciudadanos europeos frente a intromisiones ilegítimas originadas por parte de terceros en su esfera más íntima. Lo anterior se pretendía efectuar mediante la armonización de la disparidad de normativas existentes en el contexto de los Estados Miembros de la Unión Europea. Especialmente, el Reglamento se formuló bajo las pretensiones de acontecerse como un marco de referencia universal en la salvaguarda del derecho fundamental a la protección de los datos de carácter personal.

Ante toda esta amalgama normativa, se introduce la institución jurídica que centra nuestro objeto de estudio, esto es, las transferencias internacionales de datos personales. Su regulación se encontraba estipulada en la Directiva 95/46/CE, cuyo testigo ha sido relevado por el Reglamento (UE) 2016/679 aportando toda una serie de novedades en

[19] *Vid*., entre otros, SERRANO PÉREZ, M. M., *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid: Ed. Civitas, 2003.

relación con su regulación. No obstante, el esquema que se sigue no difiere en demasía del previsto originariamente en la Directiva, sino que se ha optado por reforzar algunos extremos que hasta el momento no ofrecían las suficientes garantías que deben resultar aplicables sobre esta tipología de actividades de tratamiento.

En el ámbito español, pese a no reconocerse expresamente el derecho a la protección de los datos de carácter personal en la Constitución española, podemos manifestar que el mismo dispone de rango constitucional mediante su plasmación en el artículo 18.4. Como se verá, el camino hasta su consagración definitiva fue complicado y fruto de una senda labor jurisprudencial. Su regulación se inicia con lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Posteriormente —bajo el acervo de la Directiva 95/46/CE—, seguirá con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Y finalmente, como consecuencia del proceso de adecuación del Reglamento (UE) 2016/679 al ordenamiento jurídico español, su encaje normativo culminará mediante la aprobación de la Ley Orgánica 3/2018. A los efectos de lo que a este estudio interesa, cabe destacar que a través de su "Título VI" regulará lo relativo a las transferencias internacionales de datos. Así pues, entre otras cuestiones, estipulará las especialidades relacionadas con los procedimientos a través de los cuales las autoridades de protección de datos pueden aprobar modelos contractuales o normas corporativas vinculantes, determinar los supuestos de autorización de una determinada transferencia o, en su defecto, solicitar información previa.

A nuestro juicio, esta última norma podría haber aprovechado el articulado para introducir ciertas mejoras que hubieran dotado al derecho relativo a la protección de los datos de carácter personal de una mayor seguridad jurídica. Pese a ser conscientes de que el margen de maniobra que permite un Reglamento es de mínimos, entendemos que resultaba posible haber incorporado determinadas disposiciones que redundaran en maximizar las garantías disponibles para los titulares delbien jurídico protegido. *A priori*, la dificultad de negociación debería de ser más ágil en el contexto nacional español que en el ámbito comunitario, por no existir tanta diversidad de intereses contrapuestos.

1. Perspectiva histórica del derecho a la protección de datos en Europa

El derecho a la privacidad o a la protección de datos de carácter personal —ya sea en su concepción anglosajona o europea indistintamente—, se ha visto sometido a un incipiente desarrollo normativo durante la segunda mitad del siglo XX, postergándose dicha labor hasta la actualidad. Si se realiza un ejercicio de síntesis cronológica[20], cabe remontarse al año 1948 para constatar los primeros pronunciamientos plasmados en el artículo 12[21] de la Declaración Universal de los Derechos Humanos[22], en la que, siguiendo la estela apuntada años atrás por la doctrina norteamericana, se proclama el derecho de toda persona a no ser objeto de injerencias arbitrarias respecto de su vida privada, configurándose como parte integrante de los derechos fundamentales y libertades inherentes a la persona.

1.1. CEDH y documentos conexos

En consonancia con lo indicado, se siguieron sucediendo declaraciones casi simultáneas a la Declaración Universal de los Derechos Humanos con un contenido similar u análogo, como es el caso del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales (en adelante, CEDH), adoptado en Roma

[20] *Vid*., entre otros: PUENTE ESCOBAR, A., "Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal", en PIÑAR MAÑAS, J. L. (Dir.), *Protección de datos de carácter personal en Iberoamérica*, Valencia: Ed. Agencia Española de Protección de Datos / Tirant lo Blanch, 2006, pp. 37-67.

[21] *Vid*. Artículo 12 de la Declaración Universal de los Derechos Humanos: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

[22] Proclamada en París, por la Asamblea General de las Naciones Unidas, mediante su Resolución 217 A (III), de 10 de diciembre de 1948. Consultado el 28.06.2020 desde: https://www.unorg/es/universal-declaration-human-rights/.

el 4 de noviembre de 1950[23], así como también el Pacto Internacional de los Derechos Civiles y Políticos, de 19 de diciembre de 1966[24].

Respecto del primero de los documentos aludidos, conviene destacar su transcendencia fundamental, pues en el mismo queda reflejado que el Consejo de Europa se consagra como uno de los organismos internacionales que con mayor acierto toma conciencia de los peligros venideros que supone para la protección de los datos personales la utilización de nuevas formas de tratamiento de la información, que en muchos casos conllevaban aparejada la producción de movimientos de datos personales transnacionales, sin contar con un marco jurídico sólido y apropiado que les diera cabida, evitándose movimientos de datos hacia países que no aportaban un nivel de protección adecuado.

Como respuesta ante la incerteza existente, el CEDH tuvo a bien contemplar la protección de la vida privada frente a intromisiones por parte de terceros como uno de los derechos incluidos en su decálogo, que resultaba de obligado cumplimiento para todos aquellos Estados que hubieran decidido adherirse al mismo[25]. Entre las distintas

[23] *Vid*. Artículo 8, relativo al derecho al respeto a la vida privada y familiar: "1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia; 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás". El Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales, de 4 de noviembre de 1950, entró en vigor el 3 de septiembre de 1953. Posteriormente, fue ratificado por España en fecha 26 de septiembre de 1979, y publicado en el Boletín Oficial del Estado en fecha 10 de octubre de 1979. Consultado el 28.06.2020 desde: https://www.boe.es/buscar/doc.php?id=BOE-A-1999-10148. *Vid*., entre otros: CHUECA SANCHO, A. G., "Por una Europa de los derechos humanos: la adhesión de la Unión Europea al Convenio Europeo de Derechos Humanos", en *Unión Europea y Derechos fundamentales en perspectiva constitucional*, Madrid: Ed. Dykinson, 2004, pp. 37-58; BRAGE CAMEZANO, J., "Aproximación a una teoría general de los derechos fundamentales en el Convenio Europeo de Derechos Humanos", en *Revista Española de Derecho Constitucional*, nº 74 (2005); ARENAS RAMIRO, M., *El derecho fundamental a la protección de datos personales en Europa*, Valencia: Ed. Tirant lo Blanch, 2006.

[24] Se reproduce el tenor literal de los artículos relevantes por lo que a este análisis interesa: "[…] Artículo 17.1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación; […] Artículo 19.1. Nadie podrá ser molestado a causa de sus opiniones". El Pacto Internacional de los Derechos Civiles y Políticos, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 19 de diciembre de 1966, fue ratificado por España en fecha 28 de septiembre de 1976 y publicado en el Boletín Oficial del Estado en fecha 30 de abril de 1977. Consultado el 28.06.2020 desde: https://www.boe.es/buscar/doc.php?id=BOE-A-1977-10733.

[25] A este respecto, cabe indicar que, como consecuencia de los cambios sucedidos a finales de siglo XX, la adhesión al Consejo de Europa está supeditada a la membresía de los Estados Miembros al Convenio

cuestiones que se regulan, no se incluye ninguna mención específica relacionada con la protección de los datos personales. Dicha labor fue recayendo paulatinamente en el Tribunal Europeo de Derechos Humanos (en adelante, TEDH), que, a través de su dilatada jurisprudencia[26], ha venido regulando el respeto a la vida privada y familiar como un derecho personalísimo, inherente a la existencia del ser humano, pues le permite el libre desarrollo de su propia personalidad a medida que se relaciona con otros actores sociales.

Ante esta tesitura, el Consejo de Europa en 1968 se vio obligado a constituir una Comisión para analizar los efectos de las tecnologías de la información y la comunicación sobre los derechos fundamentales de las personas, cuyos trabajos culminaron con la adopción por parte de la Asamblea del Consejo de Europa de la Resolución 65/509/CE, relativa a "[l]os derechos humanos y los nuevos logros científicos y técnicos"[27]. El texto en cuestión, pese a no mencionar de manera expresa cuestiones relativas a protección de datos de carácter personal —como había sucedido con el CEDH—, abogaba por la necesidad de revisar los mecanismos existentes hasta esa fecha en lo relativo a la protección de los derechos fundamentales para adaptarlos a las nuevas realidades tecnológicas. Dicha premisa venía motivada por la circunstancia de que estos habían sido concebidos con antelación al desarrollo y avance tecnológico suscitado durante el último tercio del siglo XX como consecuencia del avance de la informática, que permitía el tratamiento y la transmisión de grandes volúmenes de datos personales entre distintos territorios.

Con la aprobación de esta Resolución, las actuaciones regulatorias para garantizar la protección a la vida privada de los ciudadanos se intensificaron, intentando paliar la inactividad de las instituciones comunitarias. Como muestra de ello, pueden citarse las

---

Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales. *Vid.*, entre otros: ARENAS RAMIRO, M., *El derecho fundamental…*, *op. cit.*, pp. 43-44.

[26] *Vid.*, entre otros: RUIZ MIGUEL, C., *El Derecho a la Protección de la Vida Privada en la Jurisprudencia del Tribunal Europeo de Derechos Humanos*, Ed: Thomson - Reuters (Civitas), 1994; ARENAS RAMIRO, M., *El derecho fundamental…*, *op. cit.*, pp. 54-86; ARZOZ SANTIESTEBAN, X., "Artículo 8: derecho al respeto de la vida privada y familiar", en *Convenio Europeo de Derechos Humanos. Comentario sistemático*, Navarra: Ed. Thomson-Reuters (Civitas), 2009.

[27] *Vid.*, entre otros: DAVARA RODRÍGUEZ, A., *La protección de datos en Europa*, Madrid: Ed. Grupo ASNEF-Equifax / Universidad Pontificia de Comillas, 1988; LUCAS MURILLO DE LA CUEVA, P., "La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad", en *El derecho a la autodeterminación informativa*, Madrid: Ed. Fundación Coloquio Jurídico Europeo, 1993, pp. 81-179.

distintas Resoluciones y Recomendaciones adoptadas por el Comité de Ministros del Consejo de Europa[28]. De entre las cuales aquí interesa destacar, por un lado, la Resolución nº 73/22, relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector privado[29] y la Resolución nº 74/29, relativa a la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector público[30]. Las mismas tenían como principal objetivo advertir a los Estados miembros de los riesgos que suponía el tratamiento de datos personales a gran escala, pues recomendaron que se adoptaran ciertas cautelas al respecto, como garantizar la idoneidad y exactitud de la información almacenada, facilitarla a los interesados cuando estos requiriesen de su conocimiento y salvaguardarla con medidas de seguridad lo suficientemente robustas que permitiesen reducir al máximo posible el riesgo de acceso no autorizado por parte de terceros no autorizados.

Y, por otro lado, la Resolución nº (76) 3, por la que se constituía un Comité de Expertos en materia de protección de datos, que alternativamente concluyó dos posibles vías alternativas simultáneas erigidas para proseguir con la regulación que se venía suscitando hasta la fecha, ya fuera articular un protocolo específico para complementar lo dispuesto en el artículo 8 del CEDH relativo al derecho al respeto de la vida privada y familiar que hemos podido analizar, o en su defecto, un convenio que permitiera desarrollar ampliamente el referido derecho, pero introduciendo particularidades que favoreciesen los movimientos transnacionales de datos de carácter personal a terceros Estados no integrantes del Espacio Económico Europeo (en adelante, EEE)[31], pero que sí

---

[28] *Vid.*, entre otras Recomendaciones del Consejo de Europa: la Recomendación nº (83) 10, de 23 de septiembre de 1983, relativa a la protección de datos personales utilizados con fines de investigación y estadísticos; la Recomendación nº (89) 2, de 18 de enero de 1989, relativa a la protección de datos personales utilizados con fines laborales; la Recomendación nº (95) 4, de 7 de febrero de 1995, relativa a la protección de datos personales en el sector de telecomunicaciones.

[29] Fue adoptada por el Comité de Ministros del Consejo de Europa, el 26 de septiembre de 1973, durante la reunión nº 224 de los Delegados de los Ministros. Consultado el 28.06.2020 desde: https://rm.coe.int/1680502830.

[30] Fue adoptada por el Comité de Ministros del Consejo de Europa, el 20 de septiembre de 1974, durante la reunión nº 236 de los Delegados de los Ministros. Consultado el 28.06.2020 desde: https://rm.coe.int/16804d1c51.

[31] El Acuerdo sobre el Espacio Económico Europeo entró en vigor en 1994 para ampliar las disposiciones de la Unión sobre el mercado interior a los países de la Asociación Europea de Libre Comercio (EFTA, por sus siglas en inglés). Noruega, Islandia y Liechtenstein son partes en el EEE, mientras que Suiza es miembro de la EFTA, pero no forma parte del EEE, dado que votó en contra del referéndum. Este Acuerdo amplía los miembros de la EFTA y los derechos y obligaciones del mercado interior de la UE. Consultado el

fueran miembros de la Organización para la Cooperación y el Desarrollo Económico (en adelante, OCDE)[32], concretamente, Estados Unidos, Canadá y Japón.

Tomando en consideración el contenido de las Resoluciones predecesoras nº 73/22 y nº 74/29, se optó por escoger la segunda de las alternativas mencionadas, cuya consecuencia práctica dio como resultado la adopción del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, al que en las siguientes líneas nos referiremos brevemente.

En consonancia con lo que se ha venido advirtiendo[33], cabe señalar que todas estas actuaciones legislativas servirán como punto de partida para la consagración gradual del derecho a la protección de los datos de carácter personal en Europa, pues se irán recogiendo paulatinamente aquellos principios esenciales sobre la materia que han permitido que la legislación existente en la actualidad siga siendo aún a día de hoy un marco de referencia y que, en todo caso, han propiciado que se instaure un único marco común vinculante a nivel comunitario en materia de protección de datos de carácter personal.

En este mismo lapso temporal, se cree conveniente avanzar que en los Estados Unidos de América, como tendremos ocasión de ver con mayor detalle posteriormente,

24.05.2020 desde: https://www.europarl.europa.eu/ factsheets/es/sheet/169/el-espacio-economico-europeo-suiza-y-el-norte.

[32] Podemos definir la Organización para la Cooperación y el Desarrollo Económico como un organismo internacional de carácter intergubernamental del que forman parte 37 países miembros. La OCDE tuvo su origen en el Convenio firmado en París el 14 de diciembre de 1960 para dar continuidad y consolidar el trabajo realizado por la antigua Organización Europea de Cooperación Económica (OECE) que se había constituido para canalizar la implementación del Plan Marshall. La OCDE sustituyó a esta en la tarea de impulsar la reconstrucción y el desarrollo en el continente tras la Segunda Guerra Mundial. Podemos afirmar que se ha constituido como un foro internacional que permite a los gobiernos de los Estados integrantes trabajar conjuntamente para hacer frente a los nuevos desafíos económicos, políticos y sociales frete a las nuevas realidades que se suceden a nivel nacional e internacional, compartiendo experiencias y analizando problemas comunes. Cabe destacar que la preocupación mostrada en protección de datos por este organismo viene motivada por la necesidad de articular un justo equilibrio entre los beneficios económicos derivados de la explotación transnacional de datos personales y el respeto a los derechos y libertades de los afectados. Consultado el 28.06.2020 desde: http://www.oecd.org/.

[33] *Vid*. ARENAS RAMIRO, M., *El derecho fundamental…*, *op. cit.*, p. 154; ESTADELLA YUSTE, O., *La protección de la intimidad frente a la transmisión internacional de datos personales*, Madrid: Ed. Tecnos, 1995, pp. 65-66.

se promulgó la denominada *Privacy Act*[34], que se erigiría como la primera ley federal que regulaba la recopilación, el mantenimiento, el uso y la difusión de la información personal almacenada por las distintas agencias federales norteamericanas sobre sus propios conciudadanos, así como cualesquiera terceros que pudieran resultar relevantes para los fines perseguidos, quedando dicha información registrada en los respectivos sistemas de los susodichos organismos públicos.

Éstos últimos, a su vez, siguiendo con el mandato establecido por la denominada *Freedom of Information Act*[35], quedan obligados con carácter general a facilitar a los ciudadanos la información y documentación que obre en sus respectivos archivos o expedientes, siempre que en todo caso medie el consentimiento previo del afectado o, en su defecto, la divulgación se pueda efectuar por existir una habilitación normativa en virtud de alguno de los supuestos de excepción previstos en la referida norma.

1.2. Directrices de la OCDE

Teniendo en cuenta lo anterior, a finales de la década de 1970 la mayoría de los países miembros de la OCDE disponían de alguna disposición normativa que pretendía salvaguardar el derecho a la protección de los datos personales[36], aspecto que ponía de manifiesto las preocupaciones que se estaban planteando sobre el uso que se efectuaba de la información personal. Dicha tesitura propició la creación de un grupo de expertos[37] que abordaría la cuestión, cuyos trabajos culminaron con la elaboración y publicación de las Directrices sobre protección de la privacidad y del libre flujo transfronterizo de datos personales[38]. Estas tenían como principal objetivo intentar armonizar las dispares

[34] Estados Unidos. *Privacy Act*, 5 U.S.C. § 552 a), *Section* 2. Promulgada del 31 de diciembre de 1974 por parte del Congreso de los Estados Unidos de América. Consultado el 28.06.2020 desde: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1279.

[35] Estados Unidos. *Freedom of Information Act (FOIA)*, 5 U.S.C. § 552. Promulgada el 4 de julio de 1966 por parte del Congreso de los Estados Unidos de América. Consultado el 28.06.2020 desde: https://www.govtrack.us/congress/bills/89/s1160.

[36] Concretamente, nos estamos refiriendo a Alemania, Luxemburgo, Francia, Suecia, Noruega, Austria, Dinamarca, Canadá y los Estados Unidos de América.

[37] Debían finalizar los trabajos, a más tardar, el 1 de julio de 1979, en estrecha cooperación con el Consejo de Europa, que posteriormente adoptará el Convenio (108).

[38] *Vid*. OCDE. "Directrices sobre protección de la privacidad y el libre flujo transfronterizo de datos personales", adoptadas el 23 de septiembre de 1980. El documento en cuestión se estructura a través de un Preámbulo y del propio contenido de las Directrices, compuesto a su vez por la Recomendación del Consejo de la OCDE, las Directrices propiamente dichas y un Memorando explicativo. En el primero de los

normativas que se estaban adoptando por parte de los Estados miembros, que en muchas ocasiones suponían un verdadero obstáculo para la realización de movimientos transnacionales de datos personales y, a su vez, una pérdida de competitividad económica.

Dichas Directrices se conciben como uno de los primeros instrumentos jurídicos internacionales que abogan por una regulación uniforme sobre los fundamentos existentes en lo relativo al derecho a la protección de los datos de carácter personal[39], pues su valor fue posteriormente reconocido por parte del Grupo de Trabajo del Artículo 29 (en adelante, GT29)[40], a través de su Documento de Trabajo nº 12, por considerar que el cumplimiento de los principios que se preceptuaban en el referido documento podían entenderse como el punto de partida para aquellos Estados que pretendiesen alcanzar la declaración de un "nivel de protección adecuado" sobre esta materia, cuya conceptualización tendremos oportunidad de ir discerniendo a lo largo de las siguientes líneas.

Respecto del apartado de definiciones que se recoge en las propias Directrices, Guerrero Picó lo ha señalado como "parco" pues las definiciones no recogían todas las casuísticas que se pueden producir cuando las organizaciones están efectuando movimientos transfronterizos de datos personales[41]. En muchas ocasiones, no solo disponemos de la figura del responsable del tratamiento únicamente, sino que también

---

apartados citados, se destaca la importancia de los flujos transnacionales de datos desde un punto de vista socioeconómico, instando a que los países eliminen cualquier tipo de obstáculo normativo que dificulte los movimientos, tal y como hemos tenido la oportunidad de ir advirtiendo. Esta exigencia se entiende como uno de los principales ejes que se articulan mediante este instrumento normativo. Consultado el 28.06.2020 desde: https://www.oecd.org/sti/ieconomy/15590267.pdf.

[39] *Vid*., entre otros: PUENTE ESCOBAR, A., "Breve descripción de…", en PIÑAR MAÑAS, J. L. (Dir.), *Protección de datos de…*, *op. cit*., pp. 50-51; OCDE, "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", en *OECD Digital Economy Papers*, Ed. OECD Publishing, nº 176 (2011). Consultado el 28.06.2020 desde: http://dx.doi.org/10.1787/5kgf09z90c31-en.

[40] Se define al Grupo de Trabajo del Artículo 29 como un organismo de consulta independiente creado bajo el amparo de la anterior Directiva 95/46/CE, formado por representantes de la totalidad de las autoridades de control nacionales de los Estados miembros, así como por el Supervisor Europeo de Protección de Datos y representantes de la propia Comisión Europea, que se encarga principalmente del estudio y análisis relativos a la aplicabilidad de la legislación europea en materia de protección de datos de carácter personal. Consultado el 15.08.2017 desde: http://www.agpd.es/portalwebAGPD/internacional/Europa/grupo_29_europeo/index-ides-idphp.php.

[41] *Cfr*. GUERRERO PICÓ, M. C., *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Navarra: Ed. Thomson-Reuters (Civitas), 2006, p. 50.

existen terceras partes implicadas que participan en la gestión del dato durante su ciclo de vida.

Adicionalmente, puede afirmarse que el contenido de las propias Directrices se define, en términos generales, como el establecimiento de unas reglas básicas que debían permitir a los Estados fijar los límites de las respectivas políticas legislativas internas que decidiesen emprender, en aras de garantizar la consecución de un mismo nivel de protección lo suficientemente robusto en materia de protección de datos personales. Máxime, si se tiene en cuenta que las mismas habían sido articuladas con una estructura basada en conceptos, principios, derechos y obligaciones que facilitaban el respectivo desarrollo legislativo[42].

De todo el contenido esbozado con anterioridad, interesa destacar en este punto lo relativo a los principios de aplicación internacional que debían regir los movimientos de datos personales entre los distintos Estados integrantes de la OCDE, pues se partía de una premisa básica centrada en que los mismos debían adoptar todas aquellas medidas adecuadas orientadas a garantizar que las transferencias internacionales de datos personales, incluyéndose el tránsito a través de otro país miembro, fueran ininterrumpidas y seguras[43].

De esta manera, se imponía la necesidad de articular un libre flujo internacional de datos personales sin la imposición de restricciones ilegítimas, las cuales únicamente serían aplicables cuando el contenido de las Directrices no se hubiera respetado en su integridad o si la reexportación de los datos tuviera como objetivo transgredir la legislación nacional sobre la materia —transferencia ulterior—. Dicha concepción sentaría las bases de lo que se iría convirtiendo gradualmente en el fundamento básico de la materia objeto de estudio, inicialmente acogida por parte del Convenio 108, así como posteriormente por las sucesivas normas que se verían influenciadas a este respecto.

Con carácter adicional, los numerales 17 y 18 de las Directrices articulaban la posibilidad de que los Estados miembros pudieran plantear restricciones ante los movimientos transfronterizos de datos personales que incluyesen tipologías de datos sobre los que resultasen exigibles normativas específicas de carácter nacional —

[42] *Vid*., entre otros: PUENTE ESCOBAR, A., "Breve descripción de…", en PIÑAR MAÑAS, J. L. (Dir.), *Protección de datos de*…, *op. cit.*, pp. 52-53.

[43] *Vid*. OCDE. "Directrices sobre protección…", *op. cit.*, numeral16.

categorías especiales—, siempre que el país de destino no ofreciese un nivel de seguridad jurídica razonable ("nivel de protección adecuado"). Estas excepciones debían ser proporcionales al fin perseguido y, en cualquier caso, debía evitarse en la medida de lo posible la utilización de cláusulas arbitrarias basadas en la soberanía nacional, la seguridad nacional o en un interés público prevaleciente que pudiesen comportar la producción de situaciones de conflicto[44].

Al respecto, como apunta Recio Gayo, "[e]s importante tener en cuenta que el numeral 17 utilizaba el término "protección equivalente" —según la traducción del original, en inglés, "*equivalent protection*"—, término que puede considerarse como similar al de "nivel adecuado". No obstante, ambos términos, aunque aquí se usan indistintamente, podrían tener un significado diferente. En efecto, mientras que la equivalencia implica la evaluación de un nivel de similitud objetiva entre dos marcos considerando los instrumentos utilizados y los resultados de la regulación, la adecuación puede ser más flexible ya que implica estar de acuerdo con un resultado común y permite el uso de diferentes instrumentos para alcanzar dicho resultado"[45].

En definitiva, como apuntábamos, las Directrices fueron revisadas y actualizadas en 2013 para responder a los diversos cambios que se habían producido durante los últimos años a nivel tecnológico y social, pues las casuísticas que se amparaban en el momento de su creación se han visto superadas en la actualidad por nuevos escenarios. Las nuevas realidades precisan de nuevos mecanismos en materia de transferencias internacionales de datos que faciliten y agilicen el intercambio de datos personales entre los distintos países miembros de la OCDE.

1.3. Convenio 108

Todo el movimiento legislativo esbozado hasta el momento culmina en Europa con la elaboración y posterior aprobación del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (en adelante,

[44] Este precepto se ha mantenido en la actualización del documento fechada en 2013. Consultado el 28.06.2020 desde: http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

[45] *Cfr.* RECIO GAYO, M., "Nivel adecuado para transferencias internacionales de datos", en *Revista de la Facultad de Derecho de la Pontificia Universidad Católica del Perú*, nº 83 (2019), p. 5. Consultado el 28.06.2020 desde: https://doi.org/10.18800.

Convenio 108)[46]. El mismo fue elaborado en Estrasburgo, el 28 de enero de 1981, entendiéndose por parte de la doctrina como el primer instrumento internacional jurídicamente vinculante sobre la materia[47]. Su eficacia tiene una doble perspectiva, dado que aparte de hacer efectivamente aplicables los principios vigentes sobre protección de datos de carácter personal, se preceptúa como una herramienta obligatoria para los Estados firmantes[48], determinando la obligación de estos de velar por el cumplimiento de las disposiciones que intentan reforzar el respeto al derecho a la vida privada y familiar.

Dicho lo anterior, una de las consideraciones que merecen ser puestas de relieve del Convenio 108, y que en su momento fue ampliamente debatida por parte de la doctrina[49], reside en que su contenido no era susceptible de aplicación directa sobre los respectivos ordenamientos jurídicos nacionales[50]. Este aspecto resulta un tanto paradójico puesto que, si su intención era precisamente favorecer la homogeneización y armonización normativa de las diferentes legislaciones nacionales existentes sobre la materia en el contexto comunitario europeo, podía considerarse paradigmático el mandato

[46] El día 28 de enero de 1982, el Plenipotenciario de España, nombrado en buena y debida forma al efecto, firmó en Estrasburgo el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981 y ratificado posteriormente el 27 de enero de 1984. Consultado el 28.06.2020 desde: https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447.

[47] *Vid.*, entre otros: HEREDERO HIGUERAS, M., "Ante la ratificación del Convenio de protección de datos del Consejo de Europa", en *Documentación Administrativa*, nº 199 (1983), pp. 753-764; BRETAL VÁZQUEZ, M., "Convenio para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal, de 28 de enero", en *B.L.E.*, nº 4 (1982), pp. 50-76; RIPOLL CARULLA, S., "El Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal: Balance a los siete años de su apertura a la firma", en *Actas del Congreso sobre Derecho Informático*, Zaragoza: Ed. Facultad de Derecho, 1989, pp. 395-413.

[48] Actualmente, el Convenio (108) ha sido ratificado por 55 Estados y, como consecuencia de su modificación operada en el año 1999 en su artículo 23, se ha permitido la adhesión y ratificación de Estados que no forman parte del Consejo de Europa, como es el caso de la República de Mauricio, Senegal, Méjico, Argentina o, en última instancia, Marruecos, en junio de 2019. Consultado el 28.06.2020 desde: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures.

[49] *Vid*. DAVARA RODRÍGUEZ, M. A., *Derecho Informático*, Pamplona: Ed. Aranzadi, 1993, p. 64.; GARZÓN CLARIANA G., "La protección de los datos personales y la función normativa del Consejo de Europa", en *Revista de Instituciones Europeas*, vol. 8, nº 1 (enero-abril de 1981), p. 18; HEREDERO HIGUERAS M., "Ante la ratificación del Convenio de…", *op. cit.*, p. 754; PÉREZ LUÑO, A. E., *Los derechos humanos en la sociedad tecnológica*, Madrid: Ed. Universitas, 2012, pp. 175-180.

[50] *Vid.*, entre otros: GARZÓN CLARIANA, C., "La protección de los datos …", en *Revista de Instituciones Europeas*, *op. cit.*, pp. 9-25; VILLAVERDE MENÉNDEZ, I., "Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo a propósito de la STC 254/1993", en *Revista Española de Derecho Constitucional*, nº 41 (1994), pp. 187-202.

consagrado en su artículo 4.1[51], ya que parecía desvirtuar el objetivo inicialmente perseguido por la norma.

El debate generado sobre la falta de eficacia directa del Convenio 108, motivado por el hecho de que los Estados que lo ratificaban no efectuaban ningún tipo de desarrollo legislativo en sus respectivos ordenamientos jurídicos internos para su adecuación, propició que, en España, la Sala Primera del Tribunal Supremo (en adelante, TS) se pronunciara en términos similares a los pronunciamientos que se habían formulado con anterioridad por parte de la Audiencia Territorial de Pamplona. En su Sentencia de 30 de abril de 1990, el Tribunal Supremo confirma que el Convenio precisa de una actuación de transposición legislativa para que pueda desplegar sus efectos en el ordenamiento jurídico de cada parte firmante, de conformidad con el mandato establecido en el artículo 94.1, letra e), de la CE[52]. Actividad que, hasta dicha fecha, no se había efectuado.

Tres años más tarde, el 20 de julio de 1993, el Tribunal Constitucional (en adelante, "TC") vendría a otorgar el amparo solicitado por el recurrente, anulando los pronunciamientos que habían denegado su petición de amparo y declarando el derecho que el mismo ostentaba a que las autoridades correspondientes atendieran la petición de información que había solicitado[53]. El Alto Tribunal refrendaría el carácter interpretativo

---

[51] Se reproduce el tenor literal del artículo 4.1 referenciado por lo que a efectos de este análisis interesa: "[c]ada Parte tomará, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos enunciados en el presente capítulo".

[52] *Vid*. CONSEJO DE EUROPA. "Protección de Datos. Convenio del Consejo de Europa de 1981", en *Documentación Informática: serie amarilla / Tratados internacionales*, nº 3 (1983), Madrid: Ed. Presidencia del Gobierno. Servicio Central de Publicaciones. Servicio Central de informática, p. 31.

[53] El Tribunal Constitucional se pronunciaría mediante su Sentencia 254/1993, de 20 de julio de 1993 (Recurso de amparo 1827/1990), contra la presunta denegación por parte del Gobernador Civil de Guipúzcoa y del Ministro del Interior de la solicitud de información de los datos de carácter personal existentes en ficheros automatizados de la Administración del Estado, confirmada en la vía contencioso-administrativa, por una posible vulneración de los artículos 18.1 y 18.4 de la Constitución española. Consultado el 28.06.2020 desde: https://www.boe.es/diario_boe/txt.php?id=BOE-T-1993-21425. *Vid*., entre otros: GONZÁLEZ CAMPOS, J., SÁNCHEZ RODRIGUEZ, L. y ANDRÉS SÁENZ DE SANTA MARÍA, M. P., *Curso de Derecho Internacional Público*, Madrid: Ed. Thomson-Civitas, 2003, pp. 280-287. Como apunta González Murúa, "[s]in embargo, esta argumentación utilizada por el TC es criticada por el Presidente del Tribunal don Miguel Rodríguez-Piñero y Bravo-Ferrer en su voto particular formulado en este recurso de amparo. Dicho magistrado discrepa del criterio mayoritario, ya que en su opinión, en este caso el Convenio no se ha utilizado meramente, frente a lo que se dice " corno una fuente interpretativa que contribuye a la mejor interpretación del contenido de los derechos..., sino corno elemento de integración ante la demora en el desarrollo legislativo del precepto constitucional, para cuyo desarrollo desde luego habría de servir de pauta, aunque no canon autónomo de validez, el contenido de dicho Convenio". *Cfr*. GONZÁLEZ MURÚA, A. R., "Comentario a la S.T.C. 254/1993, de 20 de julio, algunas consideraciones en torno al artículo 18.4 de la Constitución y la protección de los datos personales", en *Informática y*

del Convenio 108: "[…] Los textos internacionales ratificados por España pueden desplegar ciertos efectos en relación con los derechos fundamentales, en cuanto pueden servir para configurar el sentido y alcance de los derechos recogidos en la Constitución, como hemos mantenido, en virtud del art. 10.2 de la CE, desde nuestra STC 38/1981, fundamentos jurídicos 3º y 4º. Es desde esta segunda perspectiva desde la que hay que examinar la presente demanda de amparo"[54].

Como señala González Murúa, "[e]n opinión del Tribunal, tanto los problemas a los que se tuvo que enfrentar la elaboración y la ratificación de este Tratado como la experiencia de los países del Consejo de Europa que se condensa en su articulado conducen a la conclusión de que la protección de la intimidad debe incluir la facultad de que los ciudadanos puedan conocer la existencia y los rasgos de aquellos ficheros automatizados de las Administraciones Públicas donde se conservan datos de carácter personal que les conciernen, así como cuáles son esos datos personales que obran en poder de las autoridades"[55].

Sin perjuicio de lo anterior, habría que mencionar también, que el Convenio 108 pretendía facilitar los flujos transfronterizos de datos de carácter personal por la importancia económica que cada vez más revestían. Su relevancia ya aparece constatada en el propio Preámbulo de la norma, así como en las sucesivas interpretaciones que se iban produciendo por parte de los organismos comunitarios con competencias sobre la materia, como resulta, entre otros, de los pronunciamientos efectuados por parte del GT29 y el TEDH[56].

Asimismo, en similares términos a los establecidos por el numeral 18 de las Directrices de la OCDE, el Convenio a través de su artículo 12 establecía las reglas

---

derecho: Revista iberoamericana de derecho informático, nº 6-7 (1994), p. 213. Consultado el 28.06.2020 desde: https://dialnet.unirioja.es/descarga/articulo/248368.pdf

[54] *Vid*. Fundamento Jurídico Sexto de la Sentencia del TC 254/1993, de 20 de julio de 1993 (Recurso de amparo 1827/1990).

[55] *Cfr*. GONZÁLEZ MURÚA, A. R., "Comentario a la S.T.C. 254/1993…", *op. cit.*, p. 212.

[56] Sentencias del TEDH: asunto Bernh Larsen Holding AS y otros contra Noruega, nº 24117/08, de 14 de marzo de 2013; asunto Rotaru contra Rumanía [GS], nº 28341/95, de 4 de mayo de 2000; asunto Taylor-Sabori contra Reino Unido, nº 47114/99, de 22 de octubre de 2002; asunto Peck contra el Reino Unido, nº 44647/98, de 28 de enero 2003; asunto Khelili contra Suiza, nº 16188/07, de 18 de octubre de 2011; asunto Leander contra Suecia, nº 9248/81, de 26 de marzo de 1987; asunto Haralambie contra Rumanía, nº 21737/03, de 27 de octubre de 2009; asunto K.H. y otros contra Eslovaquia, nº 32881/04, de 6 de noviembre 2009.

generales que resultaban de aplicación sobre las transferencias internacionales de datos, las cuales únicamente podían llevarse a cabo entre aquellos Estados que hubieran suscrito el Convenio. No podía alegarse objeción alguna a dicho movimiento[57], salvo en aquellas excepciones específicamente tasadas[58], ya fuese motivado por la tipología de datos personales sensibles objeto de tratamiento que pudieran precisar de una regulación específica, lo que el propio texto denominaba como "categorías particulares de datos"[59], o bien cuando existiesen sospechas razonablemente fundadas de que se pretendía articular un movimiento de datos sin respetar las disposiciones reflejadas en la norma referenciada.

En particular, este punto del Convenio 108 también fue, al igual que lo sucedido con su fuerza ejecutiva, una de las cuestiones más controvertidas entre los países que formaban parte de este, pues no introdujo una regulación lo suficientemente detallada que permitiera satisfacer las necesidades prácticas que se demandaban hasta la fecha en materia de transferencias internacionales de datos. En efecto, se omitió la introducción de una regulación que habilitara los movimientos transfronterizos de datos personales entre

[57] Se reproduce el tenor literal de los apartados primero y segundo del artículo 12 referenciado del Convenio (108) para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, en su versión inicial elaborada en Estrasburgo el 28 de enero de 1981, relativo a los flujos transfronterizos de datos de carácter personal y al derecho interno: "1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento; 2. Una Parte no podrá, con el único fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte". *Vid*., entre otros: PAVÓN PÉREZ, J. A., "La protección de datos personales en el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales", en *Anuario de la Facultad de Derecho (Universidad de Extremadura)*, nº 19-20 (2002), pp. 235-252; GARZÓN CLARIANA, C., "La protección de los datos personales…", *op. cit.*, pp. 9-25.

[58] *Vid*. Artículo 12, apartado tercero, del Convenio (108) para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, en su versión inicial elaborada en Estrasburgo el 28 de enero de 1981.

[59] *Vid*. Artículo 6 del Convenio (108) para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, en su versión inicial elaborada en Estrasburgo el 28 de enero de 1981. Término que posteriormente será modificado para denominarse "categorías especiales de datos", con la intención de alinearse con el redactado contenido en el artículo 8 sobre "categorías especiales de datos" de 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 o, más recientemente, al establecido en el artículo 9 sobre "categorías especiales de datos personales" 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 Directiva 95/46/CE (Reglamento general de protección de datos).

los distintos Estados firmantes del Convenio respecto a terceros Estados u organizaciones internacionales no integrantes del mismo.

Avanzando en nuestro razonamiento, conviene mencionar que la deficiente técnica regulatoria incurrida en lo relativo a los flujos de datos transnacionales tuvo que ser enmendada posteriormente en el año 2001, mediante la elaboración de un Protocolo Adicional[60]. Este pivotaba sobre la declaración del país de destino como de un "nivel adecuado de protección" —aunque posteriormente la nomenclatura sería reformulada nuevamente como tendremos oportunidad de analizar—, no permitiéndose los movimientos de datos transfronterizos hacia un tercer Estado u organización internacional que no formase parte del Convenio, sino se constataba de manera efectiva la condición del nivel de protección adecuado.

En este sentido, se reconocía un principio general que permitía a los Estados que formaban parte del Convenio 108 la posibilidad de habilitar transferencias internacionales de datos hacia un tercer Estado u organización internacional, siempre que la legislación interna del país de destino lo autorizase como consecuencia de la sucesión de intereses específicos de la persona interesada, o bien existiera la prevalencia de un interés legítimo o público imperante[61], como en este último caso lo podría ser, por ejemplo, la realización de un movimiento de datos por razones de índole sanitaria[62].

Otro rasgo esencial radica en que se atribuía la facultad a los Estados firmantes del Convenio 108 de articular el movimiento transnacional de datos personales a Estados u organizaciones que no gozasen de un nivel de protección adecuado, siempre que se acreditasen una serie de garantías. Concretamente, la aplicación de cláusulas contractuales que fueran lo suficientemente robustas, pues debía tenerse en cuenta que las

[60] El día 24 de septiembre de 2009, el Plenipotenciario de España, nombrado en buena y debida forma al efecto, firmó en Estrasburgo (Francia) el Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las Autoridades de control y a los flujos transfronterizos de datos, hecho en Estrasburgo el 8 de noviembre de 2001 y ratificado posteriormente el 8 de noviembre de 2001. Consultado el 28.06.2020 desde: https://www.boe.es/buscar/doc.php?id=BOE-A-2010-14380.

[61] *Vid*. Artículo 2.2, letra a), del Protocolo Adicional al Convenio (108) para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las Autoridades de control y a los flujos transfronterizos de datos, en su versión inicial elaborada en Estrasburgo el 8 de noviembre de 2001.

[62] Como se ha podido constatar de lo sucedido a tenor de la pandemia derivada del coronavirus SARS-CoV-2.

mismas tenían que ser avaladas con carácter previo por parte de la autoridad de control nacional competente en materia de protección de datos de carácter personal[63].

Además, se debe agregar que el Preámbulo del Protocolo Adicional también determinaba la importancia de las autoridades de control nacionales en materia de protección de datos personales. Por este mismo motivo, abogaba por la existencia de estas en cada uno de los Estados adheridos al marco del Convenio 108, en aras de reforzar la protección de los derechos y libertades de los interesados. A su vez, con una actitud proactiva, instaba a que las referidas autoridades de control creadas bajo el ámbito de aplicación del Protocolo[64] cooperasen entre ellas para alcanzar un mayor grado de armonización, que a su vez redundase en una mejora de la seguridad jurídica sobre el marco legislativo comunitario previsto sobre esta materia.

Aparte de regular lo que hemos visto hasta el momento, el Convenio 108 ha sido reformado recientemente para intentar adaptarse a las nuevas realidades tecnológicas existentes en lo relativo al tratamiento de datos personales mediante un Protocolo de Enmienda[65]. Las exigencias de la globalización han obligado a que los movimientos de datos transnacionales se conviertan en operaciones rutinarias para multitud de entidades del sector público y privado. Y que, en consecuencia, los retos a afrontar augmenten, motivados en gran parte por la cada vez más difícil tesitura existente relativa a intentar

[63] *Vid*. Artículo 2.2, letra b), del Protocolo Adicional al Convenio (108) para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las Autoridades de control y a los flujos transfronterizos de datos, en su versión inicial elaborada en Estrasburgo el 8 de noviembre de 2001.

[64] En el ámbito español, disponemos de una autoridad de protección de datos nacional que actúa en el marco de todo el territorio nacional, esto es, la Agencia Española de Protección de Datos. Adicionalmente, también existen autoridades de control autonómicas, como lo son la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía. En cualquier caso, para más información sobre las funciones inicialmente desempeñadas por la Autoridad Española de Protección de Datos, *vid*., entre otros: LÓPEZ RAMÓN, L., "La Agencia de Protección de Datos como Administración Independiente en el Derecho Español y Comunitario Europeo", en *Jornadas sobre el Derecho Español de la Protección de Datos Personales*, Madrid: Ed. Agencia de Protección de Datos, 1996, pp. 252-254; LUCAS MURILLO DE LA CUEVA, P., "Las Funciones de la Agencia de Protección de Datos", en *Jornadas sobre el Derecho Español de la Protección de Datos Personales*, Madrid: Ed. Agencia de Protección de Datos, 1996, pp. 263-267; MARROIG POL, L., "La Agencia de Protección de Datos. Reflexiones sobre la Administración de Datos de Carácter Personal", en *X Años de Encuentros sobre Informática y Derecho*, nº 1996-1997 (1997), Ed. Aranzadi, pp. 173-178.

[65] Modificado mediante el Protocolo de enmienda aprobado por el Comité de Ministros del Consejo de Europa, el 18 de mayo de 2018, durante la correspondiente reunión de los Delegados de los Ministros. Consultado el 28.06.2020 desde: https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8. La ratificación del Protocolo de Enmienda por España se produjo el 28 de enero de 2021. Consultado el 02.04.2021 desde: http://www.exteriores.gob.es/RepresentacionesPermanentes/ConsejodeEuropa/es/Noticias/Paginas/Articulos/20210203_NOT1.aspx.

salvaguardar la intimidad y la vida privada de los ciudadanos como sujetos especialmente protegidos.

Con la intención de intentar afrontar con éxito estos nuevos desafíos, la modificación del Convenio 108, atendiendo a su naturaleza de instrumento de derecho internacional, ha supuesto un incremento de las salvaguardas jurídicas para ayudar a velar por el respeto de los derechos y las libertades de los afectados en línea con las nuevas exigencias regulatorias[66]. Como señala la propia Comisión Europea, la norma tendrá un ámbito de aplicación uniforme para todas las partes suscribientes, sin la posibilidad de excluir completamente de su ámbito de aplicación determinados sectores o actividades, como sucede con el texto actual, entre otros, en el ámbito de la seguridad nacional. De este modo, abarcará todos los tipos de tratamiento de datos bajo la jurisdicción de las Partes, tanto en el sector público como en el privado[67].

Entre las cuestiones introducidas con mayor relevancia, podemos mencionar que: (i) se alinean las bases jurídicas que legitiman los tratamientos de datos de carácter personal con las dispuestas en las respectivas legislaciones aplicables sobre la materia; (ii) se determina la obligación de notificar a las autoridades de control en caso de que exista una brecha de seguridad; (iii) se amplían las coberturas del catálogo de derechos previsto para los afectados respecto de su redactado inicial; (iv) se introducen nuevas categorías especiales de datos como la información genética, datos biométricos o cuestiones relativas a la pertenencia a una determinada etnia; (v) se refuerza el papel de las autoridades de control nacionales con competencias sobre la materia; y (vi) se manifiesta la necesidad imperiosa de que los sujetos obligados aboguen por la implementación efectiva del principio de responsabilidad proactiva[68].

---

[66] Derivadas de la aplicación efectiva 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 Directiva 95/46/CE (Reglamento general de protección de datos).

[67] *Vid*. Propuesta de Decisión del Consejo por la que se autoriza a los Estados miembros a ratificar, en interés de la Unión Europea, el Protocolo que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STCE nº 108) (COM [2018] 451 final). Consultado el 02.04.2021 desde: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018PC0451&from=PL.

[68] El principio de responsabilidad proactiva aparece recogido en el artículo 5, apartado segundo del RGPD, como consecuencia de la importación de su figura del derecho anglosajón, preceptuándose como una de las obligaciones clave que tienen que aplicar los responsables del tratamiento para dar cumplimiento a las

En última instancia, en lo relativo a las transferencias internacionales de datos personales también se experimentan cambios significativos, pues la regulación de las mismas se traslada al artículo 14 del Convenio, que intenta mantener el espíritu de su redactado inicial vinculado al mantenimiento del principio general de libertad de movimientos transnacionales de datos personales entre los distintos Estados suscribientes al mismo[69], a excepción de que exista un riesgo real y grave de que el movimiento de datos pueda suponer un incumplimiento de las normas contenidas en el Convenio, o bien existan normas armonizadas de protección compartidas por los Estados adheridos pertenecientes a una organización internacional regional que determinen lo contrario[70].

Asimismo, también se mantiene la aplicación del concepto de "nivel adecuado de protección" que anteriormente habíamos apuntado, pero el mismo se amplía y matiza desde una doble perspectiva por no gozar su redacción inicial de suficiente claridad[71]. Por un lado, se refuerza permitiendo a los Estados adheridos al Convenio 108 garantizarlo mediante la acreditación de una de las dos condiciones previstas, esto es, que el ordenamiento jurídico del país de destino, o las normas de la organización internacional que no disponga de un nivel de protección adecuado, adopten actuaciones al respecto que incluso permitan la incorporación de tratados o acuerdos internacionales, o bien que se implementen garantías normalizadas previstas en instrumentos jurídicamente vinculantes con esos Estados u organizaciones que no posean un nivel de protección adecuado[72].

---

nuevas exigencias normativas aplicables en materia de protección de datos. En la práctica, este principio redunda en la necesidad de que las organizaciones velen por dejar evidencia rastreable de que cumplen con la legislación aplicable sobre la materia, mediante la realización de autoanálisis y recurrentes evalua ciones de riesgo sobre los distintos tratamientos de datos personales que lleven a cabo. *Vid*.: PIÑAR MAÑAS, J. L., "Introducción Hacia un nuevo modelo europeo de Protección de Datos", en PIÑAR MAÑAS, J. L. (Dir.)., *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad*, Madrid: Ed. Reus, 2016, p. 17.

[69] *Vid*. Artículo 14, apartado primero, del Protocolo de enmienda del Convenio (108) del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, en su versión inicial elaborada en Estrasburgo, el 10 de octubre de 2018.

[70] *Vid*. AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA / CONSEJO DE EUROPA, *Handbook on European data protection law*, Luxemburgo, 2018.

[71] *Vid*. CONSEJO DE EUROPA., "Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", en *Council of Europe Treaty Series*, Nº 223 (2018). Consultado el 28.06.2020 desde: https://rm.coe.int/16808ac91a.

[72] *Vid*. Artículo 14, apartado tercero, del Protocolo de enmienda del Convenio (108) del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, en su versión inicial elaborada en Estrasburgo, el 10 de octubre de 2018.

Y, por otro lado, cada uno de los Estados suscribientes tiene la potestad unilateral de llevar a término el movimiento si se cumplen una serie de condicionantes con carácter previo[73], esto es: (i) se disponga del consentimiento libre e informado del afectado; (ii) prevalezcan los intereses vitales del interesado; (iii) existan intereses legítimos superiores o públicos que avalen el movimiento; o (iv) se trate de una medida que supere el juicio de proporcionalidad.

En cualquier caso, y como tendremos ocasión de advertir en las próximas líneas, el contenido del Convenio, tras su aprobación en relación con la materia objeto de estudio, además de fomentar la creación de un marco común y uniforme en materia de protección de datos, ha resultado constituirse como uno de los fundamentos de las venideras regulaciones que se han ido sucediendo hasta la actualidad. Una muestra de ello se sucedería con 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; y, posteriormente, con 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 y por el que se deroga la Directiva 95/46/CE (en adelante, Reglamento General de Protección de Datos o RGPD, indistintamente).

Sin perjuicio de ello, cabe tener presente que aunque el Convenio ejerce una influencia directa sobre dichos textos regulatorios, los mismos disponen de un enfoque relativamente diferente. Los organismos reguladores europeos han considerado preciso que para que un país pueda ser considerado con un nivel de protección adecuado, no resulta suficiente con que el mismo sea parte del Convenio 108, sino que además debe de disponer de una declaración de adecuación realizada por parte de la Comisión Europea o, en su defecto, de alguna otra de las garantías suficientes que pueda resultar de aplicación.

[73] *Ibidem.*

1.4. Últimos movimientos doctrinales. Especial referencia al caso alemán

La doctrina[74] ha entendido conveniente considerar que la última generación normativa en materia de protección de datos de carácter personal marca su inicio con los primeros pronunciamientos abordados por la jurisprudencia alemana. A diferencia de la corriente dimanante de Estados Unidos, ésta buscaba una interpretación del derecho fundamental a la protección de datos de carácter personal vinculada al libre desarrollo de la personalidad y el respeto a la dignidad humana. Dicho movimiento jurisprudencial alemán pretendía alejarse de la discusión que se había producido en distintos países del entorno europeo, que abogaban por una regulación vinculada a la salvaguarda de la intimidad y el respeto a la vida privada[75].

En este sentido, la Sentencia del Tribunal Constitucional Federal de Alemania, de 15 de septiembre de 1983[76], a través de la cual se declaraba la inconstitucionalidad de parte del contenido establecido en la Ley del Censo de Población de 1983[77], supone el inicio de la configuración del derecho a la autodeterminación informativa. La interpretación que en ella se contiene tuvo una influencia directa en los textos constitucionales europeos que posteriormente se desarrollarían[78], permitiendo que paulatinamente se consagrara como un auténtico derecho fundamental autónomo y con contenido independiente. Dicha influencia se vería reflejada posteriormente, tanto en la Carta de Derechos Fundamentales de la Unión Europea como en la jurisprudencia del Tribunal Europeo de Derechos Humanos.

---

[74] *Vid*., entre otros: REBOLLO DELGADO, L. y SERRANO PÉREZ, M. M., *Introducción a la protección de datos*, Madrid: Ed. Dykinson, 2008, pp. 32-33; MARTÍNEZ MARTÍNEZ, R., "El derecho fundamental a la protección de datos: perspectivas", en *Revista de Internet, Derecho y Política*, nº 5 (2007), pp. 48-50.

[75] *Vid*. SERRANO PÉREZ, M. M., *El derecho fundamental…*, *op. cit.*, p. 34.

[76] Para consultar una versión traducida al castellano de la Sentencia en cuestión, *vid*. DARANAS, M., *Boletín de Jurisprudencia Constitucional (BJC)*, nº 33 (1984), pp. 126-170.

[77] La Ley sobre el recuento de la población, de las profesiones, de las viviendas y de los centros de trabajo, comúnmente denominada como "Ley del Censo de Población de 1983", fue aprobada por el Parlamento Federal (en alemán, "*Bundestag*") el 4 de marzo de 1982 y, posteriormente, publicada en el Boletín Oficial en fecha 31 de marzo de 1982, pp. 369-370.

[78] Para una visión crítica, *Vid*., entre otros: HEREDERO HIGUERAS, M., "La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del Censo de la Población de 1983", en *Documentación Administrativa*, nº 198 (1983), pp. 139-158; MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica a la autodeterminación informativa*, Madrid: Ed. Civitas, 2004, pp. 237-244; PIÑAR MAÑAS, J. L., "Protección de datos: origen, situación actual y retos de futuro", en *El derecho a la autodeterminación informativa*, Madrid: Ed. Fundación Coloquio Jurídico Europeo, 2009, pp. 98-105.

La referida Ley en cuestión determinaba la obligación de los ciudadanos de responder una serie de preguntas sobre su vida íntima y personal a las administraciones públicas, con la intención de que estas pudieran utilizar dichos datos personales obtenidos para distintas finalidades sin apenas restricciones, aspecto que determinó que en base a la Ley Fundamental de Bonn[79] se declarase su inconstitucionalidad. Según el Alto Tribunal alemán, se apreció una vulneración del principio de proporcionalidad que debía regir toda recogida de datos personales sobre los afectados —en este caso, los administrados—, pues no se entendió la necesidad de articular un registro que permitiría la concentración de grandes volúmenes de información sobre los ciudadanos, sin existir un propósito claramente definido[80].

A este respecto, el Tribunal manifestó que: "[...] Los límites a ese derecho se admiten solo con base en la prevalencia del interés general, pero requieren de un fundamento legal y constitucional acorde con el mandato del Estado que exige claridad normativa. Para su reglamentación, el legislador debe tener en cuenta además el principio de proporcionalidad. Las reglas para el sondeo consagradas en el artículo 9, párrafo 1, de la Ley de Censos de 1983 (dentro de las cuales se encuentra la comparación de los registros de residentes) contravienen el derecho general de la personalidad"[81].

En este mismo sentido, se debe afirmar, como indica Pérez Luño, que para el juzgador alemán la sensibilidad de las informaciones no depende tanto de su conexión inmediata con aspectos que afecten a la intimidad como de la posibilidad de que puedan utilizarse en procesos que afecten al ejercicio de los derechos fundamentales y, en concreto, al libre desarrollo de la personalidad[82].

---

[79] Se refiere a la Constitución de la República Federal de Alemania, aprobada el 8 de mayo de 1949 por el Consejo Parlamentario y firmada el 23 de mayo de 1949 en la ciudad de Bonn. Consultado el 28.06.2020 desde: https://www.btg-bestellservice.de/pdf/80206000.pdf.

[80] *Vid*., entre otros: LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, Madrid: Ed. Tecnos, 1990, p. 26; RUIZ MIGUEL, C., "El derecho a la intimidad informática en el ordenamiento español", *Revista general de Derecho*, nº 607 (1995), pp. 3207-3233; LUCAS MURILLO DE LA CUEVA, P., "La construcción del derecho a la autodeterminación informativa", en *Revista de estudios políticos*, nº 104 (1999), pp. 35-60.

[81] *Vid*. SCHWABE, J., "Jurisprudencia del Tribunal Constitucional Federal Alemán Extractos de las sentencias más relevantes", *Programa estado de Derecho para Latinoamérica*, 2009.

[82] *Cfr*. PÉREZ LUÑO, A. E., "Libertad informática y derecho a la autodeterminación informativa", en *I Congreso sobre Derecho Informático*, Ed. Facultad de Derecho de la Universidad de Zaragoza, 1989, pp. 359-375; PÉREZ LUÑO, A. E., "El derecho a la autodeterminación informativa", *Anuario de jornadas 1989-1990*, Ed. Servicio de Estudios del IVAP, 1991, pp. 299-331.

El Alto Tribunal impulsado por los movimientos doctrinales existentes en el momento, acogió como propia la necesidad de declarar un nuevo derecho constitucional —aunque el mismo tuviera carácter limitado—[83], pues ni la Ley Fundamental de Bonn ni la legislación específica de protección de datos existente en Alemania[84] daban cabida a esta tipología de situaciones abusivas como las que se habían planteado en el objeto de litigio. Todo ello podría considerarse un presagio de las situaciones que se producirían en las décadas venideras, en que los poderes públicos, valiéndose de la utilización de las nuevas herramientas surgidas como consecuencia del desarrollo tecnológico, pretenderían la recogida de datos personales de manera indiscriminada, sin disponer de una finalidad claramente definida.

A este respecto, resulta oportuno indicar según destaca Prieto Gutiérrez, que dicha concepción formulada por el Tribunal Constitucional Federal de Alemania no puede entenderse como el origen del derecho a la protección como lo entendemos en la actualidad, sino que lo que se hace es reconocer por primera vez el derecho fundamental a la autodeterminación informativa desde una perspectiva constitucional, entendiéndolo como la facultad del individuo de decidir básicamente por sí solo sobre la difusión y la utilización de sus datos personales[85].

1.5. Acuerdo de Schengen

Los textos constitucionales de distintos países del entorno comunitario fueron adaptándose paulatinamente a la nueva configuración que se iba forjando sobre el derecho a la protección de datos personales[86]. En este contexto, la Comunidad Europea no fue una excepción, pues el 14 de junio de 1985 se suscribió por parte de algunos Estados

[83] *Vid*. MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica…*, *op. cit.*, p. 241.

[84] *Vid*. FROSINI, V., "Banco de datos y tutela de la persona", en *Revista de Estudios Políticos*, Vol. XXX, Ed. Nueva Época, 1982, p. 21; SERRANO PÉREZ, M. M., *El derecho fundamental…*, *op. cit.*, p. 29-35.

[85] *Cfr*. PRIETO GUTIÉRREZ, J. M., "Objeto y naturaleza jurídica del derecho fundamental a la protección de datos personales", en *Estudios del Ministerio de Justicia*, Boletín nº 1971-1972 (2003), p. 25.

[86] Sírvase a título de ejemplo, la reforma operada en 1980 sobre la Constitución de Finlandia de 1919. Consultado el 12.07.2020 desde: http://www.finlex.fi/fi/laki/kaannokset/1999/es19990731.pdf. O en su defecto, la modificación operada en 1983 sobre la Ley Fundamental del Reino de los Países Bajos. Consultado el 12.07.2020 desde: http://www.wipo.int/wipolex/es/details.jsp?id=7418.

miembros[87] el Acuerdo de Schengen[88], que posteriormente se vería complementado por su Convenio de Aplicación[89]. Esta actuación se convirtió en uno de los hitos de mayor relevancia en el proceso de construcción de la Unión Europea y, a su vez, de manera indirecta, por lo que aquí nos interesa, en lo relativo a la protección de los datos de carácter personal[90].

El Acuerdo de Schengen surge con el principal objetivo de conseguir la supresión gradual de determinados obstáculos transfronterizos existentes en la Comunidad Económica Europea que dificultaban el tráfico económico entre sus distintos miembros. El texto propugnaba la creación de un régimen de libre circulación para aquellos países que lo hubieren suscrito. No obstante, debe recordarse que su ámbito de aplicación se encontraba delimitado a ciertas materias sobre las que existiera acuerdo, como el control de fronteras y aduanero —a pesar de la existencia de determinadas particularidades para algunos Estados—.

Para conseguir el objetivo apuntado, se articuló la creación del Sistema de Información de Schengen (en adelante, SIS), posibilitando que cada uno de los Estados firmantes designase una autoridad competente nacional, que, a su vez, con el soporte de una unidad de apoyo técnico en la sede central ubicada en Estrasburgo, permitiera la flexibilización del régimen existente sobre el intercambio informatizado de información

---

[87] El Acuerdo de Schengen fue inicialmente suscrito el 14 de junio de 1985 entre Alemania, Bélgica, Francia, Luxemburgo y los Países Bajos. Cabe destacar, que, en la actualidad, la mayoría de los Estados Miembros de la Unión Europea se han adherido al mismo, incluso algunos terceros países. En lo referente a España, el día 25 de junio de 1991, el Plenipotenciario de España, nombrado en buena y debida forma al efecto, firmó en Bonn el Acuerdo de Adhesión del Reino de España al Convenio de aplicación del Acuerdo de Schengen de 14 de junio de 1985 entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 19 de junio de 1990, al cual se adhirió la República Italiana por el Acuerdo firmado en París el 27 de noviembre de 1990, hecho en el mismo lugar y fecha de su firma. Consultado el 12.07.2020 desde: https://www.boe.es/buscar/doc.php?id=BOE-A-1994-7586.

[88] Para una mayor profundización sobre los antecedentes y la evolución del Acuerdo Schengen, *vid*., entre otros: RUÍZ CARRILLO, A., *"Los datos de carácter personal. Concepto, requisitos de circulación, procedimientos y formularios"*, Barcelona: Ed. Bosch, 1999, p. 109; LUQUE GONZÁLEZ, J. M., "Schengen Un espacio de libertad, seguridad y justicia", en *Revista de derecho*, Ed. División de Ciencias Jurídicas de la Universidad del Norte, nº 21 (2004), pp. 139-149; GUERRERO PICÓ, M. C., *El impacto de Internet*…, *op. cit.*, pp. 120-127.

[89] El Convenio de Aplicación complementa las disposiciones del Acuerdo de Schengen, determinando las condiciones en las que resulta de aplicación la libre circulación, el cual fue suscrito el 19 de junio de 1990.

[90] *Vid*. REBOLLO DELGADO, L. y SERRANO PÉREZ, M. M., *Introducción a la*…, *op. cit.*, p. 41.

de personas y bienes. El principal cometido del SIS se vinculaba con la prevención del fraude fiscal y aduanero, llegando a convertirse en un verdadero mecanismo de coordinación y cooperación interestatal.

Pese a que el objetivo principal del Acuerdo de Schengen no radicaba en regular aspectos vinculados a la protección de los datos de carácter personal, vino a preceptuarse como un instrumento de cooperación que indirectamente se encontraba afectado por esta materia. Todo ello resultaba de la concentración y utilización de elevados volúmenes de información —entre los que se encontraban datos de carácter personal— para garantizar el cumplimiento de los fines de seguridad pública para todo aquel tráfico de personas y bienes que accediera al espacio Schengen[91].

Posteriormente, el Convenio del Aplicación vino a establecer los principios y mecanismos que debían garantizar la protección de los datos personales que se gestionaban a través del SIS. Se obligó a que cada país miembro designase una autoridad de control que velara por garantizar el respeto a su respectivo ordenamiento jurídico, sobre todo en lo relativo a la protección de los datos de carácter personal. En el ámbito comunitario, dichas competencias serían ejercidas por parte del Supervisor Europeo de Datos Personales[92].

Asimismo, hay que añadir que el Sistema de Información Schengen ha sido objeto de varias actualizaciones desde su creación mediante la introducción de nuevas funcionalidades, propiciando que el mismo vaya adaptándose gradualmente a los nuevos escenarios tecnológicos que se van planteado. De hecho, una de las últimas actualizaciones operadas, aparte de venir motivada por los correspondientes avances técnicos sucedidos, se vio propiciada como consecuencia de la adopción del Tratado de Lisboa[93].

---

[91] *Vid*. ARENAS RAMIRO, M., *El derecho fundamental…*, *op. cit.*, p. 286.

[92] *Cfr.* Considerando 24 de la Decisión 2007/533/JAI. En su artículo 61.1. se contiene el literal siguiente: "El Supervisor Europeo de Protección de Datos controlará que las actividades de tratamiento de datos personales de la Autoridad de Gestión sean conformes a la presente Decisión. En consecuencia, serán de aplicación las disposiciones sobre funciones y competencias del Supervisor Europeo de Datos previstas en los artículos 46 y 47 del Reglamento (CE) nº 45/2001".

[93] Por cuanto el día 13 de diciembre de 2007, el Plenipotenciario de España, nombrado en buena y debida forma al efecto, firmó en Lisboa el Tratado por el que se modifican el Tratado de la Unión Europea y el Tratado Constitutivo de la Comunidad Europea, hecho en Lisboa el 13 de diciembre de 2007. Consultado el 12.07.2020 desde: https://www.boe.es/buscar/doc.php?id=BOE-A-2009-18898. *Vid*., entre otros:

Finalmente, cabe destacar que a principios de los años noventa, siendo consciente de las carencias normativas existentes en materia de protección de datos personales en el contexto comunitario, la Comisión Europea propició la posibilidad de articular nuevos cuerpos normativos sobre la materia[94]. Dichas actuaciones se verían complementadas con el cambio sustantivo que se produciría como consecuencia de la aplicación del Tratado de Maastricht[95], que tendría como principal cometido propiciar de manera efectiva la creación un mercado único interior de libre circulación entre los distintos Estados miembros, teniendo amparo, por su importancia económica, la facilitación de los movimientos transfronterizos de datos de carácter personal.

1.6. Directiva 95/46/CE

Antes de proseguir con el análisis de evolución normativa que venimos efectuando, resulta preciso destacar la multiplicidad de cuerpos legales que se fueron sucediendo en el ámbito comunitario para intentar consolidar una uniformización de parámetros que resultase aplicable en los Estados miembros y aquellos terceros países que dispusieran de un nivel de protección equiparable en materia de protección de datos de carácter personal. Por lo que se advierte que, en las siguientes líneas, únicamente se citarán aquellos instrumentos jurídicos considerados de mayor relevancia en lo que concierne a la materia objeto de estudio, esto es, las transferencias internacionales de datos personales, dedicándose los siguientes apartados de este capítulo a su detalle y análisis.

Tras el proceso de construcción normativo acaecido durante los últimos años en torno al concepto de la protección de los datos personales, sumado a un intenso período de negociaciones sucedido en el contexto comunitario, se aprueba la Directiva 95/46/CE

ARENAS GARCÍA, R. y PÉREZ FRANCESCH, J. L., "Extranjería (II) entrada en el espacio Schengen y permanencia en España", en GETE-ALONSO Y CALERA, M. C. y SOLÉ RESINA, J. (Coord.), *Tratado de Derecho de la Persona Física*, Vol. II, Navarra: Ed. Civitas, 2013, pp. 467-536.

[94] *Cfr*. Decisión del Consejo relativa a la apertura de negociaciones con vistas a la adhesión de las Comunidades Europeas al Convenio (108) del Consejo de Europa sobre la protección de las personas con respecto al tratamiento automatizado de los datos personales (COM [90] 314, de 24 de septiembre de 1990, DOCE, serie C, nº 277, de 5 de noviembre de 1990).

[95] Su firma se produce como consecuencia de la reunión mantenida por parte del Consejo Europeo y los Jefes de Estado y de Gobierno de los países de la Comunidad Europea, los días 9 y 10 de diciembre de 1991, en Maastricht (Holanda), donde se ultimó el contenido del Tratado sobre la Unión Política, cuya firma se produciría el 7 febrero de 1992 por los Estados Miembros, modificándose, en consecuencia, el Acta Única Europea vigente de 1986. Consultado el 12.07.2020 desde: https://www.boe.es/buscar/doc.php?id=BOE-A-1994-626.

del Parlamento Europeo y del Consejo, de 24 de octubre de 1995[96]. La Norma se consolida como el principal instrumento existente sobre la materia, que como su propia rúbrica indica, pretendía como cometido principal sentar las bases que regirían el tratamiento de datos de carácter personal y la libre circulación de estos en el ámbito de la Unión Europea[97].

Se trataba de una disposición normativa que vinculaba a la totalidad de los Estados Miembros destinatarios, instándoles a adoptar una serie de actuaciones dentro de un plazo determinado. Pese a que dejaba bajo criterio de las autoridades nacionales competentes nacionales la elección de los medios que permitieran alcanzar el fin establecido[98], en este sentido la Directiva pretendía garantizar un nivel de protección equivalente entre los distintos países miembros para facilitar el intercambio de datos[99], aspecto que no se había conseguido hasta el momento con la única aplicación del Convenio 108, cuyo contenido hemos tenido la oportunidad de tratar con anterioridad.

A este respecto, Troncoso Reigada afirma que la propia Unión Europea ha reconocido como antecedente de su derecho derivado el Convenio 108. Así, la Recomendación de la Comisión de 29 de julio de 1981 instó a los Estados Miembros de la Comunidad a firmar y ratificar lo antes posible el Convenio 108 del Consejo de Europa.

---

[96] Publicada el 23 de noviembre de 1995 en el Diario Oficial nº L 281, pp. 31-50.

[97] *Vid*., entre otros: ESTADELLA YUSTE, O., "The Draft Directive of the European Community Regarding the Protection of Personal Data", en *International and Comparative Law Quarterly*, nº 41 (1992), pp. 170-179; ALONSO BLAS, D., "La aplicación de la directiva europea de protección de datos en España: reformas necesarias en la L.O.R.T.A.D.", en *X Encuentro sobre Informática y Derecho*, Madrid: Ed. Universidad Pontificia Comillas, 1996; MARTÍN-CASALLO, J. J., "La Directiva 95/46/C.E. y su incidencia en el ordenamiento jurídico español", en *Jornadas sobre el Derecho Español de la protección de datos personales*, Madrid: Ed. Agencia de Protección de Datos, 1996; HEREDERO HIGUERAS, M., *La Directiva Comunitaria de Protección de los Datos de Carácter Personal. Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/C.E., 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*, Pamplona: Ed. Aranzadi, 1997; PLESSER, R. L. y CIVIDANES, E. W., "EC Personal Data Privacy: US Concerns", en *Transnational Data and Communications Report*, Vol. XIII, nº 9 (1990), p. 19; RILEY, T., "Data Protection Clash on EC Directives", en *Transnational Data and Communications Report*, Vol. XIII, n º 9 (1990), pp. 5-11; SIMITIS, S., "Analyse du project de directive pour l'harmonisation des legislations", en *XII Conférence Internationale des Commissaires à la Protection des Données*, París, 1991; HOLMES, B. P., "US criticizes EC Data Directive's Potential Burdens and Barriers", en *Transnational Data and Communications Report*, Vol. XIV, nº 6 (1991), pp. 8-9; MIRABELLI, G., "In tema di tutela dei dati personali (note a margine della proposta modificata di direttiva C.E.E.", en *Il diritto dell'informazione e dell'informatica*, 1993, pp. 609-615; CARLIN, F. M., "The Data Protection Directive: the introduction of common privacy standards", en *European Law Review*, 1996.

[98] *Cfr.* Considerandos nº 7 y 9 de la Directiva 95/46/CE.

[99] *Vid.* MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica…*, *op. cit.*, p. 224.

De hecho, el propio texto de la Directiva 95/46/CE se basa en los principios enunciados en el Convenio del Consejo de Europa. Adicionalmente, apunta que esto es así especialmente después del reforzamiento de la cooperación en asuntos de justicia e interior, que ha llevado a la celebración de distintos acuerdos entre los Estados Miembros, como el Convenio de Schengen, y que obliga a la transmisión de datos personales entre las Administraciones de dichos países[100].

En el mismo sentido se pronuncia Serrano Pérez, que determina que la Directiva mejora la regulación contenida en el Convenio, haciéndolo constar así expresamente. Pero, además, la Directiva no es una norma de mínimos al estilo de aquel. Según el contenido establecido en su artículo 1.2: "Los Estados Miembros no podrán restringir la libre circulación de datos de carácter personal asegurando así la protección del individuo". La norma comunitaria concreta un alto nivel de protección, más fuerte que el señalado por el Convenio que dejaba a disposición de los Estados parte la posibilidad de ser mejorado[101].

En relación con su contenido, cabe aducir que el ámbito de aplicación no se extendía únicamente respecto de los tratamientos automatizados de datos personales, sino que también lo hacía sobre la totalidad de tratamientos que se realizasen manualmente, esto es, a través de medios no automatizados —como sucedía cuando se gestionaba información en soporte papel—. Pese a parecer una cuestión sin demasiada trascendencia, hay que destacar todo lo contrario, pues a fecha de hoy, tanto en el sector público como el privado, existen multitud de entidades que no han realizado proyectos de transformación digital que les permitiría disponer de los datos únicamente en soporte digital[102].

En consonancia con lo anterior, existía una casuística de tratamientos de datos personales que resultaban expresamente excluidos del ámbito de aplicación de la Norma. Los mismos radicaban, por un lado, en aquellos ejercidos por una persona física en su ámbito particular o doméstico; y, por otro lado, sobre ciertas actividades no contempladas

[100] *Cfr.* TRONCOSO REIGADA, A., *La protección de datos personales: en busca del equilibrio*, Valencia: Ed. Tirant lo Blanch, 2010, pp. 58-59.

[101] *Cfr.* SERRANO PÉREZ, M. M., *El derecho fundamental…*, *op. cit.*, p. 95; REBOLLO DELGADO, L. y SERRANO PÉREZ, M. M., *Introducción a la…*, *op. cit.*, p. 37.

[102] *Cfr.* Artículo 3, apartado primero, de la Directiva 95/46/CE.

dentro del ámbito de aplicación del derecho comunitario, tales como las cuestiones vinculadas a la seguridad y defensa de los respectivos Estados Miembros[103].

Respecto al análisis de su contenido[104], resulta oportuno indicar que la Directiva 95/46/CE se encontraba dividida en siete capítulos. El primero de ellos abordaba las cuestiones relativas a su objeto y ámbito de aplicación. El segundo, recogía un conjunto de principios de obligado cumplimiento que determinaban si un tratamiento de datos personales podía llevarse a término lícitamente por parte de su responsable.

Entre el conjunto de principios aludidos, interesa destacar los siguientes: (i) los datos debían ser recabados para finalidades específicas y tratados de manera legítima, manteniéndolos debidamente actualizados; (ii) únicamente se podía proceder a un tratamiento si existía base de legitimación suficiente; (iii) resultaba imperativo cumplir con el derecho de información con antelación a proceder a la recogida de los datos personales; (iv) se debían atender y dar curso a las peticiones de ejercicio de derechos realizadas por parte de los interesados en tiempo y forma; (v) se prohibía el tratamiento de categorías especiales de datos personales, a excepción de que concurriese alguna de las excepciones expresamente previstas; (vi) se debía garantizar la confidencialidad y seguridad del tratamiento; y (vii) se imponía un deber de cooperación con la autoridad de control nacional correspondiente con competencias sobre la materia.

La doctrina ha debatido la cuestión sin encontrar una posición unánime sobre los principios rectores que incorpora la Directiva 95/46/CE, pues, por un lado, Martínez Martínez ha indicado que el núcleo central de la protección otorgada por la Directiva se basa en el consentimiento, así como en la garantía de la autodeterminación individual.

---

[103] *Vid.* REBOLLO DELGADO, L., *Derechos fundamentales y protección de datos*, Madrid: Ed. Dykinson, 2004, p. 132.

[104] *Vid.*, entre otros: PRIETO GUTIÉRREZ, J. M., "La Directiva 95/46/CE como criterio unificador", en *Revista del Poder Judicial*, nº 48 (1998), pp. 165-243; GARRIGA DOMÍNGUEZ, A., *La protección de los datos personales en el derecho español*, Dykinson, Madrid, 1999, pp. 295-337; HERRÁN ORTIZ, A. I., *El derecho a la intimidad en la nueva Ley orgánica de protección de datos personales*, Dykinson, Madrid, 2002, pp. 115-194; GUERRERO PICÓ, M. C., *El impacto de Internet…*, *op. cit.*, pp. 63-101; REBOLLO DELGADO, L. y SERRANO PÉREZ, M. M., *Introducción a la…*, *op. cit.*, pp. 36-42. En lo concerniente a la transposición en España de la Directiva 95/46/CE, *vid.*, entre otros: CASTAÑO SUÁREZ, R., "Directiva 95/46, 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: Similitudes y diferencias con la Ley Orgánica 5/1992, de 29 de octubre (LORTAD)", en *Noticias de la Unión Europea*, nº 162 (1998), pp. 9-16; HEREDERO HIGUERAS, M., "Estudio crítico de la transposición de la Directiva 95/46/CE en el ordenamiento jurídico español por la L.O. 15/1999 de 13 de diciembre", en *Revista Jurídica de Navarra*, nº 31 (2001), pp. 124-139.

Sin perjuicio de la existencia de supuestos en los que una habilitación legal, los derechos e intereses legítimos de terceros o el propio interés vital del titular de los datos habiliten un tratamiento de datos sin obtención de consentimiento[105]. En cambio, Guerrero Picó señala que el centro de gravedad del sistema instaurado por la Directiva se desplaza a las condiciones de licitud del tratamiento, a diferencia de la propuesta de 1990, que daba mayor relevancia al papel jugado por el consentimiento[106].

El tercer capítulo de la Directiva reconocía un haz de facultades a los afectados por la recogida y utilización de sus respectivos datos personales para que pudiesen acudir a la vía administrativa y judicial para velar por el respeto de sus derechos. Al mismo tiempo, se instaba a los Estados miembros para que articulasen los mecanismos necesarios que permitiesen dar cumplimiento a dichas prerrogativas, así como previeran cuadros sancionadores suficientes que permitieran garantizar la plena aplicación de las disposiciones previstas en la norma comunitaria que se viene analizando.

El cuarto capítulo se orientaba a establecer las directrices que regirían las transferencias internacionales de datos, cuyo contenido será analizado expresamente en las próximas líneas con mayor precisión. Los capítulos quinto a séptimo recogían cuestiones de diversa índole como la adopción y regulación de códigos de conducta, la necesidad de articular la creación de autoridades nacionales de protección de datos que se encargasen de velar por el cumplimiento del contenido preceptuado en la Directiva en sus respectivos territorios nacionales, así como las medidas de ejecución comunitarias relacionadas con el cumplimiento de las consideraciones previstas en la Norma comunitaria.

En este punto, conviene resaltar la importancia del mandato que se incluía en el artículo 29 de la Directiva, cuyo contenido proclamaba la necesidad de articular la creación de un grupo de expertos orientado a la protección de las personas en lo relativo al tratamiento de sus datos personales[107]. Su composición estaría conformada por los

---

[105] *Cfr*. MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica…*, *op. cit.*, p. 225.

[106] *Cfr*. GUERRERO PICÓ, M. C., *El Impacto de Internet en…*, *op. cit.*, p. 76.

[107] Posteriormente, este grupo enunciado por el artículo 29 de la Directiva 95/46/CE pasaría a ser denominado comúnmente como "Grupo de Trabajo del Artículo 29" o bajo sus siglas "GT29" -como hemos tenido la oportunidad de advertir con anterioridad-, configurándose como un factor fundamental en el desarrollo normativo de la protección de los datos personales y su aplicación homogénea en el entorno comunitario.

representantes de las autoridades de control nacionales de los países miembros de la Unión Europea, así como por los representantes de las instituciones y organismos comunitarios con competencias sobre la materia. Entre las principales funciones que tenía encomendadas, se encontraba el estudio de las cuestiones relativas a garantizar una aplicación homogénea de las distintas normativas en el territorio comunitario, el asesoramiento especializado a otros órganos comunitarios o la emisión de dictámenes sobre ciertas cuestiones específicas[108].

Como señala Troncoso Reigada, el GT29 ha jugado un papel fundamental, facilitando una cooperación más estrecha entre todas las legislaciones europeas sucedidas a tenor de la aplicación de la Directiva[109], favoreciendo una aplicación homogénea de la misma. 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, y constituye 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[110].

---

[108] Para mayor conocimiento sobre las funciones del GT29, se reproduce, a continuación, el tenor literal del artículo 30, en sus apartados 1 a 4, de la Directiva 95/46/CE: "1. El Grupo tendrá por cometido: a) 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; b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros; c) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades; d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria. 2. Si el Grupo comprobara la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieran afectar a la equivalencia de la protección de las personas en lo que se refiere al tratamiento de datos personales en la Comunidad, informará de ello a la Comisión 3. El Grupo podrá, por iniciativa propia, formular recomendaciones sobre cualquier asunto relacionado con la protección de las personas en lo que respecta al tratamiento de datos personales en la Comunidad. 4. Los dictámenes y las recomendaciones del Grupo se transmitirán a la Comisión y al Comité contemplado en el artículo 31".

[109] Entre otras medidas, se traspuso la Directiva con un carácter más temprano, en los siguientes países del contexto comunitario: Italia (1996), Grecia (1997), Luxemburgo (1998), Portugal (1998), Reino Unido (1998), Suecia (1998), Finlandia (1999), Austria (2000), Países Bajos (2000). Sin perjuicio de ello, otros territorios como Francia, Irlanda o Dinamarca adaptaron las legislaciones vigentes de las que ya disponían. A diferencia de lo que ocurre en la legislación española, en que todo pivota en base al principio de obtención del consentimiento, ello no aparece reflejado en las diferentes legislaciones a las que hemos aludido, pues optan por otros mecanismos para dar cumplimiento a las vicisitudes contenidas en la Directiva 95/46/CE. *Vid*. DAVARA RODRÍGUEZ, A., *La protección de datos…*, *op. cit.*

[110] *Cfr*. TRONCOSO REIGADA, A., "Hacia un nuevo marco jurídico europeo de protección de datos personales", en *Revista Española de Derecho Europeo*, nº 43 (2012), pp. 42-43.

Pese a que la Directiva establecía la necesidad de transponer su contenido a los respectivos ordenamientos jurídicos de los Estados miembros con antelación a su entrada en vigor[111], llegada la fecha un número importante de países no había realizado los esfuerzos necesarios para propiciar la consecución de dicho objetivo. Por este motivo, ante la situación deficiente que se había generado, la Comisión Europea optó por denunciar ante el Tribunal de las Comunidades Europeas a los territorios que habían incumplido el mandato[112]. Los mismos habían sido advertidos con antelación mediante la remisión de dictámenes razonados que les emplazaban a dar cumplimiento a los plazos que se habían estipulado al respecto.

Este hecho, sumado a que determinados Estados miembros habían rebasado los márgenes de apreciación que la Directiva permitía en su transposición[113], así como a la divergencia de posiciones interpretativas que se fueron adoptando gradualmente por parte de los órganos jurisdiccionales y las autoridades supervisoras a través de sus pronunciamientos, fue generando una situación controvertida. Dicha tesitura debía haber sido subsanada con la llegada del Reglamento General de Protección de Datos, pero no ofreció las soluciones esperadas, tal y como tendremos oportunidad de abordar en los próximos apartados.

---

[111] La entrada en vigor de la Directiva 95/46/CE se produjo en fecha 25 de octubre de 1998.

[112] La denuncia por parte de la Comisión Europea se efectuó en fecha 11 de enero del año 2000, en virtud de la potestad dimanante del artículo 226 del Tratado de las Comunidades Europeas. El grupo de Estados Miembros destinatarios de dicha acción se componía por los siguientes: Irlanda, Alemania, Francia, Luxemburgo y Holanda.

[113] Desde la perspectiva del derecho comunitario, cabe recordar, como bien es sabido, que la institución de la directiva requiere de su transposición por parte de los Estados Miembros en los respectivos ordenamientos jurídicos internos, pues no dispone de efecto directo desde su aprobación. Esta particularidad facilita que nos encontremos escenarios como los advertidos en lo concerniente a la Directiva 95/46/CE, en que los países destinatarios disponen de un holgado margen de maniobra para regular el contenido mínimo que permita completar la directiva en cuestión. En contraposición, la institución del reglamento se constituye como un instrumento con eficacia plena, tanto en sentido vertical como horizontal, pues, siguiendo el mandato establecido en el artículo 288 del Tratado de Funcionamiento de la Unión Europea, producen efectos inmediatos desde su promulgación y entrada en vigor, siendo directamente aplicable sobre los distintos Estados Miembros. A este respecto, el Considerando 13 del RGPD establece literalmente que: "[p]ara garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros".

Sobre este punto, tuvo ocasión de pronunciarse el Tribunal de Justicia de la Unión Europea[114], mediante dos pronunciamientos que aquí interesa traer a colación. Por un lado, el asunto Lindqvist[115], que se constituye como el caso de referencia en lo relativo a la aplicabilidad de la Directiva 95/46/CE[116], pues dispone el siguiente tenor literal: "[p]or tanto, la armonización de dichas legislaciones nacionales no se limita a una armonización mínima, sino que constituye, en principio, una armonización completa. Desde este punto de vista, la Directiva 95/46 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 titulares de dichos datos"[117].

Asimismo, sigue afirmando: "Es cierto que la Directiva 95/46 reconoce a los Estados miembros un margen de apreciación en ciertos aspectos y que les permite mantener o establecer regímenes particulares para situaciones específicas, tal y como lo demuestra un gran número de sus disposiciones. No obstante, dichas posibilidades deben emplearse tal y como dispone la Directiva y de conformidad con su objetivo, que consiste en mantener un equilibrio entre la libre circulación de datos personales y la tutela del derecho a la intimidad"[118].

---

[114] *Vid*., entre otros: DE MIGUEL ASENSIO, P. A., "Avances en la interpretación de la normativa comunitaria sobre protección de datos personales", en *La Ley Unión Europea*, nº 5964 (2003), Madrid, pp. 1-4; BAYO DELGADO, J., "Derecho comunitario sobre protección de datos", en GÓMEZ MARTÍNEZ, C. (Dir.), en *"Derecho a la intimidad y nuevas tecnologías"*, Madrid: Ed. Cuadernos de Derecho Judicial IX-2004, Consejo General del Poder Judicial, 2004, pp. 59-60; DE MIGUEL ASENSIO, P. A., "La protección de datos personales a la luz de la reciente jurisprudencia del TJCE", en *Revista de la Facultad de Derecho de la Universidad de Granada*, Granada, nº 7 (2003), pp. 397-417; GUERRERO PICÓ, M. C., *El impacto de Internet…*, *op. cit.*, pp. 356-361; PULIDO QUECEDO, M., "La catequista y los riesgos de Internet", en *Actualidad Jurídica Aranzadi*, nº 602 (2003), Cizur Menor (Navarra): Ed. Aranzadi, pp. 14-15; SERRERA COBOS, P., *Buenas prácticas en protección de datos*, Madrid: Ed. Fundación DINTEL, 2007, pp. 28-31. Sobre la actividad del TJUE en materia de protección de datos de carácter personal, *vid*.: ARENAS RAMIRO, M., "El derecho a la protección de datos personales en la jurisprudencia del TJCE", en *Revista de Derecho y Nuevas Tecnologías*, Vol. IV, Ed. Aranzadi, 2006, pp. 95-119.

[115] Sentencia del Tribunal de Justicia de las Comunidades Europeas (en adelante, STCE), de fecha 6 de noviembre de 2003, asunto C-101/2001, en que se analiza el supuesto de una catequista sueca que, tras realizar un curso de informática, publica una serie de datos personales de diversa índole sobre varios de sus compañeros feligreses a través de la red sin haberles advertido previamente de ello. Dicha actuación fue sancionada por incumplimiento de varios preceptos de la legislación sueca. Consultado el 12.07.2020 desde: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN.

[116] *Cfr*. RALLO LOMBARTE, A., "El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en Internet", en *Teoría y Realidad Constitucional*, nº 39 (2017), Ed. Universidad Nacional de Educación a Distancia (UNED), p. 585.

[117] *Cfr*. STCUE. Asunto C-101/2001 (Lindqvist), cit., apdo. 96.

[118] *Ibidem*, apdo. 97.

Adicionalmente, como indica Rallo Lombarte[119], se trata de la primera ocasión en que el TJUE evaluó el impacto extraterritorial -y, en consecuencia, global- de la Directiva europea a los servicios de Internet al negar que nos halláramos en este supuesto ante una transferencia internacional de datos, a pesar de que una persona difundiera datos desde una página web de un Estado miembro que fueran almacenados en un servidor del mismo Estado o de otro Estado miembro, y resultando dichos datos accesibles a cualquier persona conectada a Internet aunque se encontrara en países terceros[120].

Por otro lado, con posterioridad, el Tribunal de Justicia ha declarado en los asuntos acumulados C-468/10 (ASNEF) y C-469/10 (FEDECM)[121] el siguiente tenor literal: "[E]n este contexto, procede recordar que la Directiva 95/46 tiene por objeto, tal y como se desprende, en particular, de su octavo considerando, equiparar el nivel de protección de los derechos y libertades de las personas por lo que se refiere al tratamiento de datos personales en todos los Estados miembros. Su décimo considerando añade que la aproximación de las legislaciones nacionales en la materia no debe conducir a una disminución de la protección que garantizan, sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección dentro de la Unión"[122].

Así pues, manifiesta que: "[S]e ha declarado así que la armonización de dichas legislaciones nacionales no se limita a una armonización mínima, sino que constituye, en principio, una armonización completa. Desde este punto de vista, la Directiva 95/46 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"[123].

---

[119] Para una posición doctrinal contraria a esta interpretación, *vid.*: POULLET, Y., "Flujos de datos transfronterizos y extraterritorialidad: la postura europea", en *Revista Española de Protección de Datos*, nº 1 (2006), pp. 99-105.

[120] *Cfr.* RALLO LOMBARTE, A., "*El Tribunal de Justicia de…*", *op. cit.*, p. 586.

[121] *Vid.* Sentencia del Tribunal de Justicia de la Unión Europea, de fecha 24 de noviembre de 2011, asuntos acumulados C-468/10 y C-469/10, que tiene por objeto las peticiones de decisión prejudicial planteadas por la Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), asunto C-468/10, y la Federación de Comercio Electrónico y Marketing Directo (FECEMD), asunto C-469/10, relativas a la interpretación del artículo 7, letra f) de la Directiva 95/46/CE. Consultado el 12.07.2020 desde: http://curia.europa.eu/juris/document/document.jsf?docid=115205&doclang=ES.

[122] *Cfr.* STJUE. Asuntos acumulados C-468/10 (ASNEF) y C-469/10 (FEDECM), cit., apdo. 28.

[123] *Ibidem*, apdo. 29.

En definitiva, como señala Troncoso Reigada, todas estas incongruencias en la protección de los datos personales en los 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 todo el territorio de la Unión que reduzca o suprima el margen de elección del que disponen tanto los legisladores nacionales como las autoridades de control y los Tribunales[124].

1.7. Carta de Derechos Fundamentales de la Unión Europea

A tenor de los avances normativos detallados, se sucede la Carta de Derechos Fundamentales de la Unión Europea[125] (en adelante, CDFUE), adoptada mediante el Tratado de Niza suscrito en el año 2000. Su elaboración se enmarcó bajo la forma jurídica de una convención, estando a cargo de su redacción varios representantes del ámbito comunitario[126], para garantizar una mayor transparencia y participación durante la totalidad de su proceso de desarrollo. En este sentido, Arenas Ramiro establece que este método suponía un avance considerable en la medida en que, como se ha dicho, se

[124] *Cfr*. TRONCOSO REIGADA, A., "Hacia un nuevo marco jurídico…", *op. cit.*, p. 45.

[125] *Vid*., entre otros: FERNÁNDEZ TOMÁS, A., *La Carta de Derechos Fundamentales de la Unión Europea. Diez años de jurisprudencia*, Valencia: Ed. Tirant lo Blanch, 2001, pp. 84-89; ALONSO GARCÍA, R., "El triple marco de protección de los derechos fundamentales en la Unión Europea", en *Cuadernos de Derecho Público*, nº 13 (2001), pp. 13-17; SÁIZ ARNÁIZ, A., "La Carta de los Derechos Fundamentales de la Unión Europea y los ordenamientos nacionales: ¿qué hay de nuevo?", en *Cuadernos de Derecho Público*, nº 13 (2001), pp. 153-159; WEBER. A., "La Carta de los Derechos Fundamentales de la Unión Europea", en *Revista Española de Derecho Constitucional*, nº 64 (2002), pp. 79-84; RODRÍGUEZ BEREIJO, A., "La Carta de Derechos Fundamentales", en *Revista de Derecho de la Unión Europea*, nº 1 (2002), pp. 45-57; VICIANO PASTOR, R., "El largo camino hacia una constitución europea", en *Revista de Derecho de la Unión Europea*, nº 2 (2002), pp. 105-123; RUÍZ MIGUEL, C., "El largo y tortuoso camino hacia la Carta de los Derechos Fundamentales de la Unión Europea", en *Revista europea de derechos fundamentales*, nº 2 (2003), pp. 61-90; PAREJO NAVAJAS, T., "La Carta de los derechos fundamentales de la Unión Europea", en *Derechos y Libertades: Revista de filosofía del derecho y derechos humanos* (2010), pp. 205-239.

[126] La composición de la Convención estaba formada por miembros de las instituciones comunitarias como el Parlamento Europeo o la Comisión Europea, así como por representantes parlamentarios de los Estados Miembros. La propuesta definitiva se aprobó por la Convención en fecha 21 de julio de 2000, concluyéndose finalmente en fecha 2 de octubre de 2000 y adoptándose formalmente mediante el Tratado de Niza, firmado el 7 de diciembre de 2000. Posteriormente fue publicada en el Diario Oficial de la Unión Europea, en su nº 303, con fecha 14 de diciembre de 2007, p. 0004. Cabe destacar que, pese a que su adopción fue en el año 2000, no es hasta el 12 de diciembre de 2007 cuando se proclama en Estrasburgo, una vez que se ha ratificado el Tratado de Lisboa, que tendremos la oportunidad de analizar brevemente en las próximas líneas. Consultado el 19.07.2020 desde: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:12016P/TXT.

pretendía llevar a cabo el proceso de construcción europeo desde abajo hacia arriba, y no al contrario, como se venía haciendo hasta ahora[127].

Pese a que se tuvieron en cuenta las disposiciones normativas existentes y los pronunciamientos jurisprudenciales[128] sucedidos hasta el momento para elaborar su contenido, resulta oportuno destacar que dos instrumentos jurídicos jugaron un factor determinante: las disposiciones de la Directiva 95/46/CE y el contenido del artículo 286 del texto refundido del Tratado de la Unión Europea, introducido por el Tratado de Ámsterdam de 1997[129] —siguiendo las recomendaciones que se habían efectuado al respecto por parte del Grupo de Trabajo del Artículo 29[130]—. Dichas recomendaciones indicaban claramente la necesidad de enmarcar el derecho a la protección de datos como un derecho fundamental, en respuesta a la disparidad de criterios que se estaban sucediendo en la aplicación de legislación existente por parte de los distintos Estados miembros.

Adicionalmente a la ausencia de unidad de criterio, el contenido del artículo 8 de la Carta adolecía de cierta falta de completitud, pues no se incluían aspectos esenciales como la necesidad de articular la recogida de datos personales bajo la primacía del principio de transparencia y el cumplimiento del deber de información por parte del

---

[127] *Cfr*. ARENAS RAMIRO, M., *El derecho fundamental*…, *op. cit*., pp. 205-206. Para más información al respecto, *vid*., entre otros: CARRILLO SALCEDO, J. A., "Notas sobre el significado político y jurídico de la Carta de los Derechos Fundamentales de la Unión Europea", en *Revista de Derecho Comunitario Europeo*, nº 9 (2001), pp. 8-9.

[128] *Vid*., entre otras: la SSTJUE, de 9 de noviembre de 2010, en los asuntos acumulados C-92/09 y C-93/09, Caso Volker und Markus Schecke GbR [asunto C-92/09] y Hartmut Eifert [asunto C-93/09] contra Land Hessen. Consultado el 19.07.2020 desde: http://curia.europa.eu/juris/liste.jsf?language=es&num=C-92/09.

[129] El Tratado de Ámsterdam fue firmado el 2 de octubre de 1997 por los ministros de Asuntos Exteriores de los quince países miembros de la Unión Europea entró en vigor el 1 de mayo de 1999 tras haber sido ratificado por todos los Estados miembros, según sus propias normas constitucionales. Consultado el 19.07.2020 desde: https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_of_amsterdam_es.pdf.

[130] *Vid*. GT29. "Dictamen 4/1999 relativo a la inclusión del derecho fundamental a la protección de datos personales en el catálogo europeo de derechos fundamentales". Consultado el 19.07.2020 desde: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_enhtm#maincontent Sec19. El Grupo de Trabajo del Artículo 29, en su dictamen, terminó señalando que "la integración de la protección de datos de carácter personal entre los derechos fundamentales europeos haría aplicable esta protección en el conjunto de la Unión y pondría de relieve la importancia creciente de la protección de estos en la sociedad de la información".

responsable del tratamiento[131]. En palabras de Troncoso Reigada, 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[132].

Asimismo, resulta oportuno recordar que el contenido de los derechos a los que estamos haciendo alusión dispone a su vez de una serie de limitaciones. Las mismas vienen preceptuadas tanto en la Directiva 95/46/CE como en el propio artículo 52 de la propia Carta de Derechos Fundamentales de la Unión Europea, que en su apartado primero admite que dichas limitaciones deberán estar avaladas por una Ley, respetando al máximo el contenido esencial de los derechos y libertades, así como el principio de proporcionalidad[133].

Por el contrario, aquellas limitaciones que no respondan a objetivos de interés general, o no resulten necesarias, no podrán supeditar el ámbito de aplicación de los derechos reconocidos en el propio documento[134]. Sin perjuicio de que, tanto los propios derechos contemplados en la Carta como las posibles limitaciones que puedan resultar de aplicación deban interpretarse de conformidad con las tradiciones jurídicas constitucionales imperantes en los respectivos Estados miembros[135].

---

[131] *Vid*., entre otros: DÍEZ PICAZO, L. M., "¿Una Constitución sin declaración de derechos? (Reflexiones constitucionales sobre los derechos fundamentales en la Comunidad Europea)", en *Revista Española de Derecho Constitucional*, nº 32 (1991); ALONSO GARCÍA, R., "Derechos fundamentales y Comunidades Europeas", en *Estudios sobre la Constitución española. Homenaje al Profesor E. García de Enterría*, Tomo II, Madrid: Ed. Civitas, 1991; MAESTRO BUELGA, G., "Los derechos sociales en la Unión Europea: una perspectiva constitucional", en *Revista Vasca de Administración Pública*, nº 46 (1996); CORCUERA, J., *La protección de los derechos fundamentales en la Unión Europea*, Madrid: Ed. Dykinson, 2002; ALONSO GARCÍA, R., "La Carta de los Derechos Fundamentales de la Unión Europea", en *Gaceta jurídica de la Unión Europea y de la competencia*, nº 209 (2000), pp. 3-7; MANGAS MARTÍN, A., "El compromiso con los derechos fundamentales", en MANGAS MARTÍN, A. (Dir.), *Carta de los Derechos Fundamentales en la Unión Europea*, Madrid: Ed. Fundación BBVA, 2008, pp. 31-75.

[132] *Cfr*. TRONCOSO REIGADA, A., "Hacia un nuevo marco jurídico…", *op. cit.*, p. 80.

[133] *Cfr*. MANGAS MARTÍN, A., "Comentario al Artículo 52", en MANGAS MARTÍN, A. (Dir.), *Carta de los Derechos…*, *op. cit.*, pp. 826-851.

[134] A este respecto, "[s]in embargo, el derecho a la protección de los datos de carácter personal no constituye una prerrogativa absoluta, sino que debe ser considerado en relación con su función en la sociedad (véase en este sentido la sentencia de 12 de junio de 2003, Schmidberger, C-112/00, Rec. p. I-5659, apartado 80 y jurisprudencia citada)". *Cfr*. STJUE. Asuntos acumulados C-92/09 y C-93/09, cit., apdo. 48. Consultado el 12.07.2020 desde: http://curia.europa.eu/juris/document/document.jsf?text=&docid=79001&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=10747552.

[135] *Cfr*. Artículo 52, apartado 4, de la Carta de Derechos Fundamentales de la Unión Europea.

En este mismo sentido, se pronuncia el Tribunal de Justicia de la Unión Europea, en el asunto C-275/06, señalando que: "[...] Corresponde a los Estados miembros, a la hora de adaptar su ordenamiento jurídico a las Directivas citadas, procurar basarse en una interpretación de estas que garantice un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico comunitario. A continuación, en el momento de aplicar las medidas de adaptación del ordenamiento jurídico a estas Directivas, corresponde a las autoridades y a los órganos jurisdiccionales de los Estados miembros no solo interpretar su Derecho nacional de conformidad con dichas Directivas, sino también procurar que la interpretación de estas que tomen como base no entre en conflicto con dichos derechos fundamentales o con los demás principios generales del Derecho comunitario, como el principio de proporcionalidad"[136].

La Carta de Derechos Fundamentales de la Unión Europea viene a reforzar aún más la consagración del derecho a la protección de datos en el contexto comunitario, pues su contenido[137] viene totalmente marcado por todos los instrumentos normativos que se habían sucedido hasta la fecha, así como por los pronunciamientos efectuados por parte de los Tribunales competentes, esto es, el Tribunal de Justicia de las Comunidades Europeas y el Tribunal Europeo de Derechos Humanos[138].

Por este motivo, el artículo 8[139] de la Carta recoge expresamente el derecho a la protección de los datos personales como su propia rúbrica indica, pues a diferencia de lo

---

[136] *Vid*. STJUE de fecha, 29 de enero de 2008, en el asunto C-275/06, cit., apdo. 8. Consultado el 12.07.2020 desde: http://curia.europa.eu/juris/document/document.jsf?text=&docid=70107&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=10740906.

[137] La estructura de la Carta de Derechos Fundamentales de la Unión Europea se centra en dos partes claramente diferenciadas: un preámbulo que contiene la contextualización y su motivación, así como siete títulos que tratan el contenido de los distintos derechos, a excepción del último de ellos, que preceptúa una serie de disposiciones generales. *Vid*. ARENAS RAMIRO, M., *El derecho fundamental…*, *op. cit*., p. 207.

[138] *Vid*., entre otras: las sentencias del Tribunal Europeo de Derechos Humanos: Asunto N.K.M. contra Hungría, de 14 de mayo de 2013; Asunto M.M. contra Reino Unido, de 13 de noviembre de 2012; Asunto Joanna Szul contra Polonia, de 13 de noviembre de 2012; Asunto Khelili contra Suiza, de 18 de octubre de 2011; Asunto Goggins y otros contra Reino Unido, de 19 de julio de 2011; Asunto Wasmuth contra Alemania, de 17 de febrero de 2011; Asunto Dimitrov-Kazakov contra Bulgaria, 10 de febrero de 2011; Asunto Sanoma Uitgevers B.V. contra Países Bajos, 14 de septiembre de 2010; Asunto Bouchacourt contra Francia, de 17 de diciembre de 2009; Asunto Caso S. y Marper contra Reino Unido, de 4 de diciembre de 2008; Asunto Caso L. L. contra Francia, de 10 de octubre de 2006; Asunto Antunes Rocha contra Portugal, de 31 de mayo de 2005.

[139] Se reproduce el tenor literal del artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea referenciado, por lo que a efectos de este análisis interesa: "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan; 2. Estos datos se tratarán de modo leal, para fines

que había sucedido con el Convenio Europeo de Derechos Humanos[140] —que únicamente incluía una referencia al respeto de la vida privada como se ha detectado con anterioridad—, el nuevo texto introduce una nueva perspectiva, abordando de manera diferenciada el respeto a la vida privada y familiar[141] y el derecho a la protección de datos de carácter personal[142].

Sobre la cuestión Piñar Mañas considera que: "[...] El Tribunal de Justicia no ha tenido ocasión de hacer una manifestación expresa de reconocimiento del derecho fundamental a la protección de datos como derecho autónomo e independiente del derecho a la intimidad. Lo cual es de alguna manera lógico no solo por lo reciente de la adopción de la Carta de Derechos Fundamentales, sino por el propio valor jurídico de esta"[143].

Una vez revisado lo anterior, podemos concluir que la Carta de Derechos Fundamentales de la Unión Europea no contiene un *numerus clausus* de supuestos que habiliten restricciones sobre los derechos que en ella se reconocen, a diferencia de lo sucedido con otros textos legales analizados[144]. Las posibles limitaciones de derechos existentes se amparan bajo el concepto jurídico indeterminado del interés general, acuñado jurisprudencialmente con la expresión "*pressing social need*" por parte del Tribunal Europeo de Derechos Humanos[145].

---

concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación; 3. El respeto de estas normas estará sujeto al control de una autoridad independiente".

[140] *Cfr*. MARTÍN Y PÉREZ DE NANCLARES, J., "Artículo 8. Protección de datos de carácter personal", en MANGAS MARTÍN, A. (Dir.), *Carta de los Derechos…*, *op. cit.*, pp. 223-255; ARENAS RAMIRO, M., *El derecho fundamental…*, *op. cit.*, pp. 246-248.

[141] *Cfr*. Artículo 7 de la Carta de Derechos Fundamentales de la Unión Europea.

[142] *Vid*. ARENAS RAMIRO, M., *El derecho fundamental…*, *op. cit.*, pp. 225-248; TÉLLEZ AGUILERA, A., *La protección de datos en la Unión Europea*, Madrid: Ed. Edisofer, 2002, pp. 59-65.

[143] *Cfr*. PIÑAR MAÑAS, J. L., "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas", en *Cuadernos De Derecho Público*, nº 19-20, 2011, p. 57.

[144] *Vid*. Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales.

[145] *Cfr*., entre otras: Sentencia del Tribunal Europeo de Derechos Humanos, de 6 de septiembre de 1978, en el asunto Klass y otros contra la República de Alemania. *Vid*., entre otros: RUIZ MIGUEL, C., "El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico", en *Revista de Derecho Comunitario Europeo*, nº 14 (2003), pp. 7-43; TRONCOSO REIGADA, A., "Hacia un nuevo marco jurídico…", *op. cit.*, 2012, pp. 99-100.

1.8. Tratado de Lisboa

La promulgación del Tratado de Lisboa[146] obedece, entre otras cuestiones[147], a la necesidad de enmendar ciertas deficiencias regulatorias existentes que dificultaban el proceso de expansión que tenía previsto experimentar la Unión Europea en los años venideros[148]. Desde el prisma de la protección de datos de carácter personal, la aparición de este instrumento jurídico supone la consagración definitiva del marco jurídico existente en la actualidad sobre la materia, cuyo máximo exponente resultará en el Reglamento General de Protección de Datos.

En este sentido, por lo que a efectos de este trabajo interesa, podemos sintetizar las consecuencias que se derivan de la aprobación del Tratado de Lisboa, por un lado, en la introducción del artículo 16 del Tratado de Funcionamiento de la Unión Europea. Dicho precepto viene a constituirse como el fundamento básico que deberán de tomar en consideración los distintos Estados miembros en cuestiones vinculadas con el tratamiento

[146] El Tratado de Lisboa, publicado en el Diario Oficial de la Unión Europea, nº 2007/C 306/01, de 17 de diciembre de 2007, y cuya entrada en vigor se produjo el 1 de diciembre de 2009, por el que se modifica el Tratado de la Unión Europea y el Tratado Constitutivo de la Comunidad Europea, que a partir de esta fecha pasará a denominarse como Tratado de Funcionamiento de la Unión Europea y, en consecuencia, toda referencia a las Comunidades Europeas se deberá considerar hecha a la Unión Europea. Consultado el 12.07.2020 desde: https://www.boe.es/doue/2007/306/Z00001-00271.pdf.

[147] Cuestiones tales como los rápidos avances tecnológicos sucedidos, los nuevos riesgos que se suceden sobre la materia para los afectados derivados de la pérdida de control sobre sus respectivos datos personales, así como la necesidad de articular la homogenización normativa sobre la materia en los distintos Estados miembros son algunas de las grandes preocupaciones que motivan las nuevas iniciativas, que culminarán con la aprobación del Reglamento General de Protección de Datos. Como buena muestra de ello, estas motivaciones acabarán plasmadas en los Considerandos 5 a 8 del nuevo texto normativo.

[148] *Vid*., entre otros: JÁUREGUI BERECIARTU, G. y UGARTEMENDÍA ECEIZABARRENA, J. I., "Europa en el lecho de Procusto: de la Constitución europea al Tratado de Lisboa", en *Revista Vasca de Administración Pública*, nº 79 (2007), pp. 105-126; PÉREZ DE NANCLARES, J. M. y URREA CORRES, M., "Tratado de Lisboa" (Recensión), en *Revista De Las Cortes Generales*, nº 70-72 (2007), pp. 1249-1252; BALAGUER CALLEJÓN, F., "El Tratado de Lisboa en el diván. Una reflexión sobre estatalidad, constitucionalidad y Unión Europea", en *Revista española de derecho constitucional*, nº 83 (2008), pp. 57-92; ALDECOA LUZÁRRAGA, F. y GUINEA LLORENTE, M., *La Europa que viene: el Tratado de Lisboa*, Madrid: Ed. Marcial Pons, 2010; AYALA, J. E., "Lisboa, por fin: el tratado abre una nueva era en la UE", en *Política exterior 24*, nº 133 (2010), pp. 13-20; D'ATENA, A., "La Constitución oculta de Europa (antes y después de Lisboa)", en *Revista de derecho constitucional europeo*, nº 13 (2010), pp. 17-46; DE LA IGLESIA GARCÍA, J., "La entrada en vigor del Tratado de Lisboa", en *Revista Universitaria Europea*, nº 12 (2010), pp. 45-60; MILLÁN MORO, L., "El ordenamiento jurídico comunitario: del Tratado Constitucional al Tratado de Lisboa", en *Revista de Derecho Comunitario Europeo*, nº 36 (2010), pp. 401-438.

de datos de carácter personal en el contexto comunitario[149], reforzando así las bases existentes sobre la materia y superando ciertas restricciones que habían sido introducidas por la Directiva 95/46/CE. De esta manera, el literal de su primer apartado se constituye como toda una declaración de intenciones sobre los objetivos pretendidos, al circunscribir que: "[T]oda persona tiene derecho a la protección de los datos de carácter personal que le conciernan".

Asimismo, en su apartado segundo, se incluye un mandato de desarrollo normativo, estableciendo que: "[E]l Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes. Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea".[150]

Y, por otro lado, la supresión de la tradicional estructura de pilares comunitarios que constaba instaurada como consecuencia de la entrada en vigor del Tratado de Maastricht en 1992[151], complementada con los cambios normativos efectuados por la

[149] La categorización del derecho a la protección de datos tanto de carácter personal como fundamental debe entenderse como un hito sustancial en la propia regulación comunitaria, así como en cada uno de los respectivos ordenamientos jurídicos de los Estados Miembros. *Vid*. GONZÁLEZ FUSTER, G., *"The Emergence of Personal Data Protection as a Fundamental Right of the EU"*, Suiza: Ed. Springer, 2014, pp. 163-205.

[150] Este artículo debe entenderse en consonancia con el contenido preceptuado por el artículo 39 del Tratado de la Unión (TUE), toda vez que sustituyen al antiguo artículo 286 del Tratado Constitutivo de la Comunidad Europea. A este respecto, el referido artículo 39 del TUE reza el tenor literal siguiente: "[d]e conformidad con el artículo 16 del Tratado de Funcionamiento de la Unión Europea y, no obstante lo dispuesto en su apartado 2, el Consejo adoptará una decisión que fije las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del presente capítulo, y sobre la libre circulación de dichos datos. El respeto de dichas normas estará sometido al control de autoridades independientes".

[151] El Tratado de Maastricht, en su momento, supuso la creación de una nueva división de competencias institucionales dentro de la estructura de la Unión Europea, acuñada bajo la popular denominación de "pilares". El primero de ellos se componía por la Comunidad Europea, la Comunidad Europea del Carbón y del Acero (CECA) y la Comunidad Europea de la Energía Atómica (Euratom), organismos encargados de gestionar los asuntos internacionales y comunitarios. El segundo y el tercero los encontramos en la

Directiva 95/46/CE, vino a configurar un nuevo escenario regulatorio que redundaría en fortalecer el carácter fundamental del derecho a la protección de datos de carácter personal. Así como también permitiría ampliar el alcance de la legislación reguladora de este derecho a otros ámbitos, como el policial y judicial[152].

Como señala Troncoso Raigada, resulta esencial 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, reforzando las bases jurídicas específicas para que la Unión Europea apruebe una normativa sobre protección de datos personales aplicable a todos los ámbitos, suprimiendo las limitaciones establecidas en la Directiva[153].

Como muestra de lo apuntado, conviene señalar la importancia del contenido que se preceptúa en las Declaraciones nº 20 y 21, respectivamente, las cuales forman parte del Tratado de Lisboa analizado. La primera de ellas reza el literal siguiente: "[L]a 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

Política Exterior y de Seguridad Común (PESC) y la Cooperación Policial y Judicial en Materia Penal (CPJP), respectivamente, como parte de los mecanismos de colaboración existentes entre los distintos Estados Miembros de la Unión Europea.

[152] En relación con la evolución del derecho a la protección de carácter personal hasta su actual percepción, *vid*., entre otros: PIÑAR MAÑAS, J. L., "El derecho a la protección de datos…", *op. cit*., pp. 89-109; ARENAS RAMIRO, M., "La protección de datos personales en los países de la Unión Europea", en *Revista jurídica de Castilla y León*, nº 16 (2008), pp. 113-168; TRONCOSO REIGADA, A., *La protección de datos…*, *op. cit*., pp. 45-95; MATÍA PORTILLA, F. J., "Los derechos fundamentales de la Unión Europea en tránsito: de Niza a Lisboa, pasando por Bruselas", en *Revista Española de Derecho Europeo*, nº 39 (2011), Westlaw-Aranzadi, pp. 1-17; SOLAR CALVO, M. P., "La protección de datos en la Unión Europea: análisis y perspectivas de futuro", en *Revista Aranzadi Unión Europea*, nº 2 (2012), p. 8: "[e]n el mismo sentido, destaca el haber otorgado carácter de derecho fundamental a la protección de datos personales en el artículo 8 del Tratado constitutivo y su inclusión dentro del proyecto de Constitución Europea".

[153] *Cfr*. TRONCOSO REIGADA, A., "Hacia un nuevo marco jurídico…", *op. cit*., p. 6.

aplicable (véase, en particular, la Directiva 95/46/CE) contiene excepciones específicas a este respecto"[154].

A su vez, la segunda de las declaraciones aludidas dispone que: "[L]a 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, debido a la naturaleza específica de dichos ámbitos."[155]

En definitiva, resulta preciso traer a colación que los países que formaban la Convención para la elaboración de la Carta de Derechos Fundamentales de la Unión Europea no habían llegado a una unanimidad sobre el carácter vinculante de esta, pues las posiciones se dividían entre aquellos países que pretendían dotarla de plena eficacia con su integración en los textos comunitarios y aquellos otros territorios que no querían dotarla de fuerza vinculante. Pero este escenario descrito cambió radicalmente cuando se produjo la adopción del Tratado de Lisboa, dado que la Carta pasa a ser plenamente aplicable sobre aquellos Estados miembros que han ratificado el acuerdo[156].

---

[154] *Cfr*. Declaración nº 20 relativa al artículo 16 del Tratado de Funcionamiento de la Unión Europea. Consultado el 12.07.2020 desde: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0005.02/DOC_5&format=PDF.

[155] *Cfr*. 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. Consultado el 12.07.2020 desde: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0005.02/DOC_5&format=PDF.

[156] *Vid*., entre otros: ALONSO GARCÍA, R., "La Carta de los derechos fundamentales…", *op. cit.*, pp. 3-11; PACE, A., "¿Para qué sirve la Carta de Derechos Fundamentales de la Unión Europea?", en *Teoría y Realidad Constitucional*, nº 7 (2001), p. 174; CARRILLO SALCEDO, J. A., "Notas sobre el significado…", *op. cit.*, p. 20; RODRÍGUEZ BEREIJO, A. y GARCÍA DE ENTERRÍA, E., "El valor jurídico de la Carta de los Derechos Fundamentales de la Unión Europea después del Tratado de Niza", en GARCÍA DE ENTERRÍA, E. y ALONSO GARCÍA, R. (Dirs.), *La encrucijada constitucional de la Unión Europea*, Madrid: Ed. Civitas, 2002, p. 210; RUBIO LLORENTE, F., "Mostrar los derechos sin destruir la Unión", en *Revista Española de Derecho Constitucional*, nº 64 (2002), pp. 13-22; ALONSO GARCÍA, R., "Las cláusulas horizontales de la Carta de los derechos Fundamentales de la Unión Europea", en GARCÍA DE ENTERRÍA, E. y ALONSO GARCÍA, R. (Dirs.), *La encrucijada constitucional de la Unión Europea*, Madrid: Ed. Civitas, 2002, pp. 151-210; ARZOZ SANTISTEBAN, X., "La relevancia del Derecho de la Unión Europea para la interpretación de los derechos fundamentales constitucionales", en *Revista Española de Derecho Constitucional*, nº 74 (2005), pp. 63-74; CARRERA, S. y GEYER, F., "El Tratado de Lisboa y un Espacio de Libertad, Seguridad y Justicia: Excepcionalismo y Fragmentación en la Unión Europea", en *Revista de Derecho Comunitario Europeo*, nº 29 (2008), pp. 133-162.

A este respecto, Díez Picazo sostiene que los derechos fundamentales están en el centro de sustentación de la legitimidad democrática de los Estados constitucionales y, en consecuencia, no resultaba entendible ni justificable que una organización superior a la que se someten los nacionales de los Estados miembros no incorporase una declaración de derechos en sus textos constitutivos, pues si la Comunidad quiere legitimarse a través de un auténtico contrato social de los europeos, ese pacto habrá de basarse en el previo reconocimiento de los derechos fundamentales de los ciudadanos, de suerte que estos no pierdan, al entrar en una organización superior, lo que trabajosamente han conseguido en sus respectivos Estados[157].

[157] *Cfr*. DÍEZ PICAZO, L. M., "¿Una Constitución sin…", *op. cit.*, pp. 147-155.

2. Perspectiva histórica del derecho a la protección de datos en España

2.1. Situación contextual y doctrinal

El estudio de la materia no puede proseguir sin analizar la evolución histórica del derecho a la protección de datos de carácter personal partiendo de las disposiciones contenidas en la Constitución española de 1978. Para ello, se expondrán las principales posiciones doctrinales que se pronunciaron sobre su interpretación, así como también se analizará la jurisprudencia que gradualmente fue configurando la categorización que en la actualidad le asignamos a este derecho con rango constitucional[158].

Antes de iniciar el análisis, cabe remarcar contextualmente que los rápidos avances tecnológicos sucedidos con posterioridad a la finalización de la Segunda Guerra Mundial, sumado a la obligación cada vez más imperante de gestionar grandes volúmenes de información de una manera estructurada[159] —sobre todo por parte de las administraciones públicas respecto de sus administrados—[160], motivan progresivamente la necesidad de ofrecer una mayor tutela en la esfera privada y personal de los ciudadanos. Dicha tesitura pretendió solventarse mediante la consagración de un derecho que ofreciese amparo suficiente frente a posibles abusos arbitrarios que pudieran producirse respecto de este bien jurídico protegido. Como bien indica Serrano Pérez, este nuevo derecho del constitucionalismo democrático contemporáneo ha adquirido una creciente importancia, reconociéndose, por ejemplo, en España, como derecho fundamental en el art. 18.4 de la Constitución española[161].

---

[158] Para una perspectiva histórica detallada sobre la evolución del derecho a la protección de datos. *Vid*., entre otros: PÉREZ LUÑO, A. E., "Informática y Libertad. Comentario al artículo 18.4 de la Constitución española", en *Revista de Estudios Políticos (Nueva Época)*, nº 24 (1981), pp. 33-41; RUIZ MIGUEL, C., *La Configuración Constitucional del Derecho a la Intimidad*, Madrid: Ed. Tecnos, 1995; MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica…*, *op. cit.*, p. 61-69.

[159] *Vid*. VALERO TORRIJOS, J., "De la digitalización a la innovación tecnológica: valoración jurídica del proceso de modernización de las administraciones públicas españolas en la última década (2004-2014)", en *Revista de los Estudios de Derecho y Ciencia Política*, nº 19 (2014), pp. 117-126.

[160] *Vid*. ROVIRA FERRER, I., "La Administración electrónica tributaria: implantación y respuesta ciudadana", en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 17 (2008), Westlaw-Aranzadi, pp. 1-3; ARIZMENDI GUTIÉRREZ, M. E., "El cumplimiento de la normativa de protección de datos en el sector público: Protección de datos y Administración electrónica. El cumplimiento de la normativa de protección de datos en la administración electrónica", en VV.AA., *20 años de protección de datos en España*, Madrid: Ed. Agencia Española de Protección de Datos, 2015, p. 235.

[161] *Vid*., entre otros: SERRANO PÉREZ, M. M., *El derecho fundamental…*, *op. cit.*, p. 75. En el mismo sentido, PÉREZ LUÑO, A. E., *Manual de Informática y Derecho*, Barcelona: Ed. Ariel, 1996, p. 45;

En este contexto, que se ve influenciado en gran medida por las doctrinas alemana e italiana, que ya habían tenido la oportunidad de pronunciarse sobre el contenido y las posibles interpretaciones del derecho a la protección de los datos de carácter personal en el entorno comunitario[162], se produce el sustrato necesario que favorece la aparición de ciertas corrientes doctrinales en España que abordan el origen del contenido y el alcance de este derecho vinculado al ámbito de la intimidad, las cuales se tratarán de manera diferenciada a la luz las consideraciones de dos magistrados, uno perteneciente al Tribunal Supremo y otro al Tribunal Constitucional.

No obstante lo anterior, conviene reproducir la distinción que la ya derogada Ley Orgánica 5/1992[163] (en adelante, LORTAD) contenía en el apartado primero de su Exposición de motivos, mediante el tenor literal siguiente: "[n]ótese que se habla de la privacidad y no de la intimidad: Aquella es más amplia que esta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona —el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo—, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan

ALONSO GARCÍA, R., "Constitución española y Constitución europea: guion para una colisión virtual y otros matices sobre el principio de primacía", en *Revista Española de Derecho Constitucional*, nº 73 (2005), pp. 339-343.

[162] No debemos olvidar, en todo caso, que la totalidad de las iniciativas legislativas que se produjeron en el entorno comunitario vinieron propiciadas en su inmensa mayoría por la creciente importancia de la que las instituciones europeas estaban dotando al derecho a la protección de datos; concretamente, uno de los mayores exponentes de lo aquí afirmado se materializa con la adopción del Convenio 108, que hemos tenido la oportunidad de abordar brevemente en los anteriores apartados del presente análisis.

[163] España. Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Consultado el 12.07.2020 desde: https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189. Para una revisión histórica sobre el contenido de la LORTAD y su influencia en materia de protección de datos de carácter personal. *Vid*., entre otros: LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales*, Madrid: Ed. CEC, 1993, pp. 64-69; VILLAVERDE MENENDEZ, I., "Protección de datos personales…", *op. cit.*, pp. 187-224; VIZCAÍNO CALDERÓN, M., *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid: Ed. Civitas, 2001; APARICIO SALOM, J., *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Cizur Menor (Navarra): Ed. Aranzadi, 2002, pp. 57-59, 109-119; CARRILLO LÓPEZ, M., *El derecho a no ser molestado. Información y vida privada*, Cizur Menor (Navarra): Ed. Thomson-Aranzadi, 2003, pp. 91-101; GUICHOT, E., *Datos personales y Administración Pública*, Madrid: Ed. Civitas, 2005, pp. 226-234; GUERRERO PICÓ, M. C., *El Impacto de Internet en…*, *op. cit.*, pp. 237-248; PÉREZ LUÑO, A. E., *La tercera generación de derechos humanos*, Cizur Menor (Navarra): Ed. Thomson-Aranzadi, 2006, pp. 31-32.

como precipitado un retrato de la personalidad del individuo que este tiene derecho a mantener reservado"[164].

Sobre la cuestión, Espín Templado señala que: "[n]o obstante, el derecho a la privacidad y el derecho a la intimidad no son idénticos ni protegen el mismo interés jurídico. Si analizamos las lenguas de los países occidentales observamos que en todas existen palabras distintas para expresar la intimidad y privacidad, salvo en la lengua inglesa, que, a pesar de tenerlas, se ha decantado por privacidad. Así, en alemán se diferencia entre "*intimität*" y "*Privat Leben*"; en francés, entre "*intimité*" y "*vie privée*"; en italiano, entre "*intimitá*" y "*riservatezza*"; y en inglés, entre "*intimity*" y "*privacy*"[165].

En consecuencia, uno de los principales efectos que se producen a tenor de lo expuesto hasta el momento radica en la aprobación de la Constitución española de 1978[166] (en adelante, CE), que, pese a no contener expresamente ningún precepto que preste una atención específica sobre el derecho a la protección de datos de carácter personal, su artículo 18 propicia una clara unidad de protección sobre la esfera más íntima de la persona. Dicho precepto regula los derechos fundamentales relativos a la inviolabilidad del domicilio, al secreto de las comunicaciones, a la protección de la intimidad personal y familiar, a la propia imagen y al honor. Conviene detenerse para hacer hincapié sobre el contenido del último de los derechos aludidos[167].

---

[164] *Cfr*. TRONCOSO REIGADA, A., *La protección de datos…*, *op. cit*., p. 66.

[165] *Cfr*. ESPÍN TEMPLADO, E., "Los derechos de la esfera personal", en *Derecho Constitucional, Vol. I*, Valencia: Ed. Tirant lo Blanch, 1994, p. 208.

[166] Para una perspectiva sobre el proceso constituyente de 1978, ante la basta bibliografía existente, *vid*., entre otros: TOMÁS Y VALIENTE, F., "La Constitución de 1978 y la historia del constitucionalismo español", en *Anuario de Historia del Derecho Español*, Madrid, 1980, pp. 721-751; FERNÁNDEZ-MIRANDA LOZANA, P., "Bibliografía sobre la transición política española", en *Revista de derecho político*, nº 42 (1996), pp. 213-223; ÁLVAREZ ALONSO, C., "Los derechos y sus garantías (1812-1931)", en *Ayer*, nº 34 (1999), pp. 177-216; JIMÉNEZ ASENSIO, R., *El Constitucionalismo: proceso de formación y fundamentos del derecho constitucional*, Madrid: Ed. Marcial Pons, 2005; RUBIO LLORENTE, F., *La forma del poder. Estudio sobre la constitución*, Madrid: Ed. Centro de Estudios Políticos y Constitucionales, 2013, pp. 5-41.

[167] *Vid*. CASTÁN TOBEÑAS, J., "Los derechos de la personalidad", en *Revista General de Legislación y Jurisprudencia*, nº julio-agosto (1952), pp. 5-62; DE CASTRO Y BRAVO, F., "Los llamados derechos de la personalidad", en *Anuario de Derecho Civil*, nº 4, 1959, pp. 1237-1275; PARDO FALCÓN, J., "Los derechos del art. 18 de la Constitución española en la jurisprudencia del Tribunal Constitucional", en *Revista Española de Derecho Constitucional*, nº 34 (1992), pp. 141-178; MEDINA GUERRERO, M., "La articulación de las jurisdicciones constitucional y ordinaria en la tutela de las libertades de expresión e información", en VV. AA., *La democracia constitucional: estudios en homenaje al profesor Rubio Llorente*, Vol. II, Madrid: Ed. Centro de Estudios Políticos y Constitucionales, 2002, pp. 1669-1700.

El contenido del artículo 18.4 de la CE, situado en la *Sección 1.ª De los derechos fundamentales y de las libertades públicas*, dispone que: "[l]a ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". En este literal se advierte sobre cómo confluyen en su redacción y contenido manifestaciones propias de otros derechos fundamentales colindantes en la CE, como el derecho a la integridad moral[168] o el derecho a la dignidad humana y el libre desarrollo de la personalidad[169]. Pero, en todo caso, lo que deja claramente estipulado su redactado radica en la necesidad de establecer límites al uso de la informática, siendo consciente el legislador del momento[170] de los peligros que la misma podía entrañar para los derechos y libertades de los afectados[171].

En cualquier caso, la CE se constituyó como uno de los primerizos textos normativos comunitarios —con rango constitucional—[172] que abordaba las preocupaciones derivadas del uso masivo de los datos personales a través de las nuevas realidades tecnológicas derivadas del avance de la informática. Si bien es cierto que no supo delimitar claramente el bien jurídico protegido a través del artículo 18.4 de la CE que se viene analizado, dado que adolecía de ciertas lagunas en su redactado, tal y como tuvo la oportunidad de señalar también Troncoso Reigada[173], posibilitando así que su labor interpretativa recayera, en primera instancia, en manos de la doctrina científica.

La doctrina científica que surge a tenor de la interpretación teleológica realizada sobre este precepto se estructura a través de dos líneas conceptuales diferenciadas, esto es, la autodeterminación informativa y la libertad informática. Pese a tratarse de concepciones que coinciden en partir de la premisa que la construcción de este nuevo

---

[168] *Vid*. ÁLVAREZ CONDE, E., *Curso de Derecho Constitucional I*, Madrid: Ed. Tecnos, 2006, pp. 385-389.

[169] *Vid*. DEL CASTILLO VÁZQUEZ, I. C., *Protección de datos: cuestiones constitucionales y administrativas: el derecho a saber y la obligación de callar*, Madrid: Ed. Civitas, 2007, pp. 136-139; ÁLVAREZ CONDE, E., "Curso de…", *op. cit.*, pp. 356-360.

[170] *Vid*. LUCAS MURILLO DE LA CUEVA, P., *El derecho a…*, *op. cit.*, pp. 150-158.

[171] *Cfr*. TRONCOSO REIGADA, A., *La protección de datos…*, *op. cit.*, pp. 66-67.

[172] El primero de los textos normativos que aborda estas cuestiones lo encontramos en Portugal; pero al contrario de lo que sucede con el caso español, el texto portugués detalla con mayor alcance las preocupaciones derivadas del uso de la informática en lo relativo a los datos de carácter personal de los afectados.

[173] *Cfr*. TRONCOSO REIGADA, A., *La protección de datos…*, *op. cit.*, p. 68.

derecho debe abordarse más allá de las vicisitudes propias del derecho a la intimidad, conviene que ambas se interpreten de manera particularizada para comprender con mayor exactitud su magnitud y alcance.

El primero de los conceptos aludidos tiene su origen en la doctrina y jurisprudencia sentada en Alemania que se ha tenido la oportunidad de analizar con anterioridad. En España será acogida a través de los pronunciamientos efectuados por Lucas Murillo de la Cueva[174], quien se encarga de adecuar la jurisprudencia emanada del Tribunal Constitucional Federal alemán al ordenamiento jurídico español. Dicha labor se efectúa teniendo en cuenta tanto las consideraciones vertidas a lo largo del artículo 18 de la CE como los principios consagrados en el artículo 10 de la misma Norma, relativos al respeto de la dignidad humana y al libre desarrollo de la personalidad.[175]

El presente autor, alejándose de la interpretación literal del precepto contenido en el artículo 18.4 de la CE, realiza una vinculación directa con los avances sucedidos en el ámbito de la informática y las nuevas tecnologías para encontrar el sustrato jurídico de lo que vendría a denominar "teoría de la autodeterminación informativa"[176]. A este respecto, señala el referido autor que: "En cuanto posición jurídica subjetiva correspondiente al *status* de *habeas data*, pretende satisfacer la necesidad, sentida por las personas en las condiciones actuales de la vida social, de preservar su identidad controlando la revelación y el uso de los datos que les conciernen y protegiéndose frente a la ilimitada capacidad de archivarlos, relacionarnos y transmitirlos propia de la informática y de los peligros que esto supone"[177].

---

[174] Pablo Lucas Murillo de la Cueva fue magistrado del Tribunal Supremo y profesor titular de Derecho constitucional. Entre las principales obras de este autor centradas en la teoría de la autodeterminación informativa, *Vid.*, entre otros: LUCAS MURILLO DE LA CUEVA, P., *Informática y protección…*, *op. cit.*; LUCAS MURILLO DE LA CUEVA, P., "Las vicisitudes del Derecho de la protección de datos personales", en *Revista Vasca de Administración Pública*, nº 58-II (2000), pp. 211-219; LUCAS MURILLO DE LA CUEVA, P., "La Constitución y el derecho a la autodeterminación informativa", en *Cuadernos de Derecho Público*, nº 19-20 (2003), pp. 27-32; LUCAS MURILLO DE LA CUEVA, P., "Perspectivas del derecho a la autodeterminación informativa", en *Revista de Internet, Derecho y Política*, nº 5 (2007); LUCAS MURILLO DE LA CUEVA, P., "La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad", en *El derecho a la autodeterminación informativa*, Madrid: Ed. Fundación Coloquio Jurídico Europeo, 2009, pp. 11-80.

[175] *Cfr*. LUCAS MURILLO DE LA CUEVA, P., *El derecho a…*, *op. cit.*, p. 29.

[176] *Ibidem*, p. 30.

[177] *Ibidem*, pp. 173-175.

Sigue afirmando que se puede alcanzar el objetivo pretendido: "Por medio de lo que se denomina técnica de protección de datos, integrada por un conjunto de derechos subjetivos, deberes, procedimientos, instituciones y reglas objetivas. El individuo que se beneficia de la misma adquiere así una situación que le permite definir la intensidad con que desea que se conozcan y circulen su identidad y circunstancias, combatir las inexactitudes o falsedades que las alteren y defenderse de cualquier utilización abusiva, desleal o, simplemente, ilegal que pretenda hacerse de las mismas"[178].

De este modo, la teoría defendida por Lucas Murillo de la Cueva vino a entenderse como la proyección de un derecho fundamental del que disponía cada afectado que le permitiría ejercer un poder de control sobre aquellos datos personales que le concernían específicamente, ya fueren íntimos o públicos, que le posibilitarían, a través del libre desarrollo de su personalidad, construirse una identidad propia y libre amparada constitucionalmente[179].

El segundo de los conceptos aludidos tiene su origen en la doctrina emanada de Italia, pues fue la primera que tomó en consideración el derecho a la protección de datos vinculado a la propia libertad individual. Los movimientos doctrinales italianos habían optado por definir la teoría de la libertad informática como el derecho del interesado a controlar aquella información que le concierne, almacenada en dispositivos digitales, que dificultan su libertad de actuación y facilitan el acceso, rectificación o cancelación de la información en ellos almacenada, tal y como señala Troncoso Reigada[180].

Este movimiento en España tiene su máximo exponente en Pérez Luño[181], quien se encarga de adecuar la doctrina emanada de los textos constitucionales italianos al

---

[178] *Ibidem.*

[179] *Vid*. LUCAS MURILLO, P., *Informática y protección…*, *op. cit.*, pp. 32-33; SERRANO PÉREZ, M. M. *El derecho fundamental…*, *op. cit.*, p. 78.

[180] *Cfr*. TRONCOSO REIGADA, A., *La protección de datos…*, *op. cit.*, p. 51, en la que cita la doctrina italiana clásica más relevante: PIZZORUSSO, A., "Sul diritto alla riservatezza nella Costituzione italiana", en *Prassi e teoría*, 1976.

[181] Antonio Enrique Pérez Luño fue magistrado del Tribunal Constitucional. Entre las principales obras de este autor centradas en la teoría de la libertad informática. *Vid*., entre otros: PÉREZ LUÑO, A. E., "La juscibernética en España", en *Revista jurídica de Catalunya*, nº 2 (1972), pp. 303-310; PÉREZ LUÑO, A. E., *Cibernética, informática y derecho. Un análisis metodológico*, Bolonia: Ed. Publicaciones del Real Colegio de España, 1976, pp. 133-142; PÉREZ LUÑO, A. E., "La protección de la intimidad frente a la informática en la Constitución española de 1978", en *Revista de Estudios Políticos (Nueva Época)*, nº 9 (1979), pp. 73-79; PÉREZ LUÑO, A. E., *Problemas actuales de la documentación y la informática*

ordenamiento jurídico español. A diferencia de lo sentado por el autor citado con anterioridad respecto a la teoría de la autodeterminación informativa, este manifiesta la necesidad de fundamentar su teoría en torno al concepto de la libertad informática. Dicha concepción parece, *a priori*, totalmente distanciada de la mantenida por Lucas Murillo de la Cueva, pero en muchas ocasiones ambos postulados coinciden, resultando incluso complementarios entre sí.

A este respecto, Pérez Luño señala que: "Negar la autonomía del derecho a la autodeterminación informativa para englobarlo en el derecho al libre desarrollo de la personalidad, dificultaría la relación directa de aquel con otros derechos fundamentales"[182]. Adicionalmente, añade que: "Para garantizar la libertad informática —equiparada a la autodeterminación informativa— conviene, por tanto, concebirla como un derecho fundamental autónomo dotado de medios específicos de tutela. Por el contrario, disuelta en el ámbito de otros valores o derechos la autodeterminación informativa, corre el riesgo de relativizarse y ver comprometida su efectiva realización"[183].

En consecuencia, se puede entender la libertad informática como aquella concepción que, alejándose de los valores propios del derecho a la intimidad, se consagra como un nuevo derecho fundamental en que quedan incluidos otros derechos colindantes que complementan su contenido como la dignidad y la libertad[184]. Asimismo, el autor afirma que: "[e]l *habeas corpus* y el *habeas data* representan, además, dos garantías procesales de aspectos diferentes de la libertad. Así, mientras el primero se circunscribe a la dimensión física y externa de la libertad, el segundo tiende a proteger prioritariamente

jurídica: actas del coloquio internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986, Madrid: Ed. Fundación Cultural Enrique Luño Peña, 1987, pp. 268-276; PÉREZ LUÑO, A. E., LOSANO, M. y GUERRERO MATEUS, M. F., *Libertad informática y leyes de protección de datos personales*, Madrid: Ed. Centro de estudios constitucionales, 1989; PÉREZ LUÑO, A. E., "La protección de los datos personales del menor en Internet", en *Anuario de la Facultad de Derecho (Universidad de Alcalá)*, nº 2 (2009), pp. 143-175; PÉREZ LUÑO, A. E., *Derechos humanos, estado de derecho y Constitución*, Madrid: Ed. Tecnos, 2005, pp. 378-385; PÉREZ LUÑO, A. E., "El consentimiento de los menores: Título II. Principios de la Protección de Datos. artículo 6", en TRONCOSO REIGADA, A. (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid: Civitas, 2010, pp. 473-494.

[182] *Cfr*. PÉREZ LUÑO, A. E., *El derecho a la autodeterminación…*, *op. cit.*, pp. 326-329.

[183] *Ibidem.*

[184] *Vid*. PÉREZ LUÑO, A. E., "La protección de la intimidad frente…", *op. cit.*, pp. 59-72.

aspectos internos de la libertad: la identidad de la persona, su autodeterminación, su intimidad".[185]

Resulta oportuno señalar que las teorías que venimos exponiendo no han estado exentas de críticas, pues autores como Denninger han destacado que no se trata de ningún derecho fundamental nuevo propiciado por el Tribunal Federal alemán, sino del resultado de una corriente jurisprudencial vinculada al libre desarrollo de la personalidad[186]. Otros autores también han alertado sobre el riesgo que esta concepción puede conllevar, al entender el control de los datos como un derecho de propiedad sobre los mismos[187].

Por lo tanto, se puede concluir afirmando que la doctrina mayoritaria ha venido a reconocer que ambas teorías expuestas se hallarían incluidas bajo el origen de la institución de protección de datos personales[188], cuyo fin imperioso redundaría en "garantizar la facultad de las personas para conocer y acceder a las informaciones que les conciernen archivadas en bancos de datos (lo que se denomina *habeas data* por su función análoga en el ámbito de la información por cuanto supuso el tradicional *habeas corpus* en lo referente a la libertad personal), controlar su calidad (lo que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados) y disponer sobre su transmisión"[189].

No obstante, conviene recordar que el ordenamiento jurídico español acoge esta institución basada en la protección de datos diferenciada de la intimidad, pues esta última no permite ninguna facultad de control sobre la información personal, aunque los datos resulten estrechamente vinculados con la esfera íntima del afectado[190], pudiendo sostener —como indica Pérez Luño[191]— que la intimidad no es nada más que un aspecto concreto

---

185 *Vid*. PÉREZ LUÑO, A. E., "Del habeas corpus al habeas data", en *Informática y derecho: Revista iberoamericana de derecho informático*, nº 1 (1992), p. 162.

186 *Vid*. DENNINGER, E., "El derecho a la autodeterminación informativa", en PÉREZ LUÑO, A. E. (Coord.), *Problemas actuales de la documentación…*, *op. cit.*, p. 273.

187 *Cfr*. SERRANO PÉREZ, M. M., *El derecho fundamental a la…*, *op. cit.*, p. 69.

188 *Vid*. SERRANO PÉREZ, M. M., *El derecho fundamental a la…*, *op. cit.*, p. 76.

189 *Cfr*. PÉREZ LUÑO, A. E., "El derecho a la autodeterminación…", *op. cit.*, pp. 304.

190 *Vid*. LUCAS MURILLO DE LA CUEVA, P., *El derecho a…*, *op. cit.*, pp. 97-98.

191 *Vid*. PÉREZ LUÑO, A. E., "Informática jurídica y derecho de la informática en España", en *Informatica e Diritto*, nº 2 (1983), pp. 93-95.

de la libertad, no pudiendo dar cabida a los riesgos tecnológicos que se derivan de los nuevos escenarios surgidos como consecuencia del uso de las nuevas tecnologías[192].

2.2. Evolución jurisprudencial

Una vez esbozada la situación doctrinal existente en España por lo que al origen del derecho a la protección de los datos de carácter personal se refiere[193], conviene tener presente que las primeras aportaciones se producen de manera coetánea con la entrada en vigor de la Constitución española[194]. Uno de los órganos que toma en consideración las distintas teorías doctrinales que se habían suscitado mediante sus diversos pronunciamientos es el Tribunal Constitucional[195], cuya labor jurisprudencial ha

---

[192] *Vid*. LUCAS MURILLO DE LA CUEVA, P., *El derecho a…*, *op. cit.*, pp. 98-99.

[193] Adicionalmente, sobre la necesidad de dotar al derecho de protección de datos de carácter personal de autonomía y contenido propio, *vid.*, entre otros: LUCAS MURILLO DE LA CUEVA, P., *El derecho a…*, *op. cit.*, pp. 43-58; LUCAS MURILLO DE LA CUEVA, P., "La Constitución y el derecho a la autodeterminación informativa", en *Cuadernos de Derecho Público*, nº 19-20 (2003), pp. 27-44; CONDE ORTÍZ, C., *La protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad*, Madrid: Ed. Dykinson-UCA, 2005, pp. 40-47; ARENAS RAMIRO, M., *El derecho fundamental…*, *op. cit.*, pp. 444-458; LESMES SERRANO, C., *La ley de protección de datos. Análisis y comentario de su jurisprudencia*, Valladolid: Ed. Lex Nova, 2007, pp. 50-58; BUENO GALLARDO, E., *La configuración constitucional del derecho a la intimidad. En particular, el derecho a la intimidad de los obligados tributarios*, Madrid: Ed. Centro de Estudios Políticos y Constitucionales, 2009, pp. 424-434; CASAS BAAMONDE, M. E., "El derecho a la Protección de Datos de carácter personal en la Jurisprudencia del Tribunal Constitucional", en VV. AA., *20 años de protección de datos en España*, Madrid: Ed. Agencia Española de Protección de Datos, 2015, pp. 91-129. Ahora bien, esta doctrina difiere en algunos aspectos puesto que se defienden distintas concepciones sobre el alcance del bien jurídico protegido en materia de protección de datos de carácter personal.

[194] Al respecto, cabe advertir que hasta la entrada en vigor de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (en adelante, "LORTAD"), no se aborda la cuestión de manera específica, pues como Lucas Murillo de la Cueva señala: "[L]o anterior llama la atención toda vez que en el ámbito supranacional europeo en el Consejo de Europa ya se había aprobado el Convenio nº 108, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, que establecía los principios esenciales sobre los que descansa este derecho". Adicionalmente apunta que: "La actitud tomada por los Tribunales españoles, los que, no obstante la fórmula abierta y transversal con que se redactó el artículo 18.4 de la constitución española, que facilitaba la recepción y desarrollo del citado Convenio, le negaron valor al mismo para sustentar derechos, al considerar que este se limitaba a consagrar principios que debían concretar los legisladores nacionales, sus únicos destinatarios". *Cfr*. "La construcción del derecho…", *op. cit.*, p. 20.

[195] Sobre la jurisprudencia del Tribunal Constitucional en materia de protección de datos personales, existe una abundante bibliografía. *Vid.*, entre otros: QUILEZA AGRADA, E., "El derecho a la protección de los datos en la jurisprudencia constitucional", en DAVARA RODRÍGUEZ, A. (Coord.), *III Jornadas sobre informática y sociedad*, Madrid, 2001, pp. 187-196; HERRÁN ORTIZ, A. I., "La protección de datos personales en la jurisprudencia constitucional", en ECHANO BASALDÚA, J. I. (Coord.), *Estudios jurídicos en memoria de José María Lidón*, Universidad de Deusto, 2002, pp. 985-1000; TRONCOSO REIGADA, A., "La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional", en *Cuadernos de Derecho Público*, nº 19-20 (2003), pp. 231-334; VILLAVERDE

resultado esencial para ir consagrando el rango fundamental del que goza este derecho en la actualidad.

Como preludio de su labor de interpretación, cabe recordar en primera instancia la Sentencia del Tribunal Constitucional nº 110/1984, de 26 de noviembre[196], que viene a poner de manifiesto las constantes preocupaciones que se habían venido sufragando, tanto en el ámbito regulatorio comunitario como a nivel doctrinal, respecto de los nuevos escenarios tecnológicos que se estaban planteando y los riesgos que estos podían entrañar respecto de la protección de los datos personales de los interesados.

Concretamente, en el contenido de dicha Sentencia se aborda la dicotomía existente entre la contribución al erario público y las posibles implicaciones respecto a la protección del derecho fundamental a la intimidad mediante el siguiente tenor literal: "[e]l reconocimiento explícito en un texto constitucional del derecho a la intimidad es muy reciente y se encuentra en muy pocas Constituciones, entre ellas la española.[…] Lo ocurrido es que el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida"[197].

Durante la década de 1980 del pasado siglo XX, la jurisprudencia del Alto Tribunal español fue uniforme al vincular el derecho a la protección de los datos personales (limitación a la informática) como una vertiente propia del derecho a la intimidad, excluyéndolo de la disposición de un ámbito propio de autonomía. Dicha interpretación será parcialmente acogida por las Sentencias posteriores nº 254/1993, de 20 de julio; nº 143/1994, de 9 de mayo, y nº 110/1999, de 14 de junio, entre otras de la Corte

MENÉNDEZ, I., "La jurisprudencia del Tribunal Constitucional sobre el derecho fundamental a la protección de datos de carácter personal", en FARRIOLS I SOLÁ, A. (Coord.), *La protección de datos de carácter personal en los centros de trabajo*, 2006, pp. 48-63.

[196] *Vid*. Sentencia del Tribunal Constitucional nº 110/1984, de 26 de noviembre, relativa a un supuesto fáctico en que se debate una cuestión de índole tributaria. Consultado el 12.07.2020 desde: http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/363.

[197] *Cfr*. Fundamento jurídico 2º de la STC nº 110/1984, de 26 de noviembre.

constitucional, en un ejercicio de intentar consolidar dicha interpretación en el marco del artículo 18.4 de la CE.

No obstante lo anterior, cabe apuntar que la STC nº 254/1993, de 20 de julio, que se ha abordado con anterioridad se distancia del contenido preceptuado por la jurisprudencia citada en el párrafo anterior[198]. Se trata de la primera que reconoce —sin pronunciarse expresamente al respecto sobre su contenido—[199] un haz de facultades para el afectado que, dimanantes del contenido del derecho a la intimidad, le posibilitarían disponer del control sobre sus datos personales basándose en la tesis de la libertad informática que con anterioridad hemos tenido la oportunidad de abordar[200].

A este respecto, la STC referida contempla el literal siguiente: "[…] La garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es, así, también, el derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*)"[201]. Todo ello para venir a reconocer finalmente en su fallo una aplicación automática de los derechos fundamentales, sin que resulte preciso un previo detalle normativo habilitante, más allá del recogido en la propia CE[202].

Como manifiesta González Murúa, "[p]ara el Tribunal Constitucional, sin embargo, el derecho de la intimidad no se agota en unas facultades negativas, sino que, merced a las pautas interpretativas del Convenio 108 y como recoge su artículo 8, ha de contener facultades positivas y activas de información y de control sobre la existencia, fines y responsables de los ficheros públicos automatizados de la Administración Pública,

---

198 *Vid*. STC 254/1993, de 20 de julio. Consultado el 12.07.2020 desde: http://hj.tribunalconstitucionales/es-ES/Resolucion/Show/2383.

199 Sigue manteniendo cierta sensación de inseguridad jurídica como le ocurría a la LORTAD, pues no se concreta en ningún momento de manera específica el bien jurídico protegido. *Vid*. LUCAS MURILLO DE LA CUEVA, P., "La construcción del derecho a…", *op. cit.*, p. 32.

200 *Cfr*. Fundamento jurídico 6º de la STC 254/1993, de 20 de julio; Fundamento jurídico 6º de la STC 292/2000, de 30 de noviembre; y Fundamento jurídico 5º de la STC 254/2000, de 30 de octubre. *Vid*., entre otros: VILLAVERDE MENÉNDEZ, I., "Protección de datos personales…", *op. cit.*, pp. 187-224: MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica*…, *op. cit.*, pp. 254-300; TRONCOSO REIGADA, A., *La protección de datos*…, *op. cit.*, p. 111.

201 *Cfr*. Fundamento jurídico 7º de la STC nº 110/1984, de 26 de noviembre.

202 *Vid*. ORTI VALLEJO, A., "El nuevo derecho fundamental (y de la personalidad) a la libertad informática (a propósito de la STC 254/1994, de 20 de julio)", en *Derecho privado y Constitución*, nº 2 (1994), p. 305; CONDE ORTÍZ, C., *La protección de datos*…, *op. cit.*, pp. 40-41.

tal y corno solicitaba el demandante. Estas facultades de información forman parte del derecho a la intimidad, que vincula directamente a todos los poderes públicos, y ha de ser salvaguardado, aunque no se haya desarrollado legislativamente" [203].

Esta interpretación resulta novedosa en el contexto español, dado que hasta la fecha no se había producido ningún pronunciamiento similar respecto del tenor consagrado en el artículo 18.4 de la CE. Con posterioridad, el TC vendría a secundar nuevamente dicho razonamiento sobre la base de los diversos instrumentos jurídicos internacionales que había suscrito España sobre la materia. La nueva corriente interpretativa a nivel jurisprudencial tendría su acogida definitiva en el año 2000, preceptuando el carácter autónomo del derecho a la protección de datos de carácter personal, desvinculándolo de las conjeturas asociadas al derecho a la intimidad [204].

En este mismo sentido, Ortega Giménez afirma que: "[é]ste es uno de los derechos fundamentales que se explicitan con mayor amplitud y que aparece deslindado, con claridad meridiana, de otros como el respeto de la vida privada y familiar (art. 7), en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea. Así, la privacidad ha entrado en la categoría de los derechos humanos en la medida que garantiza libertades ulteriores como la de obtener trabajo, un crédito o de optar o acceder a determinados servicios: en definitiva, devuelve al individuo (persona física) el control sobre su entorno y garantiza la sostenibilidad del desarrollo"[205].

La nueva corriente jurisprudencial a la que se aludía en los párrafos precedentes trae causa, en gran medida, de la proclamación de la Carta de Derechos Fundamentales de la Unión Europea. La lectura de la norma comunitaria juntamente con el artículo 18.4 de la CE propiciarían que la jurisprudencia del Tribunal Constitucional, a través de, entre

[203] *Cfr*. GONZÁLEZ MURÚA, A. R., "Comentario a la S.T.C. 254/1993…", *op. cit*., p. 213.

[204] *Vid*. LUCAS MURILLO DE LA CUEVA, P., "El derecho a la autodeterminación informativa y la protección de datos personales", en *Azpilcueta Cuadernos de Derecho*, nº 20 (2008), pp. 43-58.

[205] *Cfr*. ORTEGA GIMÉNEZ, A., *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*, Madrid: Ed. Agencia Española de Protección de Datos, 2015, p. 27.

otras[206], sus Sentencias nº 290/2000[207] y nº 292/2000[208], ambas de fecha 30 de noviembre, proclamase los fundamentos jurídicos que servirían de sustento para delimitar el contenido y alcance del derecho fundamental a la protección de los datos de carácter personal.

Aparte de ser puesta de manifiesto por parte de la doctrina, esta influencia a la que se viene haciendo alusión[209] también se halla incluida en el voto particular que el magistrado Jiménez de Parga y Cabrera incluye en la STC nº 290/2000, cuando manifiesta el tenor literal siguiente: "[n]o ha de sorprendernos que en la Constitución española de 1978 no se tutelase expresamente la libertad informática. Veintidós años atrás la revolución de la técnica en este campo apenas comenzaba y apenas se percibía. No hemos de extrañarnos tampoco por la omisión de esta materia en los Estatutos de Autonomía de las Comunidades españolas" [210].

Sigue indicando el referido magistrado: "[e]l entorno es ahora distinto del que fue nuestro mundo en 1978. La informática no ofrecía las actuales posibilidades para el quehacer vital, tanto positivas como negativas, con la adecuada protección de la dignidad

---

[206] *Vid*., entre otras, las Sentencias del Tribunal Constitucional nº 127/2003, de 30 de junio; nº 233/2005, de 26 de septiembre; nº 96/2012, de 7 de mayo; nº 17/2013, de 31 de enero y nº 29/2013, de 11 de febrero, así como los Autos del Tribunal Constitucional nº 420/2003, de 16 de diciembre; nº 29/2008, de 28 de enero y nº 155/2009, de 25 de junio.

[207] *Vid*. Sentencia del Tribunal Constitucional, nº 290/2000, de 30 de noviembre, publicada en el B.O.E. nº 4, en fecha 4 de enero de 2001. Su contenido viene a reconocer la competencia exclusiva de la Agencia Española de Protección de Datos para la llevanza y control de la obligación de inscripción de los ficheros de titularidad privada que se reconocía en la anterior legislación, esto es, la LORTAD (1992) y la LOPD (1999). Consultado el 12.07.2020 desde: http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4274.

[208] *Vid*. Sentencia del Tribunal Constitucional nº 292/2000, de 30 de noviembre, publicada en el B.O.E. nº 4, en fecha 4 de enero de 2001. Su contenido se basa en los pronunciamientos derivados del recurso de inconstitucionalidad presentado por el Defensor del Pueblo respecto de los arts. 21.1, 24.1 y 24.2 de la LOPD (1999). Consultado el 12.07.2020 desde: http://hj.tribunalconstitucional.es/HJ/cs-CZ/Resolucion/Show/SENTENCIA/2000/292.

[209] A este respecto, Troncoso Reigada afirma el siguiente tenor literal: "[t]al vez la proclamación tan clara de este derecho fundamental a la protección de datos personales se debe a que el ponente de la Sentencia (el Magistrado D. Julio Diego González Campos), o más bien el Letrado encargado, había ya leído los borradores de la Carta de Derechos Fundamentales de la Unión Europea, donde se afirma este derecho de manera autónoma. De hecho, el propio texto de la Sentencia se encuentra muy influido por la Carta". *Cfr*. TRONCOSO REIGADA, A., *La protección de datos…*, *op. cit.*, p. 132.

[210] *Cfr*. Apartado tercero del voto particular que formula el Magistrado Manuel Jiménez de Parga y Cabrera en la Sentencia nº 290/2000, de 30 de noviembre, dictada en los recursos de inconstitucionalidad acumulados nº 201/1993, 219/93, 226/93 y 236/93, al que presta su adhesión el Magistrado Rafael de Mendizábal Allende. Consultado el 12.07.2020 desde: http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4274.

de la persona. Muy significativo al respecto es que en la recentísima Carta de Derechos Fundamentales de la Unión Europea se haya incluido como una de las primeras libertades (art. 8) la resultante de la protección de datos de carácter personal"[211].

Desde un punto de vista legislativo, ante el contexto descrito, tanto inicialmente la LORTAD como posteriormente la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, LOPD), tuvieron a bien acoger esta nueva corriente interpretativa desde el punto de vista regulatorio. Una buena muestra de ello la podemos encontrar en el contenido vertido por el artículo 1 de la última de las normas nacionales citadas, que enfatiza sobre su objeto, manifestando que: "[…] Garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar". Así, alejándose de las interpretaciones iniciales sucedidas sobre el derecho a la protección de datos personales, viene a preceptuarlo como un auténtico derecho fundamental[212].

Esta interpretación vendría a ser finalmente perpetuada por la jurisprudencia del Tribunal Constitucional que hemos tenido la oportunidad de referenciar pues, en una etapa de maduración más tardía, vendría a sentar el contenido esencial de este derecho de configuración legal[213], su objeto, alcance y límites, vinculándolo con los artículos 18.4 y 10.2 de la CE, así como respaldando su vigencia mediante diversos instrumentos de derecho comunitario e internacional[214]. En palabras de Lucas Murillo de la Cueva, se

---

[211] *Ibidem.*

[212] A este respecto, Lucas Murillo de la Cueva critica este tardío reconocimiento normativo, pues afirma que: "Si se pensaba que con el texto de 1999 se superaba el marco de la limitación del uso de la informática para una normativa que va más allá de tal objetivo, además de que se podía haber dicho sin ninguna dificultad, sucede que ese propósito es igualmente perseguible desde el mismo precepto constitucional que se preocupa de la garantía del pleno ejercicio de los derechos de los ciudadanos, de todos sus derechos". *Cfr.* LUCAS MURILLO DE LA CUEVA, P., *El derecho a…*, *op. cit.*, p. 24.

[213] Por lo que se refiere a la definición de un derecho constitucional de configuración legal, resulta necesario que el mismo haya sido paulatinamente desarrollado a nivel jurisprudencial, en este caso, a través de la jurisprudencia dimanante del Tribunal Constitucional. *Vid.* NOREÑA SALTO, J. R., "Acerca del contenido esencial de los derechos fundamentales de configuración legal", en *Repertorio Aranzadi del Tribunal Constitucional*, nº 18 (2004), p. 10.

[214] *Vid.* PIÑAR MAÑAS, J. L., "Protección de datos: origen, situación actual…", *op. cit.*, pp. 97-98.

consolidaría como un "instituto de garantía de los derechos a la intimidad y el honor y del pleno disfrute de los restantes derechos de los ciudadanos"[215].

De todas las resoluciones citadas, es la STC 292/2000, de 30 de noviembre, la que se encarga en mayor medida de clarificar todas las incertidumbres interpretativas que aparejaba la figura del derecho a la protección de los datos de carácter personal. De manera sintetizada, podemos afirmar que, en primera instancia, aborda su singularidad dotándolo de ciertas particularidades que permiten alejarlo de la estela que históricamente lo vinculaba con el derecho a la intimidad[216], pues el TC establece que: "El derecho a la intimidad no aporta por sí solo una protección suficiente frente a la nueva realidad derivada del progreso tecnológico"[217], dado que su objetivo principal radica en excluir que cualesquiera terceros puedan inmiscuirse en ámbitos reservados de la vida personal y familiar[218], posicionándose como una faceta claramente restrictiva[219].

En segunda instancia, se aborda su objeto de protección[220], que no es otro que la protección sobre "[…] cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es solo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal"[221]. Por lo que

---

[215] *Cfr*. LUCAS MURILLO DE LA CUEVA, P., "La construcción del derecho a…", *op. cit*., pp. 33-34.

[216] El TC define la intimidad como "[...] La existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana", *Cfr*. Fundamento jurídico nº 3 de la STC 231/1988, de 2 de diciembre, y Fundamento jurídico nº 6 de la STC 254/1993, de 20 de julio. Adicionalmente, "[...] La inviolabilidad de domicilio y de la correspondencia, que son algunas de esas libertades tradicionales, tienen como finalidad principal el respeto a un ámbito de vida privada, personal y familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado", *Cfr*. Fundamento jurídico nº 3 de la STC 110/1984, de 26 de noviembre.

[217] *Cfr*. Fundamento jurídico nº 4 de la STC 292/2000, de 30 de noviembre. El TC trae a colación la fundamentación que ya había puesto de manifiesto con anterioridad en la STC 254/1993, de 20 de julio.

[218] *Vid*. OLLERO TASSARA, A., *De la protección de la intimidad al poder de control sobre los datos personales. Exigencias jurídico-naturales e historicidad en la jurisprudencia constitucional*, Madrid: Ed. Real Academia de Ciencias Morales y Políticas, 2008, p. 127.

[219] *Vid*. GAY FUENTES, C., *Intimidad y tratamiento de datos en las Administraciones Públicas*, Madrid: Ed. Editorial Complutense, 1995, pp. 22-25.

[220] Respecto de su interpretación en el contexto comunitario, *vid*. HUSTINX, P., "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", 2014, p. 3. Consultado el 12.07.2020 desde: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_ENpdf.

[221] *Cfr*. Fundamento jurídico 6º de la STC nº 292/2000, de 30 de noviembre.

extiende su ámbito de aplicación material más allá de la intimidad individual de la persona que se consagra en el artículo 18.1 de la CE[222], pues este último goza de mayor concreción y especificidad por lo que al bien jurídico protegido se refiere[223].

En tercera instancia, relacionado con su contenido, debe mencionarse que: "A diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE)"[224]. En contraposición con lo establecido por el derecho a la intimidad, faculta al afectado para que este disponga de un conjunto de capacidades que le permitirían ejercer un control efectivo sobre los datos personales que le conciernen, no únicamente salvaguardar los mismos frente a su divulgación a terceros como ocurre con el referido derecho a la intimidad que se viene abordando[225].

En este punto, resulta oportuno recordar la definición que realiza Medina Guerrero sobre el contenido constitucionalmente protegido de un derecho fundamental, cuando preceptúa al respecto que el mismo se compone de: "Un determinado haz de garantías, facultades y posibilidades de actuación (conectado con su aspecto material) que la Constitución reconoce inmanentemente a sus titulares. Estas concretas facultades y

---

[222] *Vid*. CONDE ORTÍZ, C., *La protección de datos…*, *op. cit.*, pp. 45- 46.

[223] LUCAS MURILLO DE LA CUEVA observa que "[l]a sentencia señala que la singularidad del derecho a la protección de datos viene, de una parte, de la mayor amplitud de su objeto en comparación con el del derecho a la intimidad", ya que "extiende su garantía no solo a la intimidad en su dimensión constitucionalmente protegida por el artículo 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal […], como el derecho al honor, […] e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona". De esta manera, el derecho fundamental a la protección de datos "amplía la garantía constitucional a aquellos de esos datos que sean relevantes o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar o cualquier otro bien constitucionalmente amparado". *Cfr*. LUCAS MURILLO DE LA CUEVA, P., "La construcción del derecho a…", *op. cit.*, pp. 35-36.

[224] *Cfr*. Fundamento jurídico 5º de la STC nº 292/2000, de 30 de noviembre.

[225] *Vid*. TRONCOSO REIGADA, A., *La protección de datos…*, *op. cit.*, p. 133.

poderes, en cuanto a manifestaciones o proyecciones del bien jurídico a cuya tutela se encomienda el derecho fundamental, constituyen su contenido constitucionalmente protegido, que podría definirse como el sector de la realidad formado por el conjunto de facultades y poderes directamente relacionado con el interés individual que da vida a cada derecho fundamental, en el cual únicamente es dable aquella injerencia estatal que satisfaga las condiciones constitucionalmente establecidas"[226].

En cuarta y última instancia, debe resaltarse, por un lado, que ambos derechos no deben interpretarse de una manera totalmente autónoma y separada dado que, como anteriormente se ha tenido la oportunidad de reseñar, su contenido resulta complementario en ciertos aspectos. Especialmente en aquellos supuestos en que el derecho a la protección de datos confluye con el derecho a la intimidad al instrumentalizarse este último mediante la consagración del primero[227].

Y, por otro lado, sin perjuicio de lo anterior, el derecho a la protección de los datos de carácter personal también goza de ciertos límites sobre los que había tenido ocasión de pronunciarse en determinadas ocasiones el Tribunal Europeo de Derechos Humanos[228], aunque haciendo alusión a las vicisitudes contenidas en el artículo 8 relativo a la intimidad individual y familiar, que pueden resultar homologables sobre la materia que aquí nos concierne debido a que, como fin último, debemos tener presente que todos los límites de los derechos fundamentales se encuentran amparados en el respeto a los demás restantes y sus respectivos bienes jurídicos constitucionalmente protegidos[229].

Coincidiendo con Lucas Murillo de la Cueva, conviene manifestar que resulta cuanto menos paradigmático que la primera Sentencia sobre el derecho a la protección de datos —la STC 254/1993— se dictara pocos meses después de la entrada en vigor de la LORTAD y que la 11/1998 —y las que componen la serie que esta encabeza surgieran cuando se discute la transposición de la Directiva 46/95/CEE—. Adicionalmente, el autor

---

[226] *Cfr*. MEDINA GUERRERO, M., *La vinculación negativa del legislador a los derechos fundamentales*, Madrid: Ed. MCGraw-Hill, 1996, p. 11. Extraído de BUENO GALLARDO, E., *La configuración constitucional…*, *op. cit.*, p. 544.

[227] *Vid*. BUENO GALLARDO, E., *La configuración constitucional…*, *op. cit.*, pp. 433-435.

[228] *Vid*., entre otras: las Sentencias del Tribunal Europeo de Derechos Humanos, de 7 de julio de 1989 (Asunto Gaskin), de 26 de marzo de 1987 (Asunto Leander), de 25 de febrero de 1993 (Asunto Funke) y de 25 de febrero de 1997 (Asunto Z).

[229] *Vid*. LUCAS MURILLO DE LA CUEVA, P., "La construcción del derecho a…", *op. cit.*, p. 7.

apunta que las de 30 de noviembre de 2000 no solo cuentan ya con el referente de destacados decisiones del Tribunal de Estrasburgo, sino que aparecen casi a la par que la Carta de los Derechos Fundamentales de la Unión Europea[230].

Sentado lo anterior, se puede concluir este apartado afirmando, sin pretender extender en demasía el debate doctrinal que ha girado en torno de la dogmática de los derechos fundamentales que, como se ha apuntado —en consonancia con lo expresado por Ollero Tassara[231] y Medina Guerrero[232]—, nos encontramos ante un auténtico derecho fundamental de configuración legal. Su construcción se he posibilitado principalmente a través de la jurisprudencia emanada por parte del Tribunal Constitucional, que se ha encargado de ir perfilando su contenido esencial adecuándolo al ordenamiento jurídico español, con fundamento en las distintas disposiciones normativas comunitarias que han ido avalando su paulatina plasmación[233].

[230] *Ibidem*, p. 43.

[231] *Vid*. OLLERO TASSARA, A., *De la protección de la intimidad…*, *op. cit.*, p. 28.

[232] *Vid*. MEDINA GUERRERO, M., "Escritos sobre derechos fundamentales", en *Revista Española de Derecho Constitucional*, nº 41 (1994), pp. 323-324.

[233] *Vid*. ORTEGA GIMÉNEZ, A., *Código de Protección de Datos de Carácter Personal*, Madrid: Ed. Difusión Jurídica, 2008, pp. 337-449; LUCAS MURILLO DE LA CUEVA, P., "La construcción del derecho a…", *op. cit.*, p. 39.

3. Transferencias internaciones de datos. Fundamentación de una institución jurídica

En los últimos tiempos, a tenor del rápido avance de la tecnología y la globalización, hemos sido espectadores de los cambios que han propiciado ambos factores en el ámbito socioeconómico y jurídico, barajándose circunstancias que hasta el momento no habían sido tenidas en cuenta y, en ocasiones, ni tan siquiera planteadas. Una de las casuísticas que mayor impacto ha ido suscitando en la sociedad tecnológica ha radicado en el aumento de los movimientos transfronterizos de datos de carácter personal como consecuencia del aumento de las operaciones económicas transnacionales efectuadas entre los distintos operadores económicos, tanto aquellas propias del sector público como del privado[234].

Este nuevo planteamiento ha comportado la asunción de nuevas inquietudes e incertidumbres que hasta la fecha no se habían contemplado, convirtiéndose en uno de los mayores quebraderos de cabeza para las autoridades y entes regulatorios[235]. Si bien es cierto que se han sucedido múltiples beneficios para las organizaciones, ello no ha ostentado carácter gratuito puesto que ha significado un claro agravio para los derechos y libertades de los afectados, poniendo en jaque el contenido fundamental preceptuado en los mismos[236].

Se constata cada vez más con una mayor claridad, que las transferencias internacionales de datos personales han ido adoptando gradualmente una posición primordial en las disposiciones normativas que se han ido sucediendo en los distintos ordenamientos jurídicos comunitarios en materia de protección de datos de carácter personal. Ello no obsta a que su regulación se haya ido abordando con cierta polémica por el amplio espectro de dudas que iba generando, siendo en multitud de ocasiones

---

[234] *Vid*. GARCÍA DEL POYO, R. y GARI, F., "Régimen jurídico aplicable a las transferencias internacionales y sus implicaciones en la actividad mercantil de las empresas multinacionales", en *Revista Española de Protección de Datos*, nº 2 (2007), Madrid: Ed. Agencia de Protección de Datos de la Comunidad de Madrid-Thomson-Civitas, pp. 239-266.

[235] *Vid*. VELÁZQUEZ BAUTISTA, R., *Protección jurídica de datos personales automatizados*, Madrid: Ed. Colex, 1993, p. 184; REBOLLO DELGADO, L. y SERRANO PÉREZ, M. M., *Manual de protección de datos*, Madrid: Ed. Dykinson, 2014, pp. 72-73.

[236] *Vid*. ESTADELLA YUSTE, O., "La transmisión internacional…", en *Jornadas sobre…*, *op. cit*., p. 195.

preciso que su interpretación se viese complementada con los pronunciamientos dimanantes del sector doctrinal[237].

3.1. Conceptualización

Ante el contexto descrito, motivado además por las dispares situaciones regulatorias que se encuentran en los diferentes países que no forman parte de la Unión Europea —y que, por ende, no disponen de un nivel de protección equiparable[238]— y la dificultad añadida de regular la especial casuística de esta institución[239], propician que los intentos de su conceptualización hayan sido escasos —e incluso tardíos—, en detrimento de la imperante necesidad de los distintos operadores económicos de resolver de manera ágil las distintas controversias que se iban suscitando sobre la materia.

---

[237] *Vid*., entre otros: ALMUZARA ALMAIDA, C., *Estudio práctico sobre la protección de datos de carácter personal*, Valladolid: Ed. Lex Nova, 2007, pp. 383-417; ÁLVAREZ CIVANTOS, O. J., *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*, Granada: Ed. Comares, 2001, pp. 88-111; APARICIO SALOM, J., *Estudio sobre la Ley Orgánica de Protección…*, *op. cit*., pp. 213-214; DAVARA RODRÍGUEZ, A. (Dir.), *Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones (TIC)*, Madrid: Ed. Fundación Vodafone, 2004, pp. 15-27, 38-56; FREIXAS GUTIÉRREZ, G., *La protección de los datos de carácter personal en el Derecho español. Aspectos teóricos y prácticos*, Barcelona: Ed. Bosch, 2001, pp. 345-356; GARRIGA DOMÍNGUEZ, A., *Tratamiento de datos personales y derechos fundamentales*, Madrid: Ed. Dykinson, 2004, pp. 177-181; POULLET, Y., "Flujos de datos…", *op. cit*., pp. 93-113; RIGAUX, F., "Le régime des données informatisées en droit international privé", en *Journal du droit international*, Vol. 113 (1986), pp. 311-328; RIPOLL CARULLA, S., "El Movimiento Internacional de Datos en la Ley Española de Protección de Datos", en *Informática y Derecho. Revista Iberoamericana de Derecho Informático*, nº 6-7 (1994), Mérida: Ed. Universidad Nacional de Educación a Distancia, Centro Regional de Extremadura, pp. 313-322; PIÑOL I RULL, J. y ESTADELLA YUSTE, O., "La regulación de la transmisión internacional de datos en la L.O. 5/1992 de 29 de octubre", en RIPOLL I CARULLA, S. (Coord.), *La protección de los datos personales: regulación nacional e internacional de la seguridad informática*, Barcelona: Ed. Universitat Pompeu Fabra, 1993, pp. 78-79.

[238] *Vid*. CARRASCOSA GONZÁLEZ, J., "Circulación internacional de datos personales informatizados y la Directiva 95/46/CE", en *Actualidad Civil*, nº 23 (1997), p. 512.

[239] Como bien ha tenido ocasión de recordar el TJUE, según el siguiente literal: "En ese sentido, el capítulo IV de esta, en el que figuran los artículos 25 y 26, estableció un régimen dirigido a garantizar un control por los Estados miembros de las transferencias de datos personales hacia terceros países. Es un régimen complementario del régimen general que establece el capítulo II de la misma Directiva, que enuncia las condiciones generales de licitud de los tratamientos de datos personales (véase, en ese sentido, la sentencia Lindqvist, C-101/01, EU:C:2003:596, apartado 63)". *Cfr*. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 6 de octubre de 2015, en el asunto C- 362/14, que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por el Tribunal Supremo de Irlanda, mediante resolución de 17 de julio de 2014, recibida en el Tribunal de Justicia el 25 de julio de 2014, en el procedimiento entre Maximillian Schrems y el Comisionario de Irlanda, con la intervención de Digital Rights Ireland Ltd, apdo. 46 (en adelante también, Schrems I). Consultado el 20.08.2017 desde: http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES.

Desde la perspectiva del derecho comunitario, una vez analizados los distintos antecedentes históricos que se han abordado, se puede afirmar que el concepto de transferencia internacional de datos tampoco fue efectivamente regulado por la Directiva 95/46/CE[240]. A pesar de que la misma tenía como objetivo primordial tratar de armonizar las normativas internas de los distintos Estados miembros en materia de protección de datos de carácter personal, no lo consiguió de manera efectiva. Se pretendía que, entre otras cuestiones, los movimientos transfronterizos de datos en el seno de la Unión Europea no encontrasen ningún tipo de salvedad, al mismo tiempo que se intentaba articular un procedimiento de tutela y garantía de derechos sobre los residentes en territorio europeo.

Fue posteriormente el TJUE[241] quien se encargó de facilitar un concepto en el Caso *Bodil Lindqvist vs Kammaraklagaren*[242], pues, tras examinar diversas cuestiones prejudiciales planteadas por el tribunal nacional sueco, estableció que para que exista una transferencia internacional de datos personales resulta imprescindible que se produzca un efectivo movimiento de los datos personales entre dos sujetos. En palabras del propio Tribunal: "[…] no existe una «transferencia a un país tercero de datos» en el sentido del artículo 25 de la Directiva 95/46 cuando una persona que se encuentra en un Estado miembro difunde datos personales en una página web almacenada por su proveedor de servicios de alojamiento de páginas web que tiene su domicilio en el mismo Estado o en otro Estado miembro, de modo que dichos datos resultan accesibles a cualquier persona que se conecte a Internet, incluidas aquellas que se encuentren en países terceros"[243].

Este posicionamiento desencadenó ciertas voces doctrinales disidentes como la que encontramos en Davara Rodríguez, que considera que este pronunciamiento puede

[240] El TJUE recuerda al respecto: "La Directiva 95/46 no define ni en su artículo 25 ni en ningún otro precepto, ni siquiera en su artículo 2, el concepto de «transferencia a un país tercero»". *Cfr*. STJUE. Asunto C-101/2001 (Lindqvist), cit., 56.

[241] *Vid*. ARENAS RAMIRO, M., "El derecho a la protección…", en *Revista de Derecho…*, *op. cit.*, pp. 95-119; RODRÍGUEZ-IZQUIERDO SERRANO, M., "El Tribunal de Justicia y los derechos en la sociedad de la información: Privacidad y protección de Datos frente a libertades informativas", en *Revista de Derecho Constitucional Europeo*, nº 24 (2015).

[242] *Vid*. DE MIGUEL ASENSIO, P. A., "Avances en la interpretación...", *op. cit.*, pp. 3-4.

[243] *Cfr*. STJUE. Asunto C-101/2001 (Lindqvist), cit., 71.

entenderse como "concluyente, pero, a nuestro entender, desilusionante"[244]. Dicho autor considera que la postura del TJUE no fue controvertida, al no entrar a valorar ciertas cuestiones que subyacen en el fondo del asunto. Una de las más controvertidas radicaba en la posibilidad de que los movimientos de datos personales que se derivasen de la publicación en una página web pudieran entenderse como desencadenantes de ser considerados dentro de la categoría de transferencia internacional de datos, debido a que dichos datos personales podrían ser consultados por usuarios ubicados en terceros países fuera del entorno comunitario —derivándose un nuevo tratamiento—.

Con posterioridad, y ante las dificultades que supuso que los distintos Estados miembros adoptasen una regulación uniforme en relación con la protección de los datos personales de sus respectivos ciudadanos, las autoridades europeas con competencias sobre la materia decidieron optar por otro instrumento jurídico para conseguir el efecto armonizador perseguido inicialmente con la Directiva 95/46/CE. Se articuló la aplicación del RGPD, pues, con su eficacia directa[245], se pretendía poner fin a la dispersión y diversidad normativa que hasta el momento se había producido en el marco de la Unión Europea. Como se tendrá ocasión de constatar, este nuevo cuerpo normativo aborda la institución de la transferencia internacional de datos personales con mayor simpatía que lo hicieron sus predecesores, aunque sin incluir tampoco una definición normativa específica al respecto[246].

Desde la perspectiva del ordenamiento jurídico español, para encontrar una primera alusión normativa sobre las transferencias internacionales de datos personales cabe remontarse a inicios de siglo, en concreto, hasta la Instrucción 1/2000[247], de 1 de

---

[244] *Cfr*. DAVARA RODRÍGUEZ, A., "La transferencia internacional de datos", en *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal*, nº 8 (2010), pp. 1320-1328; POULLET, Y., "Flujos de datos…", *op. cit.*, pp. 99-105.

[245] En relación con este punto, es importante traer a colación el artículo 291, apartado 1, del Tratado de Funcionamiento de la Unión Europea (en adelante, "TFUE"), cuando señala que: "*Los Estados miembros adoptarán todas las medidas de Derecho interno necesarias para la ejecución de los actos jurídicamente vinculantes de la Unión*". Cuando se requieran condiciones uniformes de ejecución de los actos jurídicamente vinculantes de la Unión, la Comisión ejercerá competencias de ejecución (*Vid*. Artículo 291, apartado segundo, del TFUE).

[246] El RGPD sigue manteniendo la incertidumbre sobre la conceptualización de las transferencias internacionales de datos, pues no realiza ninguna alusión en su apartado 4 relativo a las definiciones, ni tampoco en su Capítulo V dedicado exclusivamente a la regulación específica de esta institución jurídica.

[247] *Vid*. España. Norma Primera, de la Sección Primera, del Título III de la Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos

diciembre, de la Agencia Española de Protección de Datos (en adelante, AEPD), cuando al abordar su ámbito de aplicación, preceptuaba que: "[…] se considera transferencia internacional de datos toda transmisión de los mismos fuera del territorio español. En particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero". Al respecto, Davara Rodríguez señala que la citada Instrucción recoge de manera expresa la interpretación por la que opta la AEPD en lo relativo a transferencias internacionales de datos personales[248].

No obstante, cabe recordar que la referida Instrucción fue objeto de anulación parcial, a través de dos sentencias que entraron a valorar su contenido. Por un lado, podemos citar la Sentencia de la Audiencia Nacional, de 15 de marzo de 2002[249], y, por otro lado, la Sentencia del Tribunal Supremo, de 25 de septiembre de 2006[250]. A este aspecto debemos añadirle que la aparición de las Cláusulas Contractuales Tipo (en adelante, CCT) de la Comisión Europea —que tendremos oportunidad de abordar— le hicieron un flaco favor, pues su utilización fue yendo gradualmente en declive.

Así pues, a raíz de un error de transposición de la Directiva 95/46/CE, la legislación española clasificaba el concepto analizado con aquellas transmisiones o comunicaciones de datos que se realizaban fuera del territorio español, de conformidad con lo preceptuado también por el contenido de la propia Ley Orgánica 15/1999[251]. Sin embargo, resulta conveniente afirmar que las transferencias internacionales de datos

internacionales de datos. Consultado el 15.08.2017 desde: https://www.boe.es/buscar/doc.php?id=BOE-A-2000-22726.

[248] *Cfr*. DAVARA RODRÍGUEZ, A., *El abogado y la protección de datos*, Madrid: Ed. Ilustre Colegio de Abogados de Madrid, 2004, p. 34.

[249] *Vid*. Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 15 de marzo de 2002, Sección Primera. Fundamento jurídico decimotercero. Consultado el 15.08.2017 desde: https://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/audiencia_nacional/common/pdfs/Sentencia_AN_15_3_2002_y_Sentencia_TS_Recurso_Casacion_25_9_2006.pdf.

[250] *Vid*. Sentencia de la Sala de lo contencioso-administrativo del Tribunal Supremo, de 25 de septiembre de 2006, Sección Sexta (Recurso de Casación nº 3223/2002). Fundamento jurídico quinto. Consultado el 15.08.2017 desde: https://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/audiencia_nacional/common/pdfs/Sentencia_AN_15_3_2002_y_Sentencia_TS_Recurso_Casacion_25_9_2006.pdf.

[251] *Vid*. España. Artículo 34, letra k), de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Consultado el 15.08.2017 desde: https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf.

tienen tal consideración cuando las mismas se producen fuera del Espacio Económico Europeo[252], como se tendrá ocasión de analizar.

Efectuado este apunte, y a los efectos de ultimar la delimitación del concepto analizado desde la perspectiva legislativa española, cabe mencionar que la citada LOPD efectuaba una clasificación de las transferencias internacionales de datos personales como una de las tipologías posibles de tratamiento de datos personales[253], en idénticos términos a los que lo realizó en su momento la derogada LORTAD.

Sin perjuicio de ello, no es hasta la entrada en vigor del Reglamento 1720/2007[254] (en adelante, RLOPD) cuando se decide optar por la inclusión de una definición expresa sobre el concepto de las transferencias internacionales de datos. Concretamente, se produce cuando existe una "[t]ransmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español"[255].

---

[252] A este respecto, es preciso mencionar que la Ley Orgánica 15/1999 únicamente alude a aquellos Estados miembros ubicados en el seno de la Unión Europea, sin incluir a Islandia, Liechtenstein y Noruega, dado que los mismos forman parte del denominado Espacio Económico Europeo. Sin embargo, a tenor de diversas resoluciones e informes emitidos por la AEPD, cabe afirmar, que los movimientos de datos personales destinados a los países anteriormente mencionados no serán entendidos como transferencias internacionales de datos personales, pues existe una incongruencia manifiesta entre lo que establece la LOPD y el RLOPD a este respecto. *Vid*. FERNÁNDEZ-LONGORIA, P. y FERNÁNDEZ-SAMANIEGO, J., *Comentarios a la Ley Orgánica de Protección de Datos Personales*, Pamplona: Thomson Reuters, 2010, p. 1779.

[253] *Vid*. España - Artículo 3, letra c), de la LOPD.

[254] *Vid*. España. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Consultado el 15.08.2017 desde: https://www.boe.es/buscar/act.php?id=BOE-A-2008-979. Para un análisis pormenorizado sobre su contenido, *vid*., entre otros: ZABÍA DE LA MATA, J. (Coord.). y VV. AA., *Protección de datos: Comentarios al Reglamento*, Ed. Lex Nova, 2008.

[255] *Vid*. España. Artículo 5, apartado primero, letra s), del RLOPD. Cabe advertir a este respecto que ni el RGPD ni tampoco la Ley Orgánica 3/2018 —a través de su Disposición derogatoria única—, que viene a sustituir la antigua LOPD, han derogado expresamente el RLOPD, por lo que su contenido sigue siendo complementario al RGPD y la nueva Ley Orgánica 3/2018 en todo lo que no los contradiga, siendo este caso un claro ejemplo, en relación con la definición de la institución jurídica de las transferencias internacionales de datos personales. *Vid*. PIÑAR MAÑAS, J. L. y RECIO GAYO, M., *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, Ed. Wolters Kluwer, 2018, pp. 156-160.

3.2. Posiciones jurídicas

Una vez sentado lo anterior, cabe identificar los diferentes sujetos que intervienen dentro del marco de las transferencias internacionales de datos personales. Desde la perspectiva del derecho comunitario, su conceptualización aparece recogida inicialmente en la Decisión de la Comisión, de 5 de febrero de 2010[256], a través de su artículo 3, en que se establece, por un lado, que el exportador de datos será "el responsable del tratamiento que transfiera los datos personales" y, por otro lado, define al importador de datos como "el encargado del tratamiento establecido en un tercer país que convenga en recibir del exportador datos personales para su posterior tratamiento en nombre de este, de conformidad con sus instrucciones y los términos de la presente Decisión, y que no esté sujeto al sistema de un tercer país que garantice la protección adecuada en el sentido del artículo 25, apartado 1, de la Directiva 95/46/CE".

Adicionalmente, la referida Decisión también introduce el término conceptual de "subencargado del tratamiento", entendiendo por tal "cualquier encargado del tratamiento contratado por el importador de datos o por cualquier otro subencargado de este que convenga en recibir del importador de datos, o de cualquier otro subencargado de este, datos personales exclusivamente para las posteriores actividades de tratamiento que se hayan de llevar a cabo en nombre del exportador de datos". En consonancia, la Decisión de Ejecución (UE) 2021/914 de la Comisión[257], que viene a derogar sus previas Decisiones nº 2001/497/CE y 2010/87/UE con efecto a partir del 27 de septiembre de 2021, acogerá esta conceptualización para desarrollar su propio contenido.

Respecto de esta última figura, la Agencia Española de Protección de Datos, ante las dificultades y dudas interpretativas que se planteaban sobre su utilización, en el año 2012 consideró conveniente elaborar un modelo de clausulado contractual aplicable a dichas casuísticas, especialmente orientado hacia aquellas subcontrataciones de servicios

[256] *Vid*. Decisión 2010/87/UE 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/CE del Parlamento Europeo y del Consejo (notificada con el número C [2010] 593). Consultado el 15.08.2017 desde: En línea: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32010D0087.

[257] *Vid*. Decisión de Ejecución (UE) 2021/914 de la Comisión, de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, que deroga las Decisiones de la Comisión Europea nº 2001/497/EC y 2010/87/EU. Consultado el 20 de junio de 2021 desde: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32021D0914

que implicasen un tratamiento de datos personales entre encargados del tratamiento ubicados en España y subencargados sitos en terceros países que no ofreciesen un nivel de protección adecuado. Para poder articular la aplicación de dicho clausulado, era imprescindible que el responsable formara parte integrante del contrato que debería de formalizarse entre todos los intervinientes, con la intención de asumir la aportación de las respectivas garantías adecuadas[258].

En similares términos a los expresados en el ámbito comunitario, desde la perspectiva del derecho español, en el RLOPD también se parte de la premisa de identificar ambas figuras. Por un lado, se define al exportador como "la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero"[259]; y por otro lado, al importador como "la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero"[260].

Incluso el RLOPD fue un paso más allá y se atrevió a incluir el concepto de "tercero"[261] —que posteriormente también sería acogido por el RGPD[262]—,

[258] La AEPD ha tenido la oportunidad de tratar esta cuestión en varios de sus informes jurídicos. *Vid*., entre otros: Informes jurídicos con nº de referencia: 582/2004, 518/2006 o 108/2007, concluyendo, entre otros aspectos, lo que veníamos apuntando, esto es, la necesidad de que el responsable del tratamiento forme parte de la relación jurídica originada entre los distintos sujetos intervinientes, en aras de responsabilizarse de la aportación de las garantías adecuadas en el momento de la solicitud de la autorización ante la autoridad de control (Director/a de la AEPD), de conformidad con lo preceptuado por la anterior normativa de protección de datos —LOPD y RLOPD—. *Vid*. FERNÁNDEZ-LONGORIA, P. y FERNÁNDEZ-SAMANIEGO, J., *Comentarios a la Ley…*, *op. cit.*, , p. 1797.

[259] España. Artículo 5, apartado primero, letra j), del RLOPD.

[260] Artículo 5, apartado primero, letra ñ), del RLOPD.

[261] A este respecto, como indica Durán Cardo, "[e]l concepto de tercero se incluyó en la Propuesta de Directiva de 1992 a raíz de la enmienda 134ª propuesta por el Parlamento Europeo que se inspiró en la Ley federal alemana de 1990. La Comisión entendió que debía utilizarse para delimitar la figura del cesionario o quien recibe la comunicación de datos […]. Se confirmó […] que la utilidad del concepto era incorporar a aquellos sujetos que estuvieran fuera del círculo de influencia del responsable […] asimilándose al concepto de tercero del derecho civil, como sujeto que no es parte de una relación jurídica determinada, normalmente la que existirá entre el responsable del tratamiento y el interesado". *Cfr*. DURÁN CARDO, B., *La figura del responsable en el derecho a la protección de datos. Génesis y evolución normativa ante el cambio tecnológico y en perspectiva multinivel*, Barcelona: Ed. Universidad Autónoma de Barcelona, 2015, p. 301.

[262] *Vid*. España. Artículo 4, apartado décimo, del RGPD.

entendiéndolo como "la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento"[263].

En cualquier caso, al abordar las diferentes figuras, resulta oportuno a efectos aclaratorios, traer a colación las consideraciones formuladas por Sancho Villa, cuando entiende al respecto que: "simplemente se crea un subconcepto para referirse con mayor precisión al empresario responsable establecido en la UE que promueve una transferencia internacional a un tercer Estado (que se denomina "exportador"), dirigida a un empresario receptor establecido en ese lugar (que denominamos "importador"), con independencia de que este último vaya a actuar como responsable o un encargado"[264].

En este punto, conviene distinguir con carácter adicional las figuras de "responsable del tratamiento" y de "encargado del tratamiento" que la anterior LOPD[265] y su Reglamento de desarrollo[266] ya introducían, siendo adoptadas por el RGPD. De esta manera, será considerado dentro de la primera categoría "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros"[267]. Si, por el contrario, "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales"[268] lo realiza por cuenta del responsable, bajo sus directrices, será considerado dentro de la segunda de las categorías descritas con anterioridad.

---

[263] *Vid*. España. Artículo 5, apartado primero, letra r), del RLOPD.

[264] *Cfr*. SANCHO VILLA, D., *Negocios Internacionales de Tratamiento de Datos Personales*, Cizur Menor (Navarra): Ed. Civitas, 2010, p. 27.

[265] *Vid*. España. Artículo 3, letra d) y g), del RLOPD, respectivamente.

[266] *Vid*. España. Artículo 5, apartado primero, letra q) e i), del RLOPD, respectivamente.

[267] *Vid*. Artículo 4, apartado séptimo, del RGPD.

[268] *Vid*. Artículo 4, apartado octavo, del RGPD.

Con base en lo expuesto, el Comité Europeo de Protección de Datos (en adelante, CEPD)[269], el pasado 2 de septiembre de 2020 hizo público un proyecto de Directrices sobre los conceptos de responsable y encargado del tratamiento conforme a las vicisitudes contenidas en el RGPD, que vendrían a sustituir las anteriores del GT29 elaboradas en 2010. El documento proporciona una serie de orientaciones sobre los conceptos mencionados, así como en relación con la figura del corresponsable del tratamiento introducida por el artículo 26 del RGPD. Entre las cuestiones más relevantes por lo que a este trabajo interesa, conviene destacar, por un lado, que los criterios que se introducen para realizar la diferenciación entre responsable y encargado del tratamiento no varían en demasía respecto los introducidos con anterioridad por parte del GT29.

Y, por otro lado, manifiesta que las relaciones entre el responsable y el encargado no se pueden resumir únicamente en la suscripción de un acuerdo que contenga las obligaciones establecidas en el artículo 28 del RGPD, sino que deberá de profundizar sobre las obligaciones y procedimientos que deben de adoptarse por ambas partes en determinadas circunstancias controvertidas, como puede sucederse ante la gestión de una brecha de seguridad o la debida atención de los derechos de los interesados. Además, el CEPD introduce un conjunto de criterios para diferenciar las situaciones que son susceptibles de ser consideradas como una corresponsabilidad del tratamiento, pues reconoce una cierta tendencia entre los responsables de confundir sus respectivas relaciones con encargados con lo que vendría a ser una corresponsabilidad, a la luz de los últimos pronunciamientos que se han producido al respecto por parte del TJUE[270].

En última instancia, pero no menos importante, se encuentra el interesado o afectado, titular del bien jurídico protegido por el derecho fundamental a la protección de los datos personales. Se trata de la figura esencial sobre la que pivota el cuadro de

[269] El Comité Europeo de Protección de Datos —que viene a sustituir al anterior GT29— puede entenderse como un organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la Unión Europea y promueve la cooperación entre las autoridades de protección de datos de la UE. El CEPD está compuesto por representantes de las autoridades nacionales de protección de datos y del Supervisor Europeo de Protección de Datos. El CEPD se encarga de adoptar directrices generales para clarificar los términos de la legislación europea de protección de datos, proporcionando a todas las partes interesadas una interpretación coherente de sus derechos y obligaciones, así como de tomar resoluciones vinculantes con respecto a las autoridades nacionales de supervisión para garantizar una aplicación coherente de la referida normativa. Consultado el 11.07.2020 desde: https://edpb.europa.eu/edpb_es.

[270] *Vid*. STJUE de fecha, 29 de julio de 2019, en el asunto C-40/17. Consultado el 21 de junio de 2021 desde: https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&doclang=ES

movimientos que se produce en el contexto de las transferencias internacionales. Su definición aparecía ya recogida en la anterior LOPD[271], constando en la actualidad también en el RGPD[272], que entiende como tal aquella "persona física identificada o identificable" titular de los datos personales que han sido recabados y, posteriormente, objeto de tratamiento para aquellas finalidades que motivaron su recogida.

Con posterioridad, cabe mencionar que la Decisión de Ejecución (UE) 2021/914 de la Comisión referenciada, mantendrá las definiciones para los distintos actores intervinientes en las transferencias en términos similares a lo establecido por sus predecesoras. Así se puede constatar en el Anexo de dicha Decisión, cuando en su Cláusula 1 de la Sección I, se alude al exportador de datos como: "la(s) persona(s) física(s) o jurídica(s), autoridad(es) pública(s), servicio(s) u organismo(s) (en lo sucesivo, «entidad» o «entidades») que va(n) a transferir los datos personales". Y respecto al importador, lo designa como: "la(s) entidad(es) en un tercer país que va(n) a recibir los datos personales del exportador de datos directamente o indirectamente por medio de otra entidad que también sea parte en el presente pliego de cláusulas".

A este respecto, se puede apreciar como los cambios más notorios se han implementado sobre la definición de la figura relativa al importador de los datos. Ello obedece al nuevo enfoque modular que se ha pretendido articular sobre el contenido de esta nueva versión actualizada de las Cláusulas Contractuales Tipo, con la intención de que puedan resultar aplicables ante las distintas complejidades que pueden sucederse durante la realización de movimientos internacionales de datos, aportando soluciones prácticas —a diferencia de lo que venía ocurriendo hasta la fecha—. Así como a la necesidad de flexibilizar la robustez de la que estaban dotadas, haciendo posible que terceras partes puedan adherirse a su contenido, tanto en su condición de exportadores como importadores, durante la totalidad de su periodo de vigencia.

3.3. Modalidades

Una vez esbozado el concepto que engloba las transferencias internacionales de datos personales e identificado a los principales sujetos que intervienen en las mismas,

[271] *Vid*. España. Artículo 5, apartado primero, letra a), del RLOPD.

[272] *Vid*. Artículo 4, apartado primero, del RGPD.

cabe manifestar que la incipiente doctrina[273] ha considerado oportuno abordar los diversos criterios que existen para clasificar las tipologías de movimientos transnacionales de datos personales que se producen, siendo el que mayor aceptación ha obtenido entre los diversos autores aquel que encuentra su fundamento en función del nivel de protección otorgado por el país de destino al que se remitan los datos personales.

En base a dicho criterio, que tiene su origen en una exigencia normativa, resulta conveniente indicar que las diversas modalidades que quedan comprendidas dentro del mismo pivotan sobre el eje básico del nivel de protección adecuado del país de destino. Por lo que, antes de entrar a discernir las distintas tipologías de trasferencias basadas en este criterio, vamos a efectuar un análisis sobre la consideración relativa al nivel de protección adecuado y a sus eventuales implicaciones.

A este respecto, como indica Matus Arenas, "[…] los perjuicios económicos que pueden derivarse de la limitación que establece el artículo 25 de la Directiva, tanto para los países europeos como para los terceros, obliga a fijar o determinar con precisión qué es lo que efectivamente quiere exigir la Directiva con el requisito de protección adecuada,

[273] Para una aproximación al debate doctrinal generado sobre esta cuestión. *Vid*., entre otros: DEL PESO NAVARRO, E. y RAMOS GONZÁLEZ, M. A., *La seguridad de los datos de carácter personal*, Madrid: Ed. Díaz de Santos, 2002, pp. 112-117; DE MIGUEL ASENSIO, P. A., "Nota a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal", en *Anuario de Derecho internacional Privado*, Vol. I (2001), Madrid: Ed. Iprolex, pp. 626-627; SANCHO VILLA, D., *Transferencia internacional de datos personales*, Madrid: Ed. Agencia de Protección de Datos, 2003, pp. 47-52; DAVARA RODRÍGUEZ, A., "La transferencia internacional de datos", en *Revista Española de Protección de Datos*, nº 1 (2007), Madrid: Ed. Agencia de Protección de Datos de la Comunidad de Madrid-CIVITAS, pp. 27-28; FERNÁNDEZ LÓPEZ, J. M., "Flujo internacional de datos", en *Informática y Derecho: Revista Iberoamericana de Derecho Informático*, nº 30-32 (1999), págs. 189 y ss.; ESTADELLA YUSTE, O., "La transmisión internacional de datos y su control", en *Jornadas sobre el Derecho español de la Protección de Datos Personales*, Madrid: Agencia de Protección de Datos, 1996, págs. 197 y ss.; RIPOLL CARULLA, S., "El Movimiento internacional de…", en *Informática y Derecho*, *op. cit.*; PIÑOL RULL, J. L. y ESTADELLA YUSTE, O., "La regulación del flujo internacional de datos", en *La protección de los datos personales: regulación nacional e internacional de la seguridad informática*, Barcelona: Ed. Centro de Investigación de la Comunicación de la Universidad Pompeu Fabra, 1993, pp. 75-91; PIÑOL RULL, J., *Los flujos internacionales de datos: aproximación a su regulación jurídica*, Tomo IV, Barbastro: Ed. U.N.E.D., 1987, págs. 137 y ss.; GARZÓN, G., *El marco jurídico del flujo de datos transfronteras*, Doc. TDF 102, Roma: Ed. IBI, 1981; FAUGEROLAS, L., *L'accés international à des banques de dones*, París: G.L.N., 1989; MADEC, A., *Les flux transfrontières de dones*, París, 1982; FISHMAN, W., *Legal Issues of Transborder Data Transmisión*, 74 h Meeting, P.A.S.I.L., 1980, p. 175.

los criterios que de alguna manera otorguen objetividad al grado de adecuación, así como quién debe declararla o concederla"[274].

Para analizar dicha consideración, resulta obligado partir de uno de los documentos publicados al respecto por parte del Grupo de Trabajo del Artículo 29[275], en que se afirma que, para lograr determinar de manera significativa el nivel de protección adecuado, debe realizarse a partir del análisis exhaustivo de dos elementos básicos: el contenido de las normas aplicables en el país de destino de los datos y los medios existentes para asegurar que la legislación resulta aplicable de manera efectiva[276]. Para garantizar el primero de los condicionantes, el GT29 propone un listado de unos mínimos aspectos que deben de evaluarse para determinar si el nivel de protección que ofrece el país de destino puede considerarse adecuado[277]. Para ello se parte del contenido preceptuado en la Directiva 95/46/CE, que deberá ser adecuado específicamente a cada caso en particular.

En relación con el segundo de los condicionantes expuestos relativos a los mecanismos de supervisión existentes que permitan garantizar la aplicación efectiva de la legislación aplicable en el país de destino de los datos personales, el GT29 considera que los objetivos que tiene que articular un sistema de estas características deben

---

[274] *Cfr*. MATUS ARENAS, J., "Transferencias internacionales a países con niveles adecuados y no adecuados de protección Aspectos prácticos", en *Ponencia para el Seminario Regional de Protección de Datos*, Uruguay, 2010, p. 4.

[275] La evaluación del nivel de protección adecuado del país de destino de los datos personales debe realizarse conjuntamente mediante la utilización de distintos instrumentos. *Vid*., entre otros: COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 4): Primeras orientaciones sobre la transferencia de datos personales a terceros países. Posibles formas de evaluar la adecuación", aprobado por el Grupo de trabajo el 26 de junio de 1997; "Documento de Trabajo (nº 7): "Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos en un tercer país?", aprobado por el Grupo de trabajo el 14 de enero de 1998; "Documento de Trabajo (nº 9): Conclusiones preliminares sobre la utilización de disposiciones contractuales en caso de transferencia de datos personales a terceros países", aprobado por el Grupo de trabajo el 22 de abril de 1998.

[276] *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 12): Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE", aprobado por el Grupo de Trabajo el 24 de julio de 1998, p. 5.

[277] El listado de principios mínimos que debería de contener la legislación de protección de datos del país de destino para considerarse adecuada serían los siguientes: (i) Principio de limitación de objetivos de tratamiento; (ii) Principio de proporcionalidad y calidad de los datos; iii) Principio de transparencia en el deber de informar a los afectados; (iv) Principio de seguridad en el tratamiento; (v) Principio de derechos sobre los afectados (acceso, rectificación y oposición); (vi) Restricciones respecto a transferencias sucesivas a terceros países que no garanticen el nivel de protección adecuado. *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 12)…", cit., p. 6-7.

fundamentarse en: (i) ofrecer un nivel satisfactorio de cumplimiento de las normas de protección de datos existentes, en que los actores conozcan los respectivos deberes y obligaciones que les atañen durante el tratamiento de datos personales; (ii) prestar apoyo y asistencia a los interesados cuando estos pretendan hacer valer sus derechos o pretensiones; y (iii) ofrecer la posibilidad de recurso a los afectados ante la inobservancia o incumplimientos de la legislación aplicable sobre la materia[278].

Ahora que se ha dimensionado la concepción derivada del nivel de protección adecuado, resulta preciso enunciar las distintas modalidades de transferencias internacionales de datos personales que se han acogido mayoritariamente por parte de la doctrina dentro de este criterio[279]. Como se apuntaba con anterioridad, dicho criterio tiene su fundamento en una exigencia normativa que permite articular la clasificación en función de la situación legislativa —en materia de protección de los datos personales— del país de destino al que se pretendan remitir los datos personales recabados.

En primer lugar, se encuentran los flujos de datos personales intracomunitarios entre los distintos países pertenecientes al EEE sobre los que no existe restricción alguna de movimiento, cuya regulación se establecía inicialmente sobre la base de lo dispuesto en la Directiva 95/46/CE[280], y que, en la actualidad, su vigencia se ha visto desplazada por el contenido previsto en el RGPD[281]. En este escenario, el papel primordial para garantizar la aplicación de la normativa lo protagonizan las distintas autoridades de control de cada uno de los Estados Miembros de la Unión. Como señala Heredero Higueras, "evaluarán, en relación con la transferencia o categoría o clase de transferencias, si un tercer Estado ofrece o no un nivel de protección adecuado sobre la base de los criterios que enumera el apartado 2 [del art. 25 de la Directiva 95/46/CE] al efecto"[282].

---

[278] *Vid*. GUASCH PORTAS, V., "La transferencia internacional de datos de carácter personal", en *Revista de Derecho – Universidad Nacional de Educación a Distancia*, nº 11 (2012), p. 423.

[279] Otro factor que la doctrina ha destacado por su posición determinante radica en la ley aplicable, dado que en función de las casuísticas de movimientos transfronterizos que nos encontremos, la misma dependerá, entre otros factores, de las disposiciones que se hayan previsto a este respecto en materia de derecho internacional. *Vid*. SANCHO VILLA, D., *Transferencia internacional…*, *op. cit.*, pp. 47-52.

[280] *Vid*. Artículo 25, apartado primero, de la Directiva 95/46/CE.

[281] *Vid*. Artículo 44, del RGPD.

[282] *Cfr*. HEREDERO HIGUERAS, M., *La Directiva Comunitaria de protección de los datos de carácter personal*, Madrid: Ed. Tecnos, 1998, p. 188.

En segundo lugar, se posibilitan los movimientos de datos transfronterizos a aquellos terceros Estados que gozan de un nivel de protección adecuado, de conformidad con las declaraciones realizadas por parte de la Comisión Europea. Dichas potestades se encontraban amparadas en los apartados 4 a 6 del artículo 25 de la Directiva 95/46/CE para, posteriormente, verse reflejadas en los apartados 3 a 6 del artículo 45 del RGPD. El listado de territorios que goza del beneplácito de la Comisión se ha ido ampliando paulatinamente. Especialmente, en relación con los territorios del entorno asiático, pues el último de los países que ha recibido tal categorización ha sido Japón, y se espera que, en breve, se sumen algunos más que ya están trabajando con sus respectivas legislaciones internas, como se tendrá ocasión de analizar.

A este respecto, cabe mencionar aquellos países que en la actualidad gozan de un nivel de protección adecuado[283], los cuales pueden enunciarse así, según su orden de aprobación: (i) Suiza (Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000); (ii) Canadá (Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos); (iii) Argentina (Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003); (iv) Guernsey (Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003); (v) Isla de Man (Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004); (vi) Jersey (Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008); (vii) Islas Feroe (Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010); (viii) Andorra (Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010); (ix) Israel (Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011); (x) Uruguay (Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012); (xi) Nueva Zelanda (Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012); y finalmente, (xi) Japón (Decisión 2019/419/UE de la Comisión, de 23 de enero de 2019)[284].

[283] No se ha incluido en el listado la Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, que resulta aplicable sobre aquellas entidades certificadas en el marco del Escudo de Privacidad UE-EE. UU., dado que ha quedado invalidada como consecuencia de la Sentencia del Tribunal de Justicia de la Unión Europea, emitida el 16 de julio de 2020, en el asunto C-311/18 (Sentencia Schrems II), que en los próximos apartados tendremos ocasión de abordar.

[284] Se trata de la última de las Decisiones de Ejecución adoptadas por la Comisión Europea, que se ha realizado durante la vigencia y aplicación del RGPD, aprovechando la habilitación que en el mismo se contiene, en virtud del apartado tercero del artículo 45 del RGPD. A diferencia de lo que ocurría con la Directiva 95/46/CE, en este supuesto, no será preciso recabar autorización nacional alguna para efectuar el movimiento de datos transfronterizo directamente a los Estados miembros aquí indicados, como

Cabe mencionar la adición venidera del Reino Unido y Corea del Sur[285] al listado expresado con anterioridad. En relación con la casuística vinculada al Reino Unido, cabe indicar que el pasado 16 de junio de 2021[286], se hacía pública la votación de los representantes de los Estados Miembros de la Unión Europea que daba la luz verde a la aprobación del Proyecto de Decisión de Ejecución, de conformidad con el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, sobre la protección adecuada de los datos personales por parte del Reino Unido [287]. Dicha actuación legislativa se adoptaba más de seis meses después de la conclusión del periodo de transición del Brexit, finalizado el 31 de diciembre de 2020, de conformidad con lo apuntado incluso por la propia autoridad británica con competencias sobre la materia[288].

En tercer y último lugar, con carácter residual, se articulan aquellos supuestos en que se efectúan transferencias internacionales de datos a países que no ostentan un nivel de protección adecuado, ya sea porque el movimiento de datos en cuestión resulta amparado en alguna de las circunstancias excepcionales habilitadas por la legislación aplicable o, *a sensu contrario,* porque las autoridades de control nacionales de los Estados miembros hayan habilitado el movimiento en aquellos supuestos en los que se hayan considerado adecuadas las garantías aportadas por parte del responsable del tratamiento. Como manifiesta Ancos Francos, "las disposiciones de la Directiva reguladoras de la transferencia de datos a países no comunitarios han provocado la preocupación de

consecuencia de lo establecido en el Considerando 103 y, a su vez, en el apartado primero, del artículo 45 del RGPD. En este sentido, conviene indicar que no se ha hecho mención alguna a los Estados Unidos, pues en la fecha de publicación de este trabajo el Acuerdo había sido anulado como se analiza y expone por parte del TJUE en su Sentencia emitida el 16 de julio de 2020, en el asunto C-311/18.

[285] La casuística relativa a Corea del Sur, será revisada y abordada con mayor detalle en el Capítulo III del presente trabajo.

[286] *Vid*. Votación sobre Proyecto de Decisión de Ejecución, de conformidad con el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, sobre la protección adecuada de los datos personales por parte del Reino Unido. Consultado el 21 de junio de 2021 desde: https://ec.europa.eu/transparency/comitology-register/screen/documents/074268/1/consult?lang=en

[287] *Vid*. Proyecto de Decisión de Ejecución, de conformidad con el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, sobre la protección adecuada de los datos personales por parte del Reino Unido. Consultado el 21 de junio de 2021 desde: https://ec.europa.eu/info/sites/default/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_19_feb_2020.pdf

[288] Publicación efectuada por parte de la autoridad de protección de datos del Reino Unido, relativa a la situación de las transferencias internacionales de datos personales con la Unión Europea . Consultado el 21 de junio de 2021 desde: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/

gobiernos y operadores económicos no comunitarios en la medida en que su aplicación puede representar un obstáculo a la libre transferencia de datos"[289].

[289] *Cfr*. ANCOS FRANCO, H., "La regulación de las transferencias internacionales de datos de carácter personal como barrera al comercio internacional: De la Directiva 95/46 a los acuerdos UE-terceros Estados", en *Revista de Derecho Comunitario Europeo*, nº 6 (1996), pp. 497-516.

4. Régimen jurídico de las transferencias internacionales de datos de carácter personal bajo el acervo de la Directiva 45/96/CE. Mención a la LORTAD, a la LOPD y al RLOPD

4.1. Terceros países con un nivel de protección adecuado

Una vez examinadas las distintas especificidades relativas a la institución jurídica de las transferencias internacionales de datos personales, resulta oportuno analizar el régimen previsto desde la perspectiva del derecho comunitario. Para ello, realizaremos un análisis comparativo entre las consideraciones previstas en la ya superada Directiva 95/46/CE respecto de lo dispuesto en el actual RGPD, pasando a su vez por las vicisitudes contenidas en las sucesivas normas españolas que han posibilitado la transposición de los distintos instrumentos de derecho comunitario al ordenamiento jurídico español.

Como inicio de la primera parte de la exposición a la que se viene haciendo alusión, cabe destacar que la Directiva 95/46/CE[290] contemplaba la regulación relativa a las transferencias internacionales de datos básicamente en dos artículos[291], el artículo 25 que recogía la regla general y, posteriormente, el 26 que complementaba al anterior con una serie de excepciones. Su punto de partida venía determinado inicialmente por el artículo 12 del Convenio 108 que se ha examinado, pues en el mismo se contenía la noción de "protección equivalente", que posteriormente se convertiría en el ya tratado "nivel de protección adecuado" contemplado en la Directiva, que resultaría de aplicación a partir de la ficción de "terceros Estados".

---

[290] *Vid*., entre otros: CARRASCOSA GONZALEZ, J., "La Directiva 95/46/CE: Entre la protección de la intimidad y la libre transferencia internacional de datos personales automatizados", en *Economist & Jurist*, p. 30-35; ESTADELLA YUSTE, O., *La protección de la intimidad…*, *op. cit*., pp. 59-75; PIERCE, G y PLATTEN, N., "Achieving Personal Data Protection in the European Union", en *Journal of Common Market Studies*, Vol. 36, nº 4 (1998), pp. 529-547; SANCHO VILLA, D., *Transferencia internacional…*, *op. cit*., pp. 49-52; ORTEGA JIMÉNEZ, A., "La transferencia internacional de datos de carácter personal y el Derecho internacional privado", en *Diario La Ley*, nº 6237 (2005), pp. 1-5.

[291] Las bases fundamentales del régimen relativo a las transferencias internacionales de datos personales en la Directiva 95/46/CE se hallan establecidas en los Considerandos 56 a 59 del referido cuerpo legal, pues resulta esencial traer a colación parte del contenido establecido en el Considerado 56 cuando establece el siguiente tenor literal: "Considerando que los flujos transfronterizos de datos personales son necesarios para la desarrollo del comercio internacional; que la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado; que el carácter adecuado del nivel de protección ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias".

Como señala Ancos Francos, "el artículo 25 se manifestaba en términos mucho más amplios que su precedente en el Convenio. Mientras que la «protección equivalente» aparecía ligada a determinadas categorías de datos cuya naturaleza exigía una protección especial o instrumentos adicionales de salvaguardia, el «nivel de protección adecuado» no se predicaba de grupos de datos concretos, sino que se estaba haciendo referencia (art. 25.2) al grueso de la legislación estatal, a la par de implicar el recurso a un completo listado de criterios que hacían el procedimiento de evaluación complejo, riguroso y, sobre todo, tornando difícil el reconocimiento de la homologación"[292].

Así pues, el eje básico sobre el que pivotaba la Directiva —con fundamento en el legado normativo efectuado por el Convenio 108— radicaba en determinar si el país de destino al que se remitían los datos personales recibía la categorización de territorio con un "nivel de protección adecuado". Si se asumía tal consideración, se habilitaban los movimientos internacionales de datos personales fuera del Espacio Económico Europeo, siempre que se prestaran las garantías suficientes por parte del responsable —o, en su caso, del corresponsable o encargado del tratamiento—[293].

La categorización que se viene examinando, podía ser declarada tanto por la Comisión Europea, como por la propia autoridad de control nacional del país de origen de la transferencia con competencias sobre la materia. En el primer supuesto, la Comisión partía de consideraciones de diversa índole para llegar a alcanzar una conclusión, pues tenía en cuenta las propias particularidades que concurrían en una transferencia internacional de datos, como "la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países"[294].

A este respecto, no es óbice recordar las declaraciones que efectuaba el GT29[295] relativas a la obligatoriedad de realizar la evaluación partiendo de las vicisitudes

[292] *Cfr*. ANCOS FRANCO, H., "La regulación de las transferencias…", *op. cit.*, p. 505.

[293] *Vid*. GRANDE SANZ, M., "La transferencia internacional de datos personales: presente y futuro", en *Diario La Ley*, nº 8808 (2016), pp. 1-10.

[294] *Cfr*. Artículo 25, apartado segundo, de la Directiva 95/46/CE.

[295] *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 12): Transferencias…", cit., 1998, pp. 4-6; COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 114): relativo a una interpretación común

estipuladas en el régimen jurídico comunitario para poder determinar con exactitud las vigentes en el Estado de destino de los datos personales, verificando así su nivel de aplicación práctica. Dichas consideraciones se vieron reforzadas posteriormente por ser acogidas por parte del Tribunal de Justicia de la Unión Europea[296]. El Alto tribunal entendió que se trataba de una garantía que permitía valorar la idoneidad de un destino, con antelación a que se produjera un movimiento transfronterizo de datos personales, evitando elusiones que podían poner en jaque la salvaguarda de los derechos y libertades fundamentales de los afectados[297].

En cualquier caso, conviene matizar que aunque se hubiera adoptado una decisión de adecuación, ello no imposibilitaba que un afectado pudiera manifestar lo contrario respecto al posible uso transnacional que se pudiera estar realizando de sus respectivos datos personales, si entendía que no se estaba respetando la legislación aplicable. En consecuencia, con fundamento en el principio de primacía del respeto al derecho fundamental de protección de datos, las autoridades de control nacionales y, en su caso, los eventuales organismos judiciales debían poner en conocimiento de la Comisión Europea que un país de destino en cuestión no estaba realizando las actuaciones necesarias para ser considerado garante del nivel de protección adecuado.

Ante estos supuestos, la autoridad de control nacional que recibía la petición que le pudiera dirigir un afectado en cuestión tenía dos alternativas que debía considerar. Por un lado, entender que la solicitud resultaba carente de fundamento, con la intención de que fuera el propio interesado el que, si lo estimaba oportuno, pudiera acudir a los

---

del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995", aprobado por el Grupo de Trabajo, el 25 de noviembre de 2005.

[296] Al respecto, el TJUE se ha pronunciado manifestando el siguiente tenor literal: "Debe entenderse la expresión «nivel de protección adecuado» en el sentido de que exige que ese tercer país garantice, efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta. En efecto, a falta de esa exigencia el objetivo mencionado en el anterior apartado de la presente sentencia se frustraría. Además, el elevado nivel de protección garantizado por la Directiva 95/46 entendida a la luz de la Carta se podría eludir fácilmente con transferencias de datos personales desde la Unión a terceros países para su tratamiento en estos". *Cfr*. STJUE. Asunto C-362/14 (Schrems I), cit., apdo. 73.

[297] *Vid*. REQUEJO ISIDRO, M., "La aplicación privada del derecho para la protección de las personas físicas en materia de tratamiento de datos personales en el Reglamento (UE) 2016/679", en *Revista La Ley Mercantil*, nº 42 (2017), pp. 1-25.

tribunales nacionales que le correspondieran para hacer valer sus pretensiones[298]. O alternativamente, por otro lado, estimar la instancia efectuada por el afectado como procedente y que fuera la propia autoridad de control la que se personase directamente en instancias judiciales para dar inicio al procedimiento, que tendría como principal objetivo plantear una cuestión prejudicial ante el TJUE sobre la validez de la decisión de adecuación adoptada. En cualquiera de los dos supuestos, sería el referido organismo judicial el que tendría la competencia judicial para conocer sobre el asunto y el que dilucidaría las eventuales cuestiones prejudiciales planteadas.

Lo anterior podemos correlacionarlo con la segunda de las casuísticas apuntadas, esto es, las facultades que se reconocían a las autoridades de control de los Estados miembros para que pudieran determinar, dentro de su respectivo ámbito nacional de soberanía, que un país de destino fuera considerado con un nivel de protección adecuado, una vez que se hubiera efectuado la correspondiente evaluación. Asimismo, en el supuesto de que constatase que un tercer país no garantizaba un nivel de protección adecuado conforme a lo indicado, serían las competentes para llevar a término todas aquellas actuaciones que resultaran precisas para detener los flujos de datos transnacionales a ese tercer país, puesto que así lo establecen las correspondientes Decisiones de Ejecución adoptadas por parte de la Comisión Europea[299].

En este mismo sentido, se pronuncia el contenido preceptuado en el artículo 25 de la Directiva, que al disponer de una regulación de mayor recorrido que su antecesor —el Convenio 108—, le permitió establecer una especie de mecanismo de cooperación mediante el contenido recogido complementariamente en los artículos 26 y 31 colindantes. Se incluían una serie de competencias conjuntas que podían ser ejercidas entre la Comisión Europea y las respectivas autoridades de control nacional de los distintos Estados miembros, en aras de supervisar y velar por el cumplimiento de la legislación aplicable en materia de protección de datos personales y, particularmente, en lo relativo a las transferencias internacionales.

Una vez examinado el régimen jurídico que se contenía en la Directiva 95/46/CE en relación con las transferencias internacionales de datos personales a terceros países que ostentaban un nivel de protección adecuado, cabe abordar las vicisitudes jurídicas

[298] *Vid*. STJUE. Asunto C 362/14 (Schrems I), cit.

[299] *Vid*. HEREDERO HIGUERAS, M., *La Directiva Comunitaria…*, *op. cit.*, p. 188.

que también se encontraban amparadas en el ordenamiento jurídico español. Para ello, se inicia el análisis con el contenido establecido en la histórica LORTAD, para posteriormente terminar con la también derogada LOPD, citando en algunos casos su Reglamento de desarrollo, que incluso en determinadas cuestiones sigue resultando de aplicación en la actualidad en todo aquello que no lo contradiga —a pesar de la vigencia del RGPD—.

La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal se adelantó a la promulgación de la Directiva, constituyéndose como la primera norma que desarrollaba el contenido preceptuado en el artículo 18.4 de la CE[300]. Como se ha tenido la oportunidad de avanzar en anteriores líneas, su proceso de tramitación parlamentaria no fue precisamente pacífico[301], pues fue objeto de multitud de enmiendas, incluyéndose además varios recursos de inconstitucionalidad[302], dado que su contenido generaba multitud de dudas interpretativas que dificultaban su efectiva aplicación.

Se trataba de una norma que, al igual que sucedería posteriormente con la LOPD, se encontraba influenciada significativamente por el contenido establecido en el Convenio 108 y por el proyecto de la Directiva 95/46/CE que se encontraba en proceso de tramitación. Por este motivo, se desencadenó su aprobación ante la necesidad de suscribir el Acuerdo de Schengen[303] antes mencionado, constituyéndose como una especie de legislación general sobre la materia que, a su vez, incluía multitud de remisiones a normativas sectoriales.

---

[300] *Vid*. DEL PESO NAVARRO, E. y RAMOS, M. A., *LORTAD. Análisis de la Ley*, Ed. Díaz de Santos, 1994, pp. 169-180; HEREDERO HIGUERAS, M., *La Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal: comentarios y textos*, Madrid: Ed. Tecnos, 1996.

[301] *Vid*. LUCAS MURILLO DE LA CUEVA, P., *El derecho a…*, *op. cit.*, pp. 165-172.

[302] *Vid*. LÓPEZ GARRIDO, D., "Aspectos de inconstitucionalidad de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal", en *RDP*, nº 38 (1993); NAVARRO RUIZ, J. C., "Algunas consideraciones sobre la tramitación de la LORTAD", en *Cuadernos de la Cátedra de Fadrique Furió Ceriol*, nº 1 (1992), pp. 98-107.

[303] *Vid*. PÉREZ LUÑO, A. E., "Comentario legislativo: La LORTAD y los derechos fundamentales", en *Derechos y Libertades*, nº 1 (1993), p. 409; PÉREZ LUÑO, A. E., *Manual de Informática…*, *op. cit.* p. 61-65; MARTÍN PALLÍN, J. A., "La Ley Orgánica de Regulación del tratamiento automatizado de datos de carácter personal. Una visión crítica", en *Informática Judicial y Protección de Datos Personales*, Vitoria: Ed. Gobierno Vasco, 1994, pp. 80-86.

El régimen relativo a las transferencias que se encontraba consagrado en la LORTAD partía de las mismas críticas sobre las que hemos venido haciendo hincapié, pues sus artículos 32 y 33[304] —pese a compartir idéntico esquema que el previsto en la Directiva—, no resultaban capaces de determinar con exactitud un escenario plausible para los movimientos de datos transfronterizos. No se contenían los criterios que debían verificarse para considerar a un tercer país con un nivel de protección adecuado[305] y, por ende, cumplir los condicionantes que permitían solicitar la autorización al director/a de la autoridad de protección de datos competente, según resultara.

En la fecha límite de transposición facilitada por la Directiva 95/46/CE, el Gobierno remitió a finales de junio de 1998 al Congreso el proyecto de Ley Orgánica que modificaba la LORTAD. Aunque inicialmente se había planteado como una actualización de la norma vigente hasta dicha fecha, con posterioridad se optó por la remisión de un nuevo texto completo. El objetivo radicaba en intentar dotar al texto de una mayor seguridad jurídica que solventase las deficiencias incurridas por las normas predecesoras.

Tras la consecución del correspondiente proceso parlamentario, ello terminaría el 25 de noviembre de 1999 en el Congreso de los Diputados con la respectiva aprobación —y posterior sanción, promulgación y publicación— de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[306]. Su tramitación no estuvo

---

[304] *Vid*. GARZÓN CLARIANA, G. y VILARIÑO PINTOS, E., *Las leyes de protección de datos personal y su incidencia en la circulación transnacional de datos*, Roma: Ed. IBI, 1980, pp. 5-11; VILARIÑO PINTOS, E., "La Ley de regulación del tratamiento automatizado de datos de datos de carácter personal ante el Derecho Internacional", en *La protección de datos personales. Regulación nacional e internacional de la seguridad informática*, Ed. Centro de Investigación de Comunicación, Universidad Pompeu Fabra, Generalitat de Catalunya, 1993, pp. 49-74.

[305] Ello no se consiguió tampoco con los artículos 3 y 4 contenidos en el Real Decreto 1332/1994, de 20 de junio, por el que se abordan aspectos concretos de la Ley 5/1992 (LORTAD), que intentaron precisar los detalles del régimen jurídico aplicable ante la modalidad de movimiento de datos objeto de análisis. Únicamente podemos encontrar alguna de esas previsiones incluidas en la Memoria de la Agencia de Protección de Datos de 1995. *Vid*. *Memoria de la Agencia de Protección de Datos*, Madrid: Ed. Agencia de Protección de Datos, 1995, pp. 71-72.

[306] Para un mayor estudio sobre el contenido de la norma, *vid*., entre otros: RUIZ CARRILLO, A., *La protección de datos de carácter personal*, Barcelona: Ed. Bosch, 2001; TÉLLEZ AGUILERA, A., *Nuevas tecnologías, intimidad y protección de datos. Estudio sistemático de la Ley Orgánica 15/1999*, Madrid: Ed. Edisofer, 2001, pp. 107-164; MARTÍN CASALLO, J. J. y MARTÍN PALLÍN, J. A., "Intimidad, privacidad y protección en la nueva Ley Orgánica 15/1999", en DAVARA RODRÍGUEZ, A. (Coord.), *XIV Encuentros sobre Informática y Derecho 2000-2001*, Navarra: Ed. Aranzadi, 2001, pp. 51-53, 55-59; PÉREZ LUÑO, A. E., *Manual de Informática…*, *op. cit.* p. 61-65; ÁLVAREZ CIENFUEGOS, J. M., *La defensa de la intimidad de los ciudadanos y la tecnología informática*, Pamplona: Ed. Aranzadi, 1999; CAMPUZANO, H., *Vida privada y datos personales*, Madrid: Ed. Tecnos, 1999.

exenta de críticas por parte del sector doctrinal por la deficiente técnica legislativa utilizada[307], tal y como en su momento sucedió con la denominada LORTAD, pero que, a diferencia de esta última, sí que logró obtener un mayor consenso.

La LOPD no venía a aportar nada novedoso en cuanto a la estructura que no recogiera ya su norma predecesora, simplemente suponía la transposición de determinadas cuestiones categóricas preceptuadas por la Directiva, que debían ser incluidas en el ordenamiento jurídico español. Durante la realización de este ejercicio, no se aprovechó la oportunidad para incluir márgenes de desarrollo y mejora que se posibilitan en el marco de la utilización de este instrumento de derecho comunitario. A este respecto, podemos traer a colación las palabras de Heredero Higueras, cuando señala que "[e]l legislador parece haber querido encerrarse, como en una prisión, en la ley derogada. Esta fidelidad a la ley anterior se refleja, ante todo, en la sistemática y, asimismo, en la concepción de base según la cual el consentimiento del interesado es la única condición de licitud de los tratamientos"[308].

Ante este contexto, podemos establecer que el contenido de la LOPD, pese a pretender ser una norma general, se hallaba repleto de excepciones que conducían a una situación de inseguridad jurídica respecto del tratamiento de datos personales[309]. Esta ley tuvo que ser posteriormente complementada por el RLOPD para dotarla de mayor coherencia y cohesión en múltiples aspectos. En este sentido, Solar Calvo señala que "[…] aparte de correcciones específicas relativas a la regulación anterior e innovaciones puntuales por implementación de la Directiva 95/46, si por algo destaca la LOPD es por

---

[307] Una muestra de ello se evidencia en el hecho de que el Proyecto de Ley sí que incluía una Exposición de Motivos, pero vemos como el texto definitivo que se aprueba adolece de dicho contenido. *Vid*., entre otros: LUCAS MURILLO DE LA CUEVA, P., "Las vicisitudes del Derecho de la protección de datos personales", en VV. AA., *La democracia constitucional: estudios en homenaje al profesor Rubio Llorente*, Vol. I, Madrid: Ed. Centro de Estudios Políticos y Constitucionales, 2001, pp. 513-515; TÉLLEZ AGUILERA, A., *Nuevas tecnologías*…, *op. cit.*, pp. 107-109; HEREDERO HIGUERAS, M., "Estudio crítico de la transposición…", *op. cit.*, pp. 124-126.

[308] *Cfr*. HEREDERO HIGUERAS, M., "Estudio crítico de la transposición…", *op. cit.*, p. 125. Aspecto que posteriormente ha supuesto multitud de controversias, pues este error en la transposición se verá duramente criticado con la entrada en vigor del RGPD, que obliga, tal y como en cierta manera lo hacía ya su predecesora, esto es, la Directiva 95/46/CE, a legitimar los eventuales tratamientos de datos personales en alguna de las múltiples bases jurídicas existentes, no únicamente en aquella basada en el consentimiento, pues en muchos casos, como tuvo la oportunidad de advertir el GT29, entre otros organismos, el mismo no se emite en condiciones óptimas que permitan su viabilidad jurídica por existir un manifiesto desequilibrio de intereses entre las distintas partes.

[309] *Vid*. PÉREZ LUÑO, A. E., *Manual de Informática*…, *op. cit.* p. 61-65; FREIXAS GUTIÉRREZ, G., *La protección de los datos* de carácter personal…, *op. cit.*, p. 222.

suponer la introducción de la filosofía de esta última de manera fiel al estilo marcado por la norma europea. Así, la huella de la referida directiva y la función esencial que la nueva ley venía a cumplir no solo se dejan ver en la definición de su ámbito de aplicación, del todo coincidente con el de la Directiva, sino también en la ideología de protección de datos que trasciende y comparten ambas normas"[310].

Asimismo, el régimen jurídico de las transferencias internacionales de datos se hallaba contenido en sus artículos 33 y 34, complementados por lo establecido en los artículos 65 a 70 del RLOPD, respectivamente, siguiendo la influencia marcada por la Directiva como se venía apuntando. En suma, de conformidad con lo establecido en su artículo 33, no se hallaban habilitados los movimientos de datos transfronterizos a terceros países si estos no proporcionaban un nivel de protección adecuado, de igual modo que sucedía con el contenido que hemos tenido la oportunidad de observar en el artículo 25.1 de la Directiva 95/46/CE. Dicha categorización se evaluaba de acuerdo con los criterios abordados, contenidos esencialmente en el artículo 25.2 de la Directiva y 33.2 de la LOPD, atendiendo, recordemos, a todas aquellas particularidades que concurrían sobre una transferencia de datos personales en cuestión.

Siguiendo este orden de cuestiones, el artículo 33.2 de la LOPD referenciado también facultaba a la Agencia Española de Protección de Datos para que, en virtud del mandato efectuado por la Directiva, pudiera evaluar el nivel de protección adecuado que podía ofrecer, en su caso, un tercer país de destino al que se pretendieran remitir los datos personales objeto de tratamiento. La evaluación debía de partir de la premisa expresada por los criterios indicados en los apartados anteriores, pues en consonancia con las facultades preceptuadas en el artículo 37.1, letra l), de la LOPD, la referida autoridad de control disponía de potestad suficiente para ejercer el control sobre las autorizaciones que se hubieran emitido en relación con las transferencias internacionales de datos personales.

En definitiva, podemos concluir afirmando que la legislación española, siguiendo el criterio marcado por la normativa comunitaria, únicamente habilitaba los movimientos transnacionales a terceros países que garantizasen un nivel de protección adecuado según lo dispuesto por la Comisión Europea o la Agencia Española de Protección de Datos[311],

[310] *Cfr*. SOLAR CALVO, M. P., "La protección de…", *op. cit.*, p. 9.

[311] Las Resoluciones del Director/a de la AEPD que considerasen la declaración de un tercer Estado como garante de un nivel de protección adecuado debían publicarse en el Boletín Oficial del Estado, en virtud del

respectivamente. En su defecto, también se podría articular, siempre que se hubiera obtenido con carácter previo a efectuar la transmisión de los datos personales[312], la correspondiente autorización del Director/a de la Autoridad de control.

Respecto de este último supuesto aludido, cabe señalar que dicho procedimiento debía tramitarse siguiendo las vicisitudes contempladas en la LOPD y el RLOPD, pues su aplicación quedaba excluida de las excepciones consagradas en el artículo 34 de la susodicha LOPD, siempre que se verificara que las garantías aportadas fueran suficientes. Al mismo tiempo, el responsable del tratamiento —o, en su caso, el encargado de este— debía velar por el cumplimiento de los principios y derechos establecidos en la legislación española aplicable, especialmente, en lo relativo al cumplimiento del deber de información a los afectados sobre la identificación de los posibles destinatarios de los datos recabados[313].

4.2. Terceros países que no ostentan un nivel de protección adecuado

A diferencia de lo preceptuado en el artículo 25 de la Directiva 95/46/CE, su artículo 26 amparaba toda una serie de excepciones que evitaban la suspensión de las transferencias internacionales de datos personales[314]. En dicho precepto se contemplaban una serie de supuestos que permitían efectuar el movimiento de los datos a terceros países que no ostentaban un nivel de protección adecuado. A este respecto, resulta oportuno recordar a García Beato cuando señala que: "[…] La regulación jurídica de las transferencias internacionales de datos plantea numerosos problemas por la existencia de diversos intereses en juego y por la dificultad práctica de dar eficacia a las garantías que

mandato efectuado por el apartado primero del artículo 67 del RLOPD. El apartado segundo del referido artículo también manifiesta la obligación de mantener un listado actualizado y accesible por medios telemáticos, con la inclusión de todos aquellos países cuyo nivel de protección haya sido considerado equiparable conforme a la legislación comunitaria y española aplicable. Adicionalmente, resulta oportuno traer a colación que desde la aplicación de la LOPD no se produjo ninguna Resolución que considerase que un tercer país proporcionase un nivel de protección adecuado; aspecto contrario sucedió con la LORTAD, pues la Disposición final primera del Reglamento Real Decreto 1332/1994 facultaba al Ministerio de Justicia e Interior para que emitiera la relación de países que ostentaban tal categorización, cuya potestad dio lugar a dos Órdenes Ministeriales, la Orden de 2 de febrero de 1995 (publicada en el B.O.E. en fecha 10 de febrero de 1995) y la Orden de 31 de julio de 1998 (publicada en el B.O.E. en fecha 21 de agosto de 1998).

[312] *Vid*. Artículos 18 y 19 de la Directiva 95/46/CE.

[313] *Vid*. España. Artículo 12 de la LOPD.

[314] *Vid*. ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M., "Notas a la nueva regulación de la protección de datos de carácter personal", en *Revista La Ley*, nº 5036 (2000), p. 1716.

se puedan establecer. Para solucionarlo y obtener una regulación eficaz, hay que intentar lograr un equilibrio entre los intereses comerciales y los derechos individuales, de tal forma que sin menoscabar la intimidad del individuo no se paralicen las transacciones y la realidad comercial"[315].

En este sentido, y en aras a facilitar un mayor entendimiento sobre las distintas excepciones que se hayan contempladas tanto en la Directiva 95/46/CE[316] como en la LOPD, se efectuará un examen conjunto sobre su contenido, partiendo para ello, de aquellas que se encuentran previstas en la primera de las normas citada. Finalmente, se prestará especial atención sobre aquellas cuestiones particulares que subyacen en ambas legislaciones, aspecto que también será abordado, pero de manera específica en las próximas líneas del presente Capítulo.

El principio general relativo a la necesidad de que el país tercero destinatario de los datos goce de un nivel de protección adecuado en el marco de una transferencia internacional, no resultará de aplicación —según la Directiva y la LOPD—, cuando, en primer lugar, el interesado haya dado su consentimiento inequívocamente a la transferencia prevista. Como establecía la Directiva[317], el mismo debía de entenderse como una manifestación de voluntad libre, específica e informada, dado que, de no ser así, como señala el propio GT29: "Esto podría significar que en muchas situaciones en que el consentimiento se da por sobreentendido (por ejemplo, porque la persona ha sido informada de una transferencia y no se ha opuesto), la excepción no resultaría aplicable"[318].

En este sentido, de conformidad con las directrices del GT29, el consentimiento debía ser específico para una transferencia concreta o una categoría específica de

---

[315] *Cfr*. GARCÍA BEATO, M. J., "Flujo internacional de datos personales", en *La protección del derecho a la intimidad de las personas (ficheros de datos), Cuadernos de Derecho Judicial*, Ed. Consejo General del Poder Judicial, 1997, p. 198.

[316] En relación con las excepciones previstas en el artículo 26 de la Directiva 95/46/CE, cabe señalar que el referido texto comunitario faculta a los distintos Estados miembros para que puedan regular más allá de lo aquí establecido, pues no debe entenderse como un listado cerrado.

[317] *Vid*. Artículo 2, letra h), de la Directiva 95/46/CE.

[318] *Cfr*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 12): Transferencias…", cit., p. 26. Adicionalmente, debe de ser complementado. *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 259): Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679", aprobadas por el Grupo de Trabajo, el 28 de noviembre de 2017, revisadas por última vez y adoptadas el 10 de abril de 2018, p. 20.

transferencias[319]. El afectado debía haber sido advertido previamente de las circunstancias específicas de la transferencia —tanto de su finalidad, identidad y datos pormenorizados de los destinatarios, entre otras cuestiones—, así como de los riesgos que suponía el hecho de que sus datos personales fueran remitidos a un país que no ofrecía un nivel de protección adecuado[320].

En segundo lugar, se contempla el momento en que la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado. Tal y como ha manifestado el GT29, esta excepción únicamente puede resultar de aplicación cuando dicha transferencia "[…] puede ser considerada necesaria para la ejecución del contrato en cuestión o la ejecución de medidas precontractuales adoptadas a petición del interesado. Esta "prueba de necesidad" exige una relación estrecha y sustancial entre el interesado y el objeto del contrato"[321].

En este contexto, se introducía como un supuesto de hecho ejemplificativo de la situación, aquellos casos en que una agencia de viajes realizara una transferencia internacional de datos a un país que no ofreciese un nivel de protección adecuado, con la intención de facilitar los datos personales de los turistas a hoteles y otros socios comerciales imprescindibles para organizar la estancia. Por el contrario, se limitaban otros supuestos como podría ser la transferencia de datos de empleados de una filial a su empresa matriz[322].

Sin perjuicio de lo anterior, el GT29 añade al respecto que: "Esta excepción no puede aplicarse a las transferencias de información adicional que no sean necesarias a efectos de la transferencia, o a las transferencias destinadas a una finalidad distinta de la ejecución del contrato. De forma más general, las excepciones contempladas en el artículo 26.1.b) a 26.1.e) solo permiten que los datos que resultan necesarios a efectos de la

[319] *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 114): relativo a una interpretación…", *op. cit.*, p. 14. Adicionalmente, debe de ser complementado. *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 259): Directrices…", cit., pp. 20-21.

[320] *Ibidem.*

[321] *Cfr*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 114): relativo a una interpretación…", cit., p. 15.

[322] *Ibidem.*

transferencia puedan ser transferidos sobre la base de excepciones individuales; para los datos adicionales, se deberán emplear otros medios para acreditar la adecuación"[323].

Asimismo, a efectos interpretativos, resulta oportuno reproducir en este punto las palabras de Herrán Ortiz, cuando señala al respecto que: "La idea de resolver, caso por caso, por vía de contratos o convenios entre responsables de los tratamientos de los Estados de origen y de destino tiene su antecedente en las prácticas y usos alemanes en materia de transferencia de datos sensibles con fines de evaluación de la solvencia y fue recogida y desarrollada en forma de Recomendación por el Consejo de Europa"[324].

En tercer lugar, se aprecia el supuesto de que la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero. La interpretación debe realizarse en el mismo sentido que la casuística anterior, dado que únicamente podía aplicarse la excepción si se superaba la "prueba de necesidad", que suponía constatar la existencia de un vínculo jurídico esencial entre el interés del afectado y el objeto del contrato[325].

En este punto, y de acuerdo con la opinión manifestada en el párrafo anterior por parte del GT29, el mismo recuerda que: "No tiene una opinión negativa sobre la posibilidad de recurrir a encargados del tratamiento situados en terceros países para llevar a cabo un tratamiento de datos, sino que desea recordar la necesidad de utilizar los distintos instrumentos jurídicos que la Directiva 95/46/CE pone a disposición de los responsables del tratamiento"[326].

Al respecto, resulta oportuno advertir que, posteriormente, el Comité Europeo de Protección de Datos emitiría un documento[327] que vendrá a complementar lo dispuesto

---

[323] *Cfr*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 114): relativo a una interpretación…", cit., p. 16.

[324] *Cfr*. HERRÁN ORTIZ, A. I., *El derecho a la protección de datos personales en la sociedad de la información*, Bilbao: Ed. Cuadernos Deusto de derechos Humanos, Universidad de Deusto, 2003, p. 181.

[325] *Ibidem*.

[326] *Cfr*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 114): relativo a una interpretación…", cit., p. 17.

[327] *Vid*. COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, "Directrices 2/2019 sobre el tratamiento de datos personales en virtud del artículo 6(1)(b) RGPD en el marco de la prestación de servicios en línea a interesados", versión 2.0, aprobada el 8 de octubre de 2019, pp. 8-12. Consultado el 11.07.2020 desde:

por el GT29, pues, entre otras cuestiones, constatará que el contrato debe de ser válido y vigente, no teniendo cabida aquellas situaciones en las que únicamente una de las partes asume obligaciones, sin que medie vínculo contractual alguno entre ellas. Al mismo tiempo, profundizará sobre el criterio de la "necesidad" manifestando —mediante una interpretación restrictiva en el uso del término— que no resulta suficiente que la ejecución del contrato sea útil, sino que además es preciso que se contemplen alternativas menos invasivas.

En cuarto lugar, se comprende aquella transferencia que resulta necesaria o legalmente exigida para la salvaguarda de un interés público importante que, como se viene constatando mediante los anteriores supuestos, también deberá interpretarse en un sentido estricto. El GT29 afirma al respecto: "Los únicos intereses públicos importantes válidos son los establecidos por la legislación nacional aplicable a los responsables del tratamiento establecidos en la UE. Cualquier otra interpretación haría muy sencillo que una autoridad extranjera eludiese el requisito de protección adecuada en el país destinatario que establece la Directiva 95/46"[328].

En este sentido, Vizcaíno Calderón apunta sobre la excepción que: "Es tan amplia que prácticamente resiste a cualquier tipo de limitaciones. Si por lo menos se hubiera limitado a la habilitación legal, sería posible concretar el supuesto a la vista de la concreta previsión legal que en cada caso se aplicare. Ahora bien, la referencia a la necesidad para la protección del mencionado interés público destruye racionalmente cualquier posibilidad de concretar el supuesto. Tampoco nos dice la norma a quién compete la apreciación del citado interés público"[329].

Sobre este punto, cabe mencionar que en el marco de la entrada en vigor y aplicación efectiva del RGPD, la AEPD ha tenido ocasión de pronunciarse sobre la interpretación del interés público esencial, estableciendo al respecto que la aplicación del mismo como base de legitimación para un tratamiento de datos requiere de una norma con rango de ley que, en todo caso, debería justificar específicamente en qué medida y en qué supuestos la utilización de dicha base de legitimación estaría amparada.

---

https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22019-processing-personal-data-under-article-61b_es.

[328] *Ibidem.*

[329] *Cfr.* VIZCAÍNO CALDERÓN, M., *Comentarios a la Ley…*, *op. cit.*, pp. 381-382.

Adicionalmente, se tendrían que incluir garantías específicas para su articulación —como exige el Tribunal Constitucional— que le permitieran cumplir con el principio de proporcionalidad y superar el juicio de necesidad, en el sentido de que no existiera otra medida más moderada con la que se consiguiera el mismo propósito con igual eficacia[330].

En quinto lugar, encontramos la transferencia necesaria para el reconocimiento, ejercicio o defensa de un derecho en el curso de un procedimiento judicial. Que, una vez más, como viene siendo tradición en todas las excepciones comentadas hasta el momento, debe ser interpretada estrictamente. Únicamente se podía aplicar si se hubieran cumplido previamente las normas que rigen los procedimientos penales o civiles aplicables a este tipo de situación internacional[331]. En este sentido, el GT29 entendía que no se podía utilizar esta excepción para justificar los movimientos de datos transfronterizos de empleados a la empresa matriz del grupo por la posibilidad de que, en algún momento, dichos datos pudieran ser precisos en sede de un procedimiento judicial[332].

En sexto lugar, se contempla la transferencia que resulta precisa para la salvaguardia del interés vital del interesado[333]. La misma encontraba su ámbito de aplicación en aquellos supuestos en que se consideraba que el movimiento transnacional de los datos personales era imprescindible para garantizar una correcta asistencia médica en caso de urgencia, pues no tiene lógica alguna imponer en estos supuestos ningún tipo de restricción. En otras casuísticas en que la finalidad no sea la de tratar un caso específico de urgencia del interesado, como podría ser llevar a cabo una investigación médica, no

---

330 *Vid*. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Informe jurídico, con nº de referencia: 010308/2019". Consultado el 11.07.2020 desde: https://www.aepd.es/es/documento/2019-0031.pdf. En la Directiva se añade el término "importante" a diferencia de lo que sucede en la LOPD. No obstante, será posteriormente la AEPD la que le añada el término "esencial".

331 *Vid*. Convenio de La Haya, de 18 de marzo de 1970, sobre la obtención de pruebas en el extranjero en materia civil o mercantil, así como el Convenio de La Haya, de 25 de octubre de 1980, tendente a facilitar el acceso internacional a la justicia.

332 *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 114): relativo a una interpretación…", cit., pp. 17-18.

333 Una de las diferencias no sustanciales que introduce la LOPD respecto de lo dispuesto en la Directiva en el ámbito de las excepciones radica en que no se especifica el sujeto que motiva la transferencia, tal y como podemos observar en el artículo 34, letra c), de la LOPD, a través del siguiente tenor literal: "Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.". *Vid*. CÁRDENAS ARTOLA, I., FERRERO RECASENS, E. y VV.AA., *Memento experto. Protección de datos*, Madrid: Ed. Francis Lefebvre, 2012, p. 130.

sería posible amparar la transferencia en esta excepción, pues deberían cumplirse las consideraciones establecidas en el artículo 26.2 de la Directiva[334].

En séptimo y último lugar, se preceptuaba la transferencia que tendría lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, estuviera concebido para facilitar información al público y se encontrase abierto para la consulta del público en general. Alternativamente, también para cualquier persona que pudiera demostrar un interés legítimo, siempre que se cumpliesen, en cada caso particular, las condiciones establecidas por la legislación en cuestión para efectuar la consulta.

A este respecto, el GT29 apunta que la libertad de transmisión no puede ser total al amparo de esta excepción que, una vez más, debe interpretarse en sentido estricto. Se consideraba posible que pudiese materializarse el riesgo de que los datos fuesen recabados de manera masiva, para posteriormente ser utilizados en un tercer Estado para finalidades distintas a las que originaron la recogida de estos, causando un grave perjuicio sobre los derechos y libertades de los afectados[335].

En el contexto español, un ejemplo de lo preceptuado por esta excepción lo podemos encontrar en el artículo 332, apartado tercero, del Decreto de 14 de febrero de 1947, por el que se aprueba el Reglamento Hipotecario[336]. Este precepto normativo determina que aquellos terceros que estén interesados en obtener información sobre los asientos del Registro de la Propiedad deberán acreditar ante el Registrador el interés legítimo que motiva la petición; y en el supuesto de que actúen en nombre y representación de un tercero, deberán acreditar, a satisfacción también del Registrador,

[334] *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 114): relativo a una interpretación…", cit., p. 18.

[335] *Ibidem*, p. 19.

[336] Se reproduce el tenor literal del artículo 332.3 referenciado por lo que a efectos de este análisis interesa: "Quien desee obtener información de los asientos deberá acreditar ante el Registrador que tiene interés legítimo en ello. Cuando el que solicite la información no sea directamente interesado, sino encargado para ello, deberá acreditar a satisfacción del Registrador el encargo recibido y la identificación de la persona o entidad en cuyo nombre actúa. Se presumen acreditadas las personas o entidades que desempeñen una actividad profesional o empresarial relacionada con el tráfico jurídico de bienes inmuebles tales como entidades financieras, abogados, procuradores, graduados sociales, auditores de cuentas, gestores administrativos, agentes de la propiedad inmobiliaria y demás profesionales que desempeñen actividades similares, así como las Entidades y Organismos públicos y los detectives, siempre que expresen la causa de la consulta y esta sea acorde con la finalidad del Registro".

tanto la idoneidad de la representación como las justificaciones que sustentan la petición de consulta.

A este respecto, conviene evocar las reflexiones que realiza la Comisión Europea sobre las divergencias que se producen entre los distintos Estados miembros respecto a la aplicación de las excepciones que se han venido examinando, cuyo contenido se encuentra preceptuado en el ya referido artículo 26 de la Directiva. Sobre la cuestión, señala el literal siguiente: "[E]s evidente que cuando un Estado miembro ha sobrepasado los límites de la Directiva o no ha cumplido sus requisitos, se crea una divergencia que se ha de solucionar mediante la modificación de la legislación del Estado miembro en cuestión"[337].

Una vez expuesto el régimen de excepciones previsto en la Directiva, resulta oportuno abordar las divergencias establecidas por la legislación interna que traspuso la referida norma al ordenamiento jurídico español, encontrándose la cuestión amparada en el artículo 34 de la derogada LOPD. En palabras de Blas, se podría resumir como: "Una lista con 11 epígrafes, sin ningún criterio sistemático ni lógico"[338]. Acogiendo su razonamiento, las cuatro primeras excepciones —letras a) hasta la d)— contienen una reproducción casi literal de los motivos de excepción que se contenían en la LORTAD, mientras que los seis siguientes —letras e) hasta la j)— son una reproducción de la lista de excepciones de la Directiva[339]. El último de los apartados puede considerarse como una obviedad, pues lo mismo había sido abordado por su artículo predecesor. Por ende, podemos considerarlo como una muestra considerable de la deficiente técnica legislativa de la que emana la presente norma abordada, tal y como se ha constatado.

Sin perjuicio de lo anterior, cabe señalar que se introducen tres aspectos que difieren del listado contenido en el artículo 26 de la Directiva. En primera instancia, podemos destacar la excepción que opera cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España. Su aplicación resulta de la ratificación del Convenio 108 por parte de las

---

[337] *Vid*. COMISIÓN EUROPEA, "Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46 CE)" (COM/2003/0265 final), 2003. Consultado el 11.07.2020 desde: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex: 52003DC0265.

[338] *Cfr*. BLAS, F., "Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales", en *Revista Derecho del Estado*, nº 23 (2009), p. 43.

[339] *Ibidem,* pp. 37-66.

autoridades españolas. Específicamente, en lo relativo a movimientos transnacionales de datos personales.

Adicionalmente, cabe mencionar que, según la Disposición transitoria primera de la LOPD relativa a los tratamientos creados por Convenios internacionales, la AEPD "será el organismo competente para la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal respecto de los tratamientos establecidos en cualquier Convenio Internacional del que sea parte España que atribuya a una autoridad nacional de control esta competencia, mientras no se cree una autoridad diferente para este cometido en desarrollo del Convenio".

En segunda instancia, encontramos aquellos movimientos de datos personales de carácter transfronterizo que estén motivados para prestar o solicitar auxilio judicial internacional, cuya regulación se encuentra amparada en los artículos 276 a 278 de la Ley Orgánica del Poder Judicial[340], en relación con la cooperación jurisdiccional internacional. Un ejemplo de ello radica en lo previsto por el artículo 7.4 del Reglamento Penitenciario[341], que manifiesta el tenor literal siguiente: "[l]as transferencias internacionales de datos de carácter personal contenidos en los ficheros informáticos penitenciarios se efectuarán en los supuestos de prestación de auxilio judicial internacional, de acuerdo con lo establecido en los tratados o convenios en los que sea parte España".

Y en tercera y última instancia, se refiere a los movimientos transnacionales de datos cuando estos hagan referencia a transferencias dinerarias conforme a su legislación específica. El fundamento de dicha excepción se encuentra en la realización de actuaciones relacionadas con la prevención del blanqueo de capitales y la financiación del terrorismo, cuyas obligaciones quedan articuladas en España a través de la Ley 10/2010, de 28 de abril.

A modo de conclusión del presente apartado, entendemos conveniente, por un lado, traer a colación las palabras que tuvo la ocasión de pronunciar la Audiencia Nacional sobre el conjunto de excepciones analizadas, señalando el siguiente literal: "La existencia

[340] *Vid*. España. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Consultado el 11.07.2020 desde: https://www.boe.es/buscar/act.php?id=BOE-A-1985-12666.

[341] *Vid*. España. Real Decreto 190/1996, de 9 de febrero, por el que se aprueba el Reglamento Penitenciario. Consultado el 11.07.2020 desde: https://www.boe.es/buscar/doc.php?id=BOE-A-1996-3307.

de las mencionadas excepciones a la regla general en modo alguno significa, claro es, que en estos supuestos de inexigibilidad de la autorización previa el responsable del fichero que promueve la transferencia de datos quede liberado del conjunto de deberes y obligaciones que le impone la Ley Orgánica 15/1999; ni que pueda eludir las responsabilidades derivadas de su actuación. Únicamente queda liberado de la exigencia de autorización previa de la transferencia por el Director de la Agencia, y ello por disponerlo así de manera expresa el mencionado artículo 34"[342].

Y, por otro lado, hay que señalar que las garantías adecuadas que se han ido abordando a lo largo de los párrafos anteriores, tanto desde el punto de vista comunitario como del derecho nacional, pueden acreditarse a través de la adopción de dos mecanismos. Un contrato por escrito, celebrado entre el exportador y el importador, en el que consten aquellas garantías que las partes se comprometen a adoptar para garantizar la tutela de los derechos y libertades fundamentales de los afectados. O bien, cuando en el seno de grupos multinacionales de empresas existan normas internas que acrediten la adopción de garantías necesarias de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados. Ambos mecanismos serán abordados en los apartados venideros con mayor detalle.

5. Enfoque de las transferencias internacionales de datos de carácter personal bajo el acervo del Reglamento (UE) 2016/679, General de Protección de Datos. Mención a la Ley Orgánica 3/2018.

Una vez que se ha examinado el régimen previsto en la Directiva del 95/46/CE en lo concerniente a la institución jurídica de las transferencias internacionales de datos, cabe entrar a revisar los cambios que la reciente regulación europea ha supuesto para las mismas. En las siguientes líneas, se analizarán las principales modificaciones que se producido por la entrada en vigor y aplicación efectiva del Reglamento General de Protección de Datos. Se puede anticipar que la sistemática que se prevé no difiere en demasía de la que se contenía originariamente en la Directiva 95/46/CE, sino que se ha optado por reforzar algunos extremos que hasta el momento no ofrecían la seguridad jurídica que resulta aplicable a esta tipología de tratamientos de datos personales.

[342] *Cfr*. Fundamento jurídico 3º, de la Sentencia de la Sección Primera, de la Sala de lo Contencioso-Administrativo, de la Audiencia Nacional (nº de recurso: 271/2001), de 15 de marzo de 2002, sobre la interpretación de la Instrucción 1/2000 emitida por parte de la AEPD.

Con carácter previo a entrar a valorar el contenido en detalle, resulta preciso tener en cuenta un matiz importante, el cual radica en que el Reglamento no centra su objeto de protección en el derecho a la intimidad como lo hacía su predecesora[343], sino que lo hace en relación con el derecho a la protección de los datos personales[344], siguiendo lo preceptuado por el artículo 8.1 de la Carta de Derechos Fundamentales de la Unión Europea y el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea, donde se le considera un derecho autónomo y con carácter fundamental.

Así pues, en aras a propiciar un correcto equilibrio de intereses entre la expansión del comercio y los mecanismos de cooperación internacional frente a la salvaguarda del derecho fundamental a la protección de los datos de carácter personal[345], el régimen de las transferencias internacionales de datos previsto en el Capítulo V del RGPD ostenta una doble motivación. Por un lado, pretende facilitar el libre intercambio de datos a nivel internacional motivado por la creciente evolución tecnológica de la sociedad. Y, por otro lado, intentar salvaguardar al máximo posible los intereses en juego de los afectados por la recogida y tratamiento de sus respectivos datos personales[346].

Esta dualidad de objetivos ha pretendido irse tutelando a lo largo de la evolución y desarrollo del derecho a la protección de datos personales como hemos tenido la oportunidad de observar, siendo en el Reglamento donde encuentra su máxima expresión consagrada normativamente. Mediante este cuerpo normativo se consigue la articulación de un régimen jurídico específico que se verá reforzado por la eficacia directa que propicia esta tipología de instrumento comunitario —evitando así las disyuntivas existentes hasta el momento entre los distintos ordenamientos jurídicos de los Estados miembros—. A la vez que también aumentará la robustez de las garantías que deben adoptarse por parte de los sujetos obligados en el momento de llevar a cabo una

[343] *Vid*. Artículo 1, apartado primero, de la Directiva 95/46/CE.

[344] *Vid*. Artículo 1, apartado segundo, del RGPD.

[345] *Vid*. Considerando 101 del RGPD, anteriormente Considerando 56 de la Directiva 95/46/CE.

[346] *Vid*. PIÑAR MAÑAS, J. L., "Transferencias de datos personales a terceros países u organizaciones internacionales", en PIÑAR MAÑAS, J. L. (Dir.)., *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad*, Madrid: Reus, 2016, pp. 431-460.

transferencia internacional de datos de carácter personal, dotándola de una mayor seguridad jurídica[347].

El Reglamento ampara el nuevo régimen previsto con mayor detalle que lo hacía la Directiva 95/46/CE pues, como ejemplo de ello, pasamos de ver un régimen que se ventilaba en dos artículos —del 25 al 26—, a encontrar el Capítulo V, conformado por 7 artículos —del 44 al 50— encargados de regular esta institución jurídica. Se parte de la misma premisa que se venía optando hasta el momento, pero adecuada a las nuevas realidades que se han ido sucediendo dado que, al margen de los supuestos de excepción —previstos en el artículo 49— que se abordaran en las líneas venideras. Se han previsto tres grandes casuísticas generales que operan sobre el marco de un principio general de prohibición, las cuales son: (i) transferencias basadas en una decisión de adecuación (artículo 45); (ii) transferencias mediante garantías adecuadas (artículo 46); y (iii) supuestos relativos a las normas corporativas vinculantes (artículo 47).

En primer lugar, en el artículo 44 del RGPD se prevé un principio de prohibición general en consonancia con la tradición histórica de la institución que encuentra su única excepción cuando el país, territorio, sector u organismo internacional[348] destinatario de los datos personales objeto de transferencia ofrezca un nivel de protección adecuado, se aporten las suficientes garantías que permitan la viabilidad de la operación o, en su defecto, el supuesto de hecho concreto se pueda enmarcar en alguna de las circunstancias establecidas como excepciones, de conformidad con el texto del Reglamento.

En segundo lugar, el planteamiento de las decisiones de adecuación contenido en el artículo 45 cambia parcialmente de perspectiva respecto de lo que preceptuaba la

[347] *Vid*. DÍAZ DÍAZ, E., "El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones", en *Revista Aranzadi Doctrinal*, nº 6 (2016), pp. 155-190.

[348] Se ha ampliado el espectro de destinatarios de los datos personales en el marco de las transferencias internacionales, dado que en la anterior Directiva 95/46/CE el eje vertebrador se focalizaba sobre la figura del "tercer país", pero en la actual regulación vemos como se ha optado por introducir adicionalmente un nuevo concepto de "organización internacional", y que aparece inicialmente recogido como parte del texto incluido en el título del Capítulo V del RGPD —dedicado a regular esta materia—, convirtiéndose, por ende, en toda una declaración de intenciones. A este respecto, cabe recordar que las decisiones de adecuación permiten realizar las transferencias de datos personales sin que el exportador de los datos deba aportar las garantías adicionales, así como tampoco solicitar ningún tipo de autorización, pues la condición del país de destino será la misma que cualquier Estado miembro por lo que a los movimientos de datos personales se refiere, gozando de los beneficios económicos que esta posición ventajosa puede suponer.

anterior regulación[349], que dejaba esencialmente en manos de los Estados miembros esta decisión. Tal y como se desprende del tenor literal introducido en el artículo 25, apartado primero, de la ya reiterada Directiva, cuando establecía que: "[l]os Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado".

No obstante lo anterior, el propio artículo aludido, en su apartado sexto, facultaba a la Comisión para que pudiera efectuar un reconocimiento similar al otorgado a los Estados miembros. Pero en este caso la decisión adoptada gozaría de plenos efectos en todo el territorio comunitario, no únicamente en el marco de la soberanía nacional que se le reconoce a cada Estado miembro. Tal potestad ha sido efectivamente ejercida por parte de la Comisión a lo largo de los últimos años, máxime si tenemos en cuenta que, en la actualidad, las autoridades de control europeas no han realizado pronunciamientos individuales al respecto, constituyéndose una facultad que, en la práctica, le ha quedado reservada en régimen de exclusividad al citado organismo europeo.

Como consecuencia del planteamiento aducido, el Reglamento parte de esta concepción como la única posibilidad por antonomasia, siendo la Comisión Europea el único ente habilitado para realizar el reconocimiento de una decisión de adecuación respecto de un tercer país o una organización internacional, para que este sea considerado como un destino que garantiza un nivel de protección adecuado en materia de protección de datos de carácter personal[350]. Todo ello sin perjuicio de que la autoridad de control nacional competente siga ostentando las potestades relativas a impedir ciertos

[349] Conviene subrayar al respecto la importancia de la Decisión 2008/615/JAI del Consejo, 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, así como la Decisión marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, dado que intenta salvaguardar la ausencia de regulación que establece la Directiva 95/46/CE sobre este asunto debido a la exclusión que se efectúa sobre aquellos datos que tengan como objetivo la seguridad pública y las actividades del Estado en el ámbito penal.

[350] Siguiendo el mandato establecido en el RGPD, la Ley Orgánica 3/2018 recoge esta obligación, y en el apartado primero del artículo 42 se incluye una remisión a lo dispuesto en el apartado segundo del artículo 46 del RGPD, en relación con los supuestos de transferencias internacionales que precisan de autorización previa por parte de la autoridad de control competente. En este caso, las competencias son ejercidas por la AEPD.

movimientos transfronterizos de datos, en caso de que se puedan poner en jaque ciertos derechos fundamentales de los afectados[351].

Avanzando en nuestro razonamiento, resulta conveniente remarcar que los criterios que se seguían en la Directiva 95/46/CE para evaluar la consideración relativa al nivel de protección adecuado[352] no resultaban tan extensivos como los que se apuntan en el nuevo régimen previsto en el RGPD. Destacándose especialmente, cuando se refiere, entre otras cuestiones, a la valoración sobre "el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles, de recursos administrativos y de acciones judiciales que sean efectivos"[353].

Desde un punto de vista pragmático, resulta dificultosa la revisión de todas las consideraciones reproducidas con anterioridad en jurisdicciones como la estadounidense, donde la legislación sobre la materia es ampliamente sectorial —que incluso es tildada de incurrir en una técnica legislativa basada en la dispersión normativa— y respaldada por mecanismos de autorregulación. Las precisiones acotadas por el Reglamento adoptan una importancia trascendental a la hora de determinar la viabilidad de una decisión, pero en

[351] Un ejemplo de lo anterior lo vimos con la invalidez del acuerdo de Puerto Seguro y, posteriormente, con el Escudo de Privacidad, ambos marcos contractuales fueron invalidados gracias a esta facultad reservada para las autoridades de control nacionales —tal y como tendremos oportunidad de tratar—. Ello se motiva en los artículos 7, 8 y 47 de la CDFUE.

[352] En referencia a este punto, el artículo 25, apartado segundo, establecía que: "[e]l carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".

[353] *Vid.* Artículo 45, apartado 2º, letra a), del Reglamento General de Protección de Datos.

la práctica su correspondiente evaluación puede llegar a lastrar determinadas actividades mercantiles.

A este respecto, cabe recordar las consideraciones manifestadas por parte del GT29, que en consonancia con la doctrina expuesta por el TJUE en el caso "Schrems I"[354], señala que: "[l]a finalidad de las medidas de adecuación de la Comisión Europea es confirmar formalmente con efectos vinculantes para los Estados miembros que el nivel de protección de datos en un tercer país u organización internacional es sustancialmente equivalente al nivel de protección de datos en la Unión Europea. Se puede lograr la adecuación a través de una combinación de derechos para los interesados y obligaciones para aquellos que realizan el tratamiento de los datos, o que ejercen control sobre dicho tratamiento, y la supervisión por parte de organismos independientes. No obstante, las normas de protección de datos solo resultan efectivas si son exigibles y se siguen en la práctica. Por tanto, se debe tener en cuenta no solo el contenido de las normas aplicables a los datos personales transferidos a un tercer país u organización internacional, sino también el sistema existente para garantizar la efectividad de dichas normas"[355].

De ahí que, una vez valorados todos los elementos que preceptúa el artículo 45, apartado segundo, del RGPD, se faculta a la Comisión para que decida mediante un acto de ejecución[356], si un tercer país u organización internacional goza de un nivel de protección adecuado. Si ello se produce, resulta obligatorio que ese concreto acto de ejecución lleve aparejado un procedimiento de revisión, de al menos cada cuatro años, que permita valorar periódicamente las circunstancias que llevaron a la consecución de tal decisión. Sobre este punto, el GT29 ha considerado necesario matizar que se trata de un plazo orientativo que debe ser ajustado a cada situación en particular, dado que quizás,

---

[354] En relación con esta cuestión, el GT29 establece sobre el concepto de "nivel de protección adecuado" el siguiente tenor literal: "Ya existía en la Directiva 95/46, ha sido ampliado por el TJUE. En este punto, conviene recordar la norma establecida por el TJUE en el asunto Schrems, en particular que, aunque el «nivel de protección» en el tercer país debe ser «sustancialmente equivalente» al garantizado en la UE, «los medios de los que se sirva ese tercer país para garantizar ese nivel de protección pueden ser diferentes de los aplicados en la [UE]». Por tanto, el objetivo no es reflejar punto por punto la legislación europea, sino establecer los requisitos esenciales y básicos de dicha legislación". *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 254): Referencias sobre adecuación", aprobadas por el Grupo de Trabajo, el 28 de noviembre de 2017, revisadas por última vez y adoptadas el 6 de febrero de 2018, p. 3.

[355] *Ibidem.*

[356] *Vid*. Artículo 291 del Tratado de Funcionamiento de la Unión Europea. Consultado el 15.08.2017 desde: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:12012E291.

en determinadas circunstancias, pueda ser preciso que la revisión se efectúe en un período de tiempo más corto[357].

En este mismo sentido, cabe destacar que el Reglamento sigue manteniendo la vigencia de aquellas autorizaciones emitidas por los Estados miembros y/o sus autoridades de control, así como de aquellas decisiones adoptadas por la Comisión[358] —en el ejercicio de sus competencias—, en tanto en cuanto no resulten modificadas, sustituidas o derogadas. Por ende, se mantiene plenamente vigente el listado de países que gozan de un nivel de protección adecuado hasta la fecha, a excepción de los Estados Unidos, tal y como en los próximos apartados tendremos la ocasión de analizar.

En tercer lugar, vemos como el artículo 46 del RGPD aborda las garantías adecuadas como mecanismo a aplicar ante la inexistencia de una decisión de adecuación. Las mismas podrán llevarse a cabo si se cumplen dos condicionantes cumulativos que han sido objeto de introducción en el Reglamento[359], esto es, la imperiosa necesidad de que los interesados dispongan de "derechos exigibles" y "acciones legales efectivas". Ello se traduce en un intento de reforzar las garantías de las que disponen los afectados sobre el control de sus respectivos datos personales, a través de la introducción de esta presunción favorable.

En relación con lo manifestado en el párrafo anterior, se ha procedido a la división de las garantías adecuadas en dos tipologías diferenciadas. Por un lado, aquellas en que no se precisa ninguna autorización expresa por parte de una autoridad de control nacional[360] —aspecto que simplifica las cargas burocráticas—. Por otro lado, aquellas que precisan de dicha una autorización. Respecto de la primera de las tipologías expuestas, la misma se ha tenido en cuenta para ampliar el catálogo de instrumentos que hasta la fecha se encontraban disponibles respecto de su anterior regulación —esto es, la

[357] *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 254): Referencias…", cit., p. 3.

[358] A este respecto, cabe mencionar aquellos países que en la actualidad gozan de un nivel de protección adecuado, que se pueden encontrar detallados en el apartado dedicado al nivel de protección adecuado del presente trabajo.

[359] *Vid*. Artículo 46, apartado 1º, del Reglamento General de Protección de Datos.

[360] *Vid*. Artículo 46, apartado 2º, del Reglamento General de Protección de Datos.

Directiva 95/46/CE—[361]. Se trata de los códigos de conducta y los mecanismos de certificación aprobados de conformidad con lo establecido en el artículo 42 del RGPD[362].

Una de las alternativas que se contemplan dentro de este primer grupo de instrumentos que no precisan de autorización radica en las Normas Corporativas Vinculantes (en adelante, NCV), en que el Reglamento ha optado por su reconocimiento legal[363]. En consecuencia, habrán de entenderse como un mecanismo válido para ser utilizado por los grupos y/o conglomerados de empresas multinacionales que precisan, para la correcta gestión de sus negocios y actuaciones jurídicas, un elevado número de operaciones transfronterizas con datos personales. Dicha situación ha ido favoreciendo gradualmente en los últimos años la adopción de este tipo de instrumentos.

Dicho reconocimiento ha sido posible como consecuencia del arduo trabajo llevado a término por el Grupo de Trabajo del Artículo 29[364], con la intención de posibilitar la utilización de las NCV en aquellos Estados miembros donde su validez y utilización no estaba legalmente amparada. Así pues, a diferencia de la Directiva, en que

---

[361] Cabe destacar a este respecto que la LOPD no recogía en su contenido mención alguna sobre las NCV, sino que es el RLOPD el único que las menciona como mecanismo a través del cual puede obtenerse la autorización del Director/a de la AEPD en aras de posibilitar la transferencia internacional de datos que se pretenda articular. En cualquier caso, resulta oportuno afirmar que el RLOPD tampoco da detalles sobre dicha figura, sino que todo el contenido debía obtenerse de los distintos pronunciamientos que había realizado al respecto el GT29. A este respecto, la propia doctrina civilista española planteó serias dudas sobre el carácter vinculante de las NCV, fue la AEPD la que se encargó de establecer el criterio manifestando que "los tratamientos de datos llevados a cabo en territorio español quedarán en todo caso sometidos a la LOPD y su normativa de desarrollo, siendo las NCV en lo que se refiere a tales tratamientos meramente complementarias de lo previsto en dicha normativa. De este modo, si las exigencias contenidas en las NCV, aun cuando pudieran ser suficientes para amparar una transferencia internacional de datos, fueran menos estrictas que las previstas en la legislación española, será esta la que se aplique en lo referente a los tratamientos de datos efectuados dentro del ámbito de aplicación establecido en el artículo 2.1 de la LOPD y 3 del RLOPD". *Vid*. GUASCH PORTAS, V., "La transferencia internacional…", *op. cit.*, pp. 413-453.

[362] Se reproduce, a continuación, el tenor literal del artículo 46.2, letra f), en cuestión: "[…] junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados".

[363] La anterior Directiva 95/46/CE dejaba en el ámbito de competencia de los Estados miembros si resultaba preciso obtener autorización previa por parte de la autoridad de control competente. En el caso de España, ello se había preceptuado como obligatorio, siendo la AEPD el órgano competente para realizar tales pronunciamientos. Con la entrada en vigor y aplicación efectiva del RGPD, el escenario es diferente, pues a través de este reconocimiento legal se permiten los movimientos de datos personales dentro de un mismo grupo empresarial, sin resultar obligatoria la tramitación de la autorización previa.

[364] *Vid*., entre otros: COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 107): Procedimiento de Cooperación para el Establecimiento de una Opinión Común sobre la Adecuación de las Medidas Adoptadas en las Binding Corporate Rules", aprobadas por el Grupo de Trabajo el 14 de abril de 2005.

era la autoridad de control considerada líder la que habilitaba las NCV como consecuencia de la autorización previa, el Reglamento cambia de perspectiva y elimina este supuesto al no precisarse la misma. No obstante, en la actualidad, al amparo de lo establecido en el mecanismo de coherencia del artículo 63, será también la autoridad de control nacional competente la encargada de aprobarlas, siempre que se dé estricto cumplimiento de las obligaciones preceptuadas en el artículo 47 al que venimos haciendo mención específica[365].

A este respecto, conviene señalar que el RGPD parte de tres condiciones básicas para apreciar la validez y posterior aprobación de las NCV. En primer término, exige que el conjunto de reglas sea jurídicamente vinculante para todos los miembros del grupo empresarial o unión de empresas. En segundo término, obliga a que los interesados dispongan de medios efectivos para hacer valer sus derechos o pretensiones. Y, en tercer y último término, que se cumplan los requisitos incluidos en el listado facilitado por el artículo 47.2 del RGPD.

En palabras de Grande Sanz, "[a]unque con relación a las RCV[366] puede distinguirse entre las RCV dirigidas a los responsables (WP74, WP107, WP108, WP133, WP153, WP154 y WP155 del GT29) y las RCV para encargados (WP195, WP195a y WP204 del GT29), con carácter general, este tipo de reglas suelen contemplar los siguientes aspectos: a) el respeto a los principios de protección de datos de la UE y de los Estados miembros; b) la determinación de los flujos de información y de los fines del tratamiento; c) la posible limitación de las transferencias a entidades del grupo o de las transferencias posteriores bajo el esquema de garantías; d) la obligatoriedad interna y externa de las RCV; e) la posibilidad de obtener una reparación e indemnización por parte del afectado o de plantear, en su caso, recursos; f) los procedimientos para su ejecución;

[365] En cualquier caso, se deberán tener en cuenta las consideraciones previstas en el artículo 93, apartado segundo, del RGPD, que incluye una remisión al artículo 5 del Reglamento (UE), nº 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión.

[366] A efectos aclaratorios, conviene precisar que con la utilización del acrónimo RCV, la autora se está refiriendo a lo que en este trabajo hemos venido a denominar bajo el acrónimo NCV, relativo a la nomenclatura utilizadas para hacer alusión a las Normas Corporativas Vinculantes.

g) la cooperación con las autoridades de control; h) el procedimiento de actualización; e i) la jurisdicción competente"[367].

Otra de las alternativas disponibles para efectuar el movimiento de datos transnacional sin necesidad de recabar la previa autorización expresa por parte de la autoridad de control, radica en la acreditación del cumplimiento de las garantías suficientes mediante la aportación de CCT[368] aprobadas por la Comisión Europea[369], cuya regulación ya la encontrábamos en la antigua Directiva 95/46/CE[370], al igual que también lo reconoce el RGPD[371]. En su versión inicial, se encontraban disponibles para dos supuestos de hecho específicos en el marco de las transferencias internacionales de datos personales: por un lado, cuando el movimiento se producía entre responsables del tratamiento[372], y, por otro lado, cuando el flujo de datos transnacionales se producía entre un responsable respecto de un encargado del tratamiento de los datos[373].

Mientras que las primeras regulaban los movimientos de datos entre responsables cuando uno de ellos estuviera establecido en un tercer estado situado fuera del EEE, las segundas daban cobertura sobre los flujos transfronterizos de datos entre un responsable situado en el EEE respecto de un encargado que estuviera situado fuera del mismo. Así entonces, encontramos divergencias en el contenido de ambos documentos, pues las

---

[367] *Cfr*. GRANDE SANZ, M., "La transferencia internacional…", *op. cit*., pp. 4-5.

[368] Para un análisis detallado sobre las cláusulas contractuales tipo y su evolución histórica, *vid*., entre otros: GUASCH PORTAS, V. y SOLER FUENSANTA, J. R., "Cloud computing: cláusulas contractuales y reglas corporativas vinculantes", en *Revista de Derecho – Universidad Nacional de Educación a Distancia (UNED)*, nº 14 (2014), pp. 257-260.

[369] Con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado segundo, del RGPD.

[370] *Vid*. Artículo 26, apartado cuarto, de la Directiva 95/46/CE.

[371] *Vid*. Artículo 46, apartado segundo, letras c) y d), del RGPD.

[372] *Vid*. (I) Decisión de la Comisión (2001/497/CE), de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE; (II) Decisión de la Comisión (2010/87/CE), 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/CE del Parlamento Europeo y del Consejo —produce la derogación de la Decisión de la Comisión (2002/16/CE), de 27 de diciembre de 2001—. Consultado el 17.08.2020 desde: (I) https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A32001D0497; (II) https://eur-lex.europa.eu/legal-content/ES/TXT/?uri= celex%3A32010D0087.

[373] *Vid*. Decisión de la Comisión (2004/915/CE), de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países. Consultado el 17.08.2020 desde: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri= CELEX%3A32004D0915.

casuísticas a contemplar suponían la asunción de obligaciones jurídicas claramente distintas. Sobre todo, en el último de los casos citados, donde el encargado del tratamiento estará actuando en todo momento bajo las directrices que le marque exclusivamente el responsable[374].

Sobre esta cuestión, resulta oportuno citar también que ante la incertidumbre existente respecto de las transferencias internacionales de datos personales entre un encargado establecido en el ámbito del EEE respecto de un subencargado situado fuera del mismo[375], La AEPD —a pesar de su inicial reticencia en publicarlas— emitió unas cláusulas contractuales aplicables ante estos supuestos[376], como hemos tenido la ocasión de observar con anterioridad.

Vemos entonces como el aspecto esencial de las CCT radicaba en que, por un lado, permitía que el solicitante de la transferencia pudiera ser directamente el encargado del tratamiento —cuando siempre había resultado preciso que la solicitud la tramitara el responsable—. Y, por otro lado, la viabilidad del clausulado quedaba supeditada a la existencia de un contrato principal entre el responsable y el encargado que habilitase la

[374] A este respecto, no es cuestión baladí señalar que el Reglamento ha equiparado la posición jurídica del encargado a la del responsable del tratamiento, haciéndole extensibles las mismas obligaciones que hasta el momento únicamente eran aplicables a los responsables por lo que atañe al cumplimiento de la legislación vigente en materia de protección de datos de carácter personal. Todo ello viene propiciado por las dificultades que hasta el momento se venían sucediendo para efectuar la subcontratación de terceros para la prestación de determinados servicios en terceros países, intentando favorecer así tales cuestiones, siempre que se respeten las obligaciones preceptuadas por la legislación aplicable.

[375] El Grupo de Trabajo del Artículo 29, pese abordar la cuestión, no ha optado por ninguna alternativa expresamente, aspecto que ha propiciado que, en estos supuestos, existiera cierto grado de inseguridad jurídica cuando se optaba por los mismos. *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 176): Preguntas frecuentes para abordar algunas cuestiones planteadas por la entrada en vigor de la Decisión 2010/87/UE de la Comisión de la UE, 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/CE", aprobadas por el Grupo de Trabajo el 12 de julio de 2010.

[376] A tenor de lo comentado, cabe recordar que, a efectos del artículo 26, apartado 2, de 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; y 33 y 70.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter General (LOPD) y de su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RLOPD), respectivamente, la AEPD aprueba las cláusulas contractuales para la transferencia de datos personales a los subencargados del tratamiento establecidos en terceros países que no garanticen una adecuada protección de los datos personales.

subcontratación, así, como en su caso, las eventuales transferencias internacionales que su ejecución pudiera suponer[377].

A efectos sumatorios sobre sobre la versión inicial del contenido de las Cláusulas Contractuales Tipo, resulta oportuno traer a colación las observaciones de Grande Sanz, cuando afirma que: "[e]n las CCT se suelen contemplar los siguientes aspectos: a) una estipulación a favor de un tercero para que el afectado pueda hacer valer el contrato en caso de vulneración; b) una cláusula de responsabilidad solidaria entre las partes (responsable-responsable) o basada en *culpa in eligendo* o *in vigilando* o subsidiaria (responsable-encargado); c) la restricción de las transferencias posteriores; d) una cláusula sobre seguridad y control del cumplimiento de las garantías y de los compromisos establecidos en las CCT; y e) una estipulación impidiendo la modificación de las cláusulas a favor de tercero[378]".

Por último, sobre el contenido de las CCT que se viene analizando, conviene indicar que el mismo ha sufrido una modificación sustancial respecto su versión inicial. La Decisión de Ejecución (UE) 2021/914 de la Comisión, de 4 de junio, contempla la posibilidad de que puedan ser utilizadas tanto por el responsable como por el encargado del tratamiento. Como se ha indicado en el capítulo anterior, el documento preserva la estructura modular introducida en su proyecto inicial sometido a consulta pública, previendo cuatro escenarios posibles: i) de responsable a responsable; ii) de responsable a encargado; iii) de encargado a encargado; y, iv) de encargado a responsable. En cualquier caso, uno de los puntos relevantes recae en que, si el tratamiento de datos proyectado prevé la posibilidad de que el responsable o el encargado sujeto al RGPD, deba de realizar una transferencia fuera de la Unión, el uso de las CCT permitirá dar cumplimiento a las obligaciones establecidas en el artículo 28, apartados 3 y 4 del RGPD.

En consonancia con el orden que se viene formulando, cabe resaltar aquellas garantías adecuadas que precisan de una autorización de la autoridad de control nacional competente para desplegar su efectividad[379]. Estas podrían ser aportadas mediante "cláusulas contractuales entre el responsable o el encargado y el responsable, encargado

---

[377] *Vid*., entre otros: GUASCH PORTAS, V. y SOLER FUENSANTA, J. R., "Cloud computing: cláusulas…", *op. cit.*, pp. 261-264.

[378] *Cfr*. GRANDE SANZ, M., "La transferencia internacional…", *op. cit.*, p. 4.

[379] *Vid*. Artículo 46, apartado tercero, del RGPD.

o destinatario de los datos personales en el tercer país u organización internacional" o "disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados".

Se ha incluido esta posibilidad en el Reglamento, en aras de facilitar mecanismos alternativos a los que se habían previsto históricamente en la Directiva. En particular, resultan necesarios en determinados sectores de actividad o modelos de negocio, en que, por su especial casuística, ostentan características o necesidades particulares que motivan que se prevean soluciones adaptadas a sus exigencias en materia de movimientos transfronterizos de datos de carácter personal.

En cuarto lugar, resulta preciso hacer alusión a uno de los últimos artículos que el Reglamento recoge sobre la materia objeto de análisis, esto es, los supuestos de excepción para situaciones específicas[380], que, en gran medida, resultan similares a los estipulados en la anterior regulación —esto es, la Directiva 95/46/CE—, y especialmente, en lo recogido en el artículo 34 de la LOPD. Dichas excepciones facultan a los sujetos obligados para que, en determinados supuestos, puedan ejecutar transferencias internacionales de datos personales sin disponer de una decisión de adecuación o de las garantías adecuadas referenciadas con anterioridad.

Aunque como se viene indicando, la previsión de este régimen de excepciones no supone ninguna novedad sustancial, sí que se han incluido ciertas precisiones que deben de tenerse en cuenta en la práctica, siempre que se opte por la aplicación de alguna de ellas. Al no tratarse de una cuestión baladí, el CEPD también ha creído conveniente pronunciarse al respecto, viniendo a completar y adecuar lo previsto en el WP114, a través de sus nuevas Directrices emitidas sobre este asunto[381], en aras de efectuar una interpretación estricta respecto de la utilización de cada uno de los supuestos como ya lo hizo en su momento el GT29[382] respecto de lo previsto en la Directiva[383].

---

[380] *Vid*. Artículo 49, apartado primero, del RGPD.

[381] *Vid*. COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, "Directrices 2/2018 sobre las excepciones al artículo 49 del Reglamento 2016/679", adoptadas el 25 de mayo de 2018. Consultado el 11.07.2020 desde: https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22018-derogations-article-49-under-regulation_en.

[382] *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 12): Transferencias…", *op. cit.*, pp. 5-28.

[383] *Vid*. Artículo 26 de la Directiva 95/46/CE.

En este mismo sentido, podemos destacar, en primera instancia, que se han previsto ciertas consideraciones respecto de la utilización del consentimiento del interesado como mecanismo de excepcionalidad para posibilitar una transferencia de datos de carácter personal. En este punto, se ha introducido la necesidad de que el afectado haya "sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas"[384]. El deber de información deberá realizarse siempre con carácter previo, recogiéndose así las reiteradas peticiones que se habían venido formulando al respecto, en los últimos tiempos, por parte del GT29[385].

Asimismo, y en línea con lo propugnado por el texto del propio Reglamento, así como por las interpretaciones del mismo efectuadas por el ya referido GT29, se indica en sus nuevas Directrices que el consentimiento deberá de ser explícito —sin ambigüedad alguna—, específico para la transferencia o el conjunto de transferencias que se pretendan efectuar al amparo de la excepción, así como informado sobre los riesgos que la misma puede conllevar en línea con lo expresado en el párrafo anterior, atendiendo especialmente a las obligaciones de transparencias preceptuadas en los artículos 13 y 14 del RGPD.

En consecuencia, a la luz de lo expuesto —por lo que a la interpretación restrictiva del uso de la excepción se refiere—, así como de la dificultad práctica que supone para las organizaciones la utilización del consentimiento como base de legitimación suficiente para articular una transferencia internacional de datos fuera del EEE. Se puede concluir afirmando que esta base jurídica no resulta recomendable para los responsables del tratamiento, pues la carga de la prueba resulta complicada en escenarios digitalizados. A pesar de que en la actualidad existen medios técnicos que permiten, aunque sea parcialmente, acreditar su obtención.

En segunda instancia, en relación con la figura del interés público, el CEPD introduce ciertas apreciaciones que resulta conveniente mencionar[386], pues indica que el

[384] *Cfr*. Artículo 49, apartado primero, letra a), del RGPD.

[385] *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 114): relativo a una interpretación…", cit., p. 14. Adicionalmente, debe ser complementado. *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 259): Directrices…", cit., pp. 20-21.

[386] *Vid*. COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, "Directrices 2/2018…", cit., p. 10.

mismo debe estar previsto en la legislación de la Unión Europea —incluyéndose la legislación interna de los Estados miembros—. Ello se traduce en que la referida legislación a la que esté sujeto el responsable del tratamiento deberá posibilitar las transferencias para cuestiones derivadas del interés público, así como también lo deberá reconocer la del territorio de destino de los datos —principio de reciprocidad—. El CEPD aprovecha para recordar que el uso de esta excepción no está limitado a los poderes públicos, sino que también la pueden utilizar entes privados.

En tercera instancia, el Reglamento ha habilitado una especie de "cajón de sastre" —que no estaba previsto en la Directiva 95/46/CE— a través del último inciso del apartado primero del artículo 49, cuando se afirma el tenor literal siguiente: "[c]uando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos". Lo anterior entra en contradicción, a nuestro entender, con las intenciones de protección que se contienen en los propios considerandos del RGPD.

Aunque el redactado del texto está orientado hacia la acumulación de requisitos que deberían dificultar su aplicabilidad, cierto es que será interesante esperar la interpretación que se efectúe por parte de las autoridades de control sobre cada uno de los condicionantes que se incluyen. En su inmensa mayoría, se trata de conceptos jurídicos indeterminados, que pueden suponer el riesgo de inmiscuirse en interpretaciones distanciadas del principio de seguridad jurídica, tal y como podría ocurrir, a título ejemplificativo, con la institución de los "intereses legítimos imperiosos", cuya utilización en la práctica se ha acotado a supuestos concretos tasados.

Sobre esta excepción, el CEPD ha tenido ocasión de pronunciarse, indicando que: *"[t]his can only be used in residual cases according to recital 113 and is dependent on a significant number of conditions expressly laid down by law. In line with the principle of accountability enshrined in the GDPR the data exporter must be therefore able to demonstrate that it was neither possible to frame the data transfer by appropriate safeguards pursuant to Article 46 nor to apply one of the derogations as contained in Article 49 (1) § 1*"[387].

En definitiva, podemos concluir afirmando que se han realizado diversas matizaciones sobre el texto que ya incorporaba la anterior Directiva —y, por ende, la derogada LOPD—, que han venido a clarificar, pero sobre todo a acotar, las interpretaciones que se podían efectuar de las diversas excepciones que se preveían. Fruto todo ello, de la experiencia que se ha ido acumulado en los últimos años, como consecuencia de su aplicación práctica.

No obstante, llegados a este punto, conviene citar las reflexiones realizadas por Sancho López —con las que no se puede estar más de acuerdo—, cuando manifiesta que: "[...] es ingenuo pensar que la finalidad última del Reglamento es acabar con la desprotección de los ciudadanos europeos, nada más lejos de la realidad pues lo que realmente quiere evitarse es que se continúen produciendo obstáculos para el mercado interior de la UE, lo que dificulta el ejercicio de actividades económicas a escala comunitaria y está provocando un falseamiento de la competencia"[388].

A modo de conclusión del presente apartado, debe hacerse mención obligatoria a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), que, tal y como preceptúa la propia Disposición derogatoria única que en la misma se contiene, trae consigo la derogación de la Ley Orgánica 15/1999. A este respecto, debemos indicar que su aprobación no supone ninguna novedad, pues parece ser que se ha optado por la costumbre de que las normas que se encargan de transponer la normativa comunitaria a nuestro maltrecho ordenamiento jurídico no aportan cuestiones de calado, sino que, lejos de incluir mejoras

[387] *Vid*. COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, "Directrices 2/2018…", cit., p. 14.

[388] *Cfr*. SANCHO LÓPEZ, M., "Consideraciones procesales del ejercicio del derecho al olvido: examen de jurisprudencia reciente y del nuevo marco legal", en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 41 (2016), pp. 1-17.

respecto de lo previsto por el legislador europeo, en determinados aspectos la LOPDGDD supone incluso una merma de garantías.

A este respecto, y con fundamento en lo apuntado en el párrafo anterior, cabe mencionar con carácter obligatorio la nota de prensa[389], publicada en fecha 26 de julio de 2017, por parte del Consejo General del Poder Judicial[390] (en adelante, CGPJ), en que se daba a conocer que el pleno del susodicho órgano había aprobado, con carácter unánime, el informe elaborado en lo relativo a la transposición del RGPD al ordenamiento jurídico español[391], estableciendo al respecto que: "Se advierte en el anteproyecto una cierta falta de coherencia con la función y finalidad propia de una norma que ha de limitarse a adecuar y, en su caso —y con la configuración que ha hecho la jurisprudencia europea de esta función—, a complementar el Reglamento europeo. En ocasiones, señala el informe, el articulado propuesto traspasa los límites de esas funciones, pues algunos artículos resultan innecesarios, otros reiterativos y otros van más allá en sus marcos reguladores"[392].

Ante esta tesitura, el redactado del que se ha dotado al nuevo cuerpo legal realiza una adaptación de lo estipulado en el RGPD, así como incluye ciertas particularidades relacionadas con los mecanismos mediante los cuales las autoridades de control nacionales pueden realizar ciertas actividades y desplegar, por ende, el ejercicio de sus competencias. Todo ello se ha articulado mediante la introducción del Título VI dedicado a las transferencias internacionales de datos (artículos 40 a 43).

---

[389] *Vid*. Nota de prensa emitida por parte del Consejo General del Poder Judicial, de fecha 26 de julio de 2017. Consultado el 15.08.2017 desde: http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Consejo-General-del-Poder-Judicial/Sala-de-Prensa/Notas-de-prensa/El-CGPJ-propone-articular-un-procedimiento-judicial-completo-para-resolver-las-reclamaciones-contra-las-transferencias-internacionales-de-datos-personales.

[390] España. El artículo 122, ap. segundo de la Constitución española de 1978 define el Consejo General del Poder Judicial como "órgano de gobierno del mismo". Consultado el 15.08.2017 desde: https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf.

[391] A este respecto, conviene indicar que en fecha 23 de junio de 2017 se hacía pública una nota de prensa efectuada por el Ministerio de Justicia en la que se daban a conocer las principales novedades que incorporaba el anteproyecto. Consultado el 15.08.2017 desde: http://www.mjusticia.gob.es/cs/Satellite/Portal/1292428446044?blobheader=application%2Fpdf&blobheadername1=ContentDisposition&blobheadername2=Medios&blobheadervalue1=attachment%3B+filename%3D170623_Anteproyecto_LO_Protecci%C3%B3n_de_Datos.pdf&blobheadervalue2=1288795476854

[392] *Cfr*. Nota de prensa emitida por parte del Consejo General del Poder Judicial, de fecha 26 de julio de 2017, cit.

En este sentido, cabe mencionar como aspectos más significativos en lo que a este estudio interesa, en primer término, los plazos que se incluyen en sus artículos 41 y 42, respectivamente. El primero de ellos indica que el plazo de duración de un procedimiento orientado a la aprobación de las NCV tendrá una duración máxima de nueve meses, quedando en suspensión como consecuencia de la remisión del expediente al CEPD. El segundo de ellos alude al plazo de seis meses del procedimiento por el que se recaba la autorización de la AEPD o, en su caso, de las autoridades autonómicas, cuando el país de destino de los datos no disponga de una decisión de adecuación o no se aplique ninguna de las garantías adecuadas.

En segundo término, como hemos identificado, se incluyen una serie de potestades de las autoridades de control autonómicas que podrían suponer una merma de las competencias asignadas históricamente a la Agencia Española de Protección de Datos. Máxime, si tenemos en cuenta, que se estarían obviando los pronunciamientos judiciales efectuados al respecto por parte del Tribunal Constitucional, incluidos en la sentencia analizada con anterioridad, de fecha 30 de noviembre de 2000.

Y, en tercer término, resulta oportuno señalar que se ha incluido una Disposición adicional quinta relativa a la autorización judicial en relación con decisiones de la Comisión Europea en materia de transferencia internacional de datos, que tampoco ha estado exenta de crítica desde que la misma se recogió en el Anteproyecto. De hecho, la nota de prensa antes mencionada manifestaba que el eje central del informe del CGPJ se había desarrollado en torno a este precepto, resaltándose la sugerencia efectuada sobre la introducción de mejoras técnicas en su redacción, que resultasen alineadas con las preceptuadas por el derecho alemán. De hecho, el CGPJ manifestó literalmente que consideraría más adecuado que la nueva legislación sobre la materia previese *"*la completa configuración de un procedimiento judicial desde el cual se va a entablar el diálogo prejudicial, a raíz de la solicitud de la decisión judicial formulada por la autoridad de control que conoce de la reclamación, y cuya resolución depende de la validez de la decisión de la Comisión"[393].

[393] *Ibidem.*

CAPÍTULO II – TRANSFERENCIAS INTERNACIONALES DE DATOS A LOS ESTADOS UNIDOS DE AMÉRICA

SUMARIO: 1. Estados Unidos de América y su particular concepción de *"privacy"*; 2. Evolución de la Decisión de la Comisión, de 26 de julio de 2000, sobre los principios de Puerto Seguro ("*Safe Harbor*"); 3. Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015, asunto C-362/14 ("Schrems I"); 4. Nuevo paradigma para las transferencias internacionales de datos a Estados Unidos. El novedoso "*EU–U.S. Privacy Shield framework*"; 5. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 16 de julio de 2020, asunto C-311/18) ("Schrems II").

Introducción

En el presente capítulo se propone abordar la concepción jurídica que existe en Estados Unidos sobre el concepto de "*privacy*", así como las eventuales implicaciones que dicha caracterización ha supuesto para los movimientos transfronterizos de datos personales hacia dicho territorio. Máxime si tenemos en cuenta que, en los últimos años, como se tendrá oportunidad de analizar, los cambios que se han producido en los acuerdos adoptados entre el país norteamericano y las autoridades comunitarias se han visto ampliamente afectados por una serie de acontecimientos que han marcado un punto de inflexión en las relaciones comerciales entre ambos territorios.

Antes de proceder a dicha exposición, no es cuestión baladí señalar que cuando abordamos el sistema jurídico de los Estados Unidos no debemos obviar que su construcción parte de la premisa de la consolidación paulatina de un Estado federalizado. Los inicios parten de la consagración gradual a través de las declaraciones de independencia efectuadas por las trece colonias británicas hasta su federalización definitiva en 1789, una vez ratificada la Constitución de los Estados Unidos de América

por los referidos "nuevos Estados", se da por concluido el periodo colonial británico para dar cabida y entrada al sistema federal norteamericano[394].

A este respecto, resulta oportuno tener presente que el proceso de federalización al que hemos hecho alusión no finalizará nunca, pues el mismo ha estado en constante evolución desde entonces como consecuencia de las distintas iniciativas legislativas que se han ido sucediendo. Su efecto ha ido perfilando el contenido de la propia Constitución, así como el propio ordenamiento jurídico —marcado por la tradición jurídica propia del derecho anglosajón— sujeto a las eventuales interpretaciones efectuadas por parte del Tribunal Supremo de los Estados Unidos. En la actualidad, llega a conformarse por un total de 50 Estados y el Distrito Federal de Columbia, que acoge la capital de los EE. UU., esto es, la ciudad de Washington[395].

En este contexto, la regulación del derecho a la privacidad se ha dividido tradicionalmente entre las competencias propias de cada uno de los Estados juntamente con aquellas que resultan aplicables a nivel supranacional fruto de las competencias derivadas del sistema federal[396]. Al encontrarnos delante de un derecho que no dispone de encaje o desarrollo constitucional, esto motiva que su ámbito de aplicación no se encuentre supeditado a delimitaciones, pudiéndose regular desde las perspectivas federales o estatales, aunque siempre diferenciando entre el sector público y el privado, puesto que el primero de los ámbitos de aplicación citados resulta más encorsetado legislativamente que el segundo de ellos[397].

---

394 Para más información sobre la construcción histórica del constitucionalismo de los Estados Unidos de América, *vid*., entre otros: CHEMERINSKY, E., *Constitutional Law: Principles and Policies*, Nueva York: Ed. Wolters Kluwer (Aspen Publishing Co.), 2015; CURTIS, G. T., *History of the Origin, Formation, and Adoption of the Constitution of the United States; with Notices of its Principal Framers*, Nueva York: Ed. Harper and Brothers, 2010; WHITMAN, J. Q., "The Two Western Cultures of Privacy: Dignity versus Liberty", en *Yale Law Journal*, nº 113 (2004), pp. 1151-1221; WOOD, G. S., *The Creation of the American Republic, 1776-1787*, University of North Carolina Press, 1998.

395 *Vid*. U.S. CENSUS BUREAU FOR THE UNITED STATES OF AMERICA. U.S. and World Population Clock. Consultado el 15.08.2020 desde: https://www.census.gov/popclock/.

396 *Vid*. PÉREZ ROYO, J., *Lecciones de Derecho Político I*, Sevilla: Ed. Minerva, 1993, p. 24; ALCARAZ VARÓ, E., *El inglés jurídico norteamericano*, Barcelona: Ariel, 2001, pp. 13-17.

397 Asimismo, resulta oportuno recordar que la concepción del derecho a la privacidad en Estados Unidos nace para garantizar la protección respecto de las injerencias estatales, dejando ciertamente al margen al sector privado, que se regulará a partir de la autorregulación. *Vid*. SOLOVE, D. J. y SCHWARTZ, P. M., *Information Privacy Law*, Nueva York: Ed. Wolters Kluwer, 2018, pp. 35-37; MACDONALD, D. A., "Privacy, Self-Regulation, and the Contractual Model: A Report from Citicorp Credit Services, Inc.", en

1. Estados Unidos de América y su particular concepción de "*privacy*"

Los conceptos de intimidad y protección de datos personales —acuñado bajo el término de privacidad en los EE. UU. por ser una conjunción de ambos[398]— han ido estrechamente ligados durante los últimos dos siglos por lo que a su interpretación y desarrollo jurídico se refiere. Desde sus orígenes, las respectivas implicaciones que han proyectado se encontraban entrelazadas, pese a disponer de significados y ámbitos de aplicación diferenciados —que posteriormente han sido matizados y acotados—[399]. En este sentido, puede reconocerse en el contexto español una cierta confusión respecto de la utilización de los términos que venimos aludiendo, motivada esencialmente por el reconocimiento tardío del derecho a la protección de datos de carácter personal como un derecho autónomo y con contenido jurídico independiente.[400]

El embrión del concepto de protección de datos, pese a que puede resultar sorprendente, no lo encontramos en el ámbito europeo estrictamente, sino que para ello debemos realizar un ejercicio de reminiscencia para remontarnos a los Estados Unidos de América de finales del siglo XIX. En dicho período histórico encontramos los primeros

---

WELLBERY, B. S. (Coord.), *Privacy and Self-Regulation in the Information Age*, U.S. Department of Commerce, 1997; MULLIGAN, D. K. y GOLDMAN, J., "The Limits and the Necessity of Self-Regulation: The Case for Both", en WELLBERY, B. S., (Coord.) *Privacy and Self-Regulation in the Information Age*, U.S. Department of Commerce, 1997.

398 Respecto de la conceptualización del derecho a la privacidad en Estados Unidos, resulta oportuno destacar que han sido múltiples los factores que han intervenido en su caracterización y que, a su vez, han dificultado que en la actualidad exista una posición unánime por lo que a su contenido se refiere. *Vid*., entre otros: SOLOVE, D. J., "Conceptualizing privacy", en *California Law Review*, nº 90 (2002), pp. 1087-1155; POST, R. C., "Three Concepts of Privacy", en *Georgetown Law Journal*, nº 89 (2001), pp. 2087-2098; RUBENFELD, J., "The Right of Privacy", en *Harvard Law Review*, nº 102 (1989), pp. 737-807; GAVISON, R., "Privacy and the Limits of Law", en *The Yale Law Journal*, nº 89 (1980), pp. 421-471.

399 En el contexto español, el Tribunal Constitucional tuvo también ocasión de pronunciarse al respecto, concretamente a través de su Sentencia 290/2000, de 30 de noviembre, estableciendo el siguiente literal, en su Fundamento Jurídico Sexto: "[l]a función del derecho fundamental a la intimidad del art. 18.1 C.E. es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas, STC 144/1999, de 22 de julio, F.J. 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado". Adicionalmente, el referido Tribunal también apuntaba en su Fundamento Jurídico Séptimo que: "El contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso".

400 *Vid*. REMOLINA ANGARITA, N., *Recolección internacional de datos personales: un reto del mundo post-internet*, Madrid: Ed. Agencia Estatal Boletín Oficial del Estado, 2015, pp. 95-97.

resquicios sobre lo apuntando, concretamente de la mano de dos célebres jóvenes abogados de Boston, Samuel D. Warren y Louis D. Brandeis, quienes en el año 1890 publicaron un ensayo titulado *The Right to Privacy*[401], que sentaría las bases de lo que posteriormente sería acogido por el referido país norteamericano, tanto doctrinal[402] como jurisprudencialmente[403], como la protección de la esfera privada frente a intromisiones ilegítimas, cuya deriva finalizaría en la constatación plausible de la existencia de un derecho a la privacidad en Estados Unidos[404].

La doctrina que ha tenido la oportunidad de abordar la cuestión[405] encuentra las motivaciones del ensayo en los avances que se habían producido en el ámbito de la fotografía y su abusiva utilización por parte de los medios de comunicación, creando situaciones desagradables para uno de los autores del artículo, el joven Samuel D. Warren, quien se había visto acosado en distintas ocasiones por la prensa sensacionalista de Boston por cuestiones íntimas de su vida familiar[406]. Problemática que, si la trasladásemos a la actualidad, seguiría resultando de plena aplicabilidad, dado que la pérdida de intimidad y

---

401 *Vid*. WARREN, S. D. y BRANDEIS, L., "The Right to Privacy", en *Harvard Law Review*, Vol. 4, nº 5 (1890), pp. 194-220. Existe traducción al castellano: WARREN, S. D. y BRANDEIS, L., *El derecho a la intimidad*, Madrid: Ed. Thomson-Reuters, Civitas, 1890. Cabe indicar que la traducción al español ha sido criticada por parte de la doctrina, pues no debe confundirse el derecho a la privacidad en su concepción anglosajona con el contenido del derecho a la intimidad que conocemos desde el ordenamiento jurídico español. El primero de ellos aglutina características propias de dos derechos autónomos, uno relativo a la intimidad y otro a la protección de los datos de carácter personal. En España, cierto sector doctrinal ha profundizado sobre la obra en cuestión. *Vid*., entre otros: CARRILLO LÓPEZ, M., *El derecho a no…*, *op. cit.*, pp. 36-39; MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica…*, *op. cit.*, pp. 66-73; GARRIGA DOMÍNGUEZ, A., *Tratamiento de datos personales…*, *op. cit.*, pp. 17-23; PÉREZ LUÑO, A. E., *Derechos Humanos, Estado de…*, *op. cit.*, pp. 327-328; LUCAS MURILLO DE LA CUEVA, P., *El derecho a…*, *op. cit.*, pp. 57-59.

402 *Vid*., entre otros: GLANCY, D. J., "The Invention of the Right to Privacy", en *Arizona Law Review*, Vol. 21, nº 1 (1979), pp. 1-39; KRAMER, I. R., "The Birth of Privacy Law: A Century Since Warren and Brandeis", en *Catholic University Law Review*, nº 39 (1990), pp. 703-724; BRATMAN, B. E., "Brandeis and Warren's «The Right to Privacy» and The Birth of The Right to Privacy", en *Tennessee Law Review*, nº 69 (2002), pp. 623-651.

403 *Vid*., entre otras: *Katz v. United States*, 389 U.S. 347 (1967); *Doe v. Bolton*, 410 U.S. 179, 213 (1973). Más recientemente, *Bartnicki v. Vopper*, 532 U.S. 514, 534 (2001).

404 *Vid*. WARREN, S. D. y BRANDEIS, L., "The Right to…", *op. cit.*, pp. 193-220.

405 *Vid*. MILLER, A. R. y ARBOR, A., *The Assault on Privacy: Computers, Data Banks and Dossiers*, Ed. The University of Michigan Press, 1971, p. 170; MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica…*, *op. cit.*, p. 66-67; NIEVES SALDAÑA, M., "«The right to privacy». La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis", en *Revista de Derecho Político*, Universidad Nacional de Educación a Distancia (UNED), nº 85 (2012), Madrid, pp. 209-210.

406 *Vid*. KONEFSKY, S. J., *The Legacy of Holmes and Brandeis*, Nueva York: Macmillan & Co.,1956.

control sobre la información personal cada vez resulta más frecuente. Este hecho viene producido, en cierta manera, por los avances sucedidos en el campo de la tecnología, que han propiciado la aparición de situaciones de riesgo similares a la expuesta.

En resumen, podríamos identificar que una de las principales consideraciones que se incluyen en el ensayo de Warren y Brandeis radica en la manifestación de una acuciante necesidad de actualizar los instrumentos de protección de la vida privada del individuo frente a intromisiones ilegítimas por parte de terceros. Cabe recordar que los mismos se encontraban basados en una legislación relativa al libelo y la difamación que había quedado obsoleta, pues no ofrecía una respuesta óptima ante los nuevos retos jurídicos que se estaban planteando en ese momento[407].

Al respecto, se produjeron ciertos pronunciamientos doctrinales y jurisprudenciales que reaccionaron ante la publicación, llegando incluso a incentivar que algunos Estados establecieran la posibilidad de articular mecanismos de protección frente a las intromisiones injustificadas que venimos apuntando[408]. Sin embargo, en ningún caso se generalizó una necesidad de reconocer expresamente un derecho a la privacidad en el marco del sistema jurídico norteamericano.

En el mismo sentido se pronuncia Nieves Saldaña, cuando establece que: "Warren y Brandeis abogaron por un sistema legal que reconociera y protegiera el derecho a la privacidad porque consideraron que cuando la información sobre la vida privada de una persona es conocida por terceros se menoscaba el núcleo de la personalidad individual. Por tanto, la concepción original del derecho a la privacidad refleja una dimensión psicológica, para Warren y Brandeis el derecho a la privacidad es el derecho de toda persona a proteger su integridad psicológica ejerciendo control sobre aquella información que afecta a la personalidad individual por reflejar su propia autoestima, de ahí que el derecho a la privacidad forme parte del derecho más general a la inmunidad de la persona, en definitiva «*the right to one's personality*»"[409].

Sin perjuicio de lo anterior, cabe destacar que, aunque Warren y Brandeis se han posicionado históricamente como los precursores de la doctrina sobre privacidad en el

[407] *Vid*. WARREN, S. D. y BRANDEIS, L., "The Right to…", *op. cit.*, pp. 207-212.

[408] *Vid*. SOLOVE, D. J. y SCHWARTZ, P. M., *Information Privacy Law*, *op. cit.*, pp. 25-27.

[409] *Cfr*. NIEVES SALDAÑA, M., "The right to privacy». La génesis…", *op. cit.*, p. 207.

ámbito del derecho estadounidense desde la publicación de su famoso ensayo. Muchas han sido las voces que han aclamado un origen aún más lejano del término "*privacy*", situándolo en el período colonial acaecido como consecuencia de la importación de la tradición jurídica inglesa[410].

Máxime, si tenemos en cuenta que en 1879, once años antes de la publicación de Warren y Brandeis, el juez Thomas Cooley expresaba la aseveración "*the right to be let alone*" —el derecho a no ser molestado— mediante una de sus obras más representativas[411], dirigida especialmente a la prevención de agresiones físicas. Este hecho daría lugar a una doctrina que inicialmente sería acogida por parte de las colonias norteamericanas para dotarla de contenido constitucional, pues se incluyó en la Tercera, Cuarta y Quinta Enmienda, respectivamente —que serán analizadas en los apartados siguientes—, para posteriormente, en el año 1886, ser amparada por parte del Tribunal Supremo en un supuesto de hecho específico relativo a la prevención del fraude[412].

A este respecto, resulta oportuno añadir que el juez Cooley realizó una interpretación conjunta de las enmiendas aludidas bajo la óptica de la aseveración acuñada en 1879, manifestando su contribución a la protección de la privacidad del individuo frente a intromisiones arbitrarias producidas por parte de terceros. Las referenciadas intromisiones podrían provenir tanto de las propias autoridades gubernamentales como de la sociedad en general, en aras de garantizar la protección de la propiedad privada y la inviolabilidad del domicilio particular[413].

En este sentido, tal y como indica Nieves Saldaña: "[p]or todo, a finales del siglo XIX el suelo constitucional norteamericano estaba ya sembrado de principios heredados

---

410 *Vid.*, entre otros: O'CONNOR, T. (1968). "The Right to Privacy in Historical Perspective", *Massachusetts Law Review*, nº 53, pp. 101-110; así como la revisión histórica de los antecedentes apuntados, FLAHERTY, D. H. (1972). *Privacy in Colonial New England*, University Press of Virginia, Charlottesville; GOLDMAN, L. (2006). "The Constitutional Right to Privacy", *Denver University Law Review*, nº 84, pp. 601-644.

411 *Vid*. COOLEY, T. M., *A Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract*, Chicago: Callaghan & Co., 1879; COOLEY, T. M., "Inviolability of Telegraphic Correspondence", en *American Law Register*, nº 27 (1879), pp. 65-78. En el contexto español, acogen esta interpretación: PIÑAR MAÑAS, J. L., "Protección de datos: origen, situación actual…", *op. cit.*, pp. 97-98; LUCAS MURILLO DE LA CUEVA, P., "La construcción del derecho a…", *op. cit.*, pp. 11-80.

412 *Vid. Boyd v. United States*, 116 U.S. 616 (1886).

413 *Vid*. COOLEY, T. M., *A Treatise on the Constitutional Limitations Which Rest upon the Legislative Power of the States of the American Union*, Boston: Ed. Brown & Co., 1879, pp. 299-305.

de la tradición jurídica inglesa, que recepcionados en el sistema jurídico de las colonias habían alcanzado plasmación constitucional en las Enmiendas ratificadas en 1791 y en las aportaciones de conocidos constitucionalistas. Sin embargo, el gran desarrollo de la prensa y la proliferación de mecanismos de reproducción de imágenes, especialmente gracias a los avances en la fotografía, generalizó que en el último tercio del siglo XIX proliferaran las publicaciones por la prensa sensacionalista de aspectos relativos a la vida privada, frente a los que no podía ejercitarse acción legal alguna en defensa de una supuesta violación de la privacidad"[414].

No obstante, las aportaciones de Warren y Brandeis debían entenderse como la consecución de una nueva vertiente interpretativa orientada a resolver las problemáticas acontecidas durante el contexto histórico en el que fueron contraídas. Estas se centran en trasladar la tradición jurídica anclada en los conceptos clásicos vinculados a la protección de la propiedad privada hacía una nueva concepción basada en la prevalencia de la dignidad e inviolabilidad del ser humano[415].

Con posterioridad, numerosos autores han disertado sobre las concepciones incluidas en el famoso ensayo de Warren y Brandeis[416], incluso extendiéndose el debate hasta la actualidad[417]. La llegada de internet y su consiguiente utilización ha comportado la aparición de nuevos riesgos respecto de la protección de la privacidad que requieren ser abordados desde distintas perspectivas y disciplinas, incluso trayendo a colación de nuevo cuestiones de ataño que parecían del todo superadas.

Teniendo en cuenta lo anterior, resulta oportuno señalar que el sistema constitucional de Estados Unidos fue acogiendo gradualmente la noción de la protección

---

[414] *Vid*. NIEVES SALDAÑA, M., "«The right to privacy». La génesis…", *op. cit.*, p. 207.

[415] *Vid*. MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica…*, *op. cit.*, pp. 237-244.

[416] Respecto de esta cuestión, resulta oportuno apuntar que William Prosser fue una de las personas que se interesó por la referida publicación —convirtiéndose en uno de los ensayos más citados de la historia de los Estados Unidos—. Se encargó de analizar la totalidad de trescientos casos que habían planteado Warren y Brandeis, distinguiendo la tipología de ataques en: (i) intrusiones respecto de la intimidad (*intrusion upon seclusion*); (ii) divulgación de cuestiones íntimas (*public disclosure of private facts*); (iii) manifestación de hechos falsos o vejatorios (*false light or publicity*); y (iv) apropiación de la identidad de un tercero en beneficio propio (*appropriation*). *Vid*. PROSSER, W., "Privacy", en *California Law Review*, nº 48 (1960). Y, adicionalmente, *vid*., entre otros: WESTIN, A., *Privacy and Freedom*, New York: Ed. Atheneum, 1970.

[417] *Vid*., entre otros: SCHWARTZ, P. M., "Privacy and Democracy in Cyberspace", en *Vanderbilt Law Review*, nº 52 (1999); SCHWARTZ, P. M., "Internet privacy and the State", en *Connecticut Law Review*, nº 32 (2000); LESSIG, L., *El código y otras leyes del ciberespacio*, Taurus: Ed. Madrid, 2001.

de la vida privada frente a intrusiones arbitrarias e injustificadas como parte integrante de su contenido. A pesar de que no se reconoce expresamente un "*right to privacy*", sí que cabe afirmar que, como consecuencia de la labor realizada por parte del Tribunal Supremo a través de, entre otros, los pronunciamientos realizados por Louis D. Brandeis[418], cuando este formó parte del referido órgano judicial en 1928, se ha ido configurando el derecho a la privacidad como parte integrante del contenido previsto en diversas enmiendas situadas a lo largo del texto que integra la Constitución de los Estados Unidos de América de 1787.

En suma, en primer lugar, la vacilante jurisprudencia[419] lo ha considerado embebido dentro de la Primera Enmienda que se encarga de garantizar la libertad de pensamiento, de asociación y el derecho a mantener el anonimato[420]. Se establece la salvaguarda de los ciudadanos de preservar la confidencialidad sobre la pertenencia a un grupo u organización en la que puedan participar o contribuir[421], teniendo en cuenta, a su vez, que el derecho a la libertad de expresión tiene prevalencia frente a otros derechos como resulta en el supuesto de la privacidad.

En segundo lugar, se ha considerado también amparado en la protección que se confiere en la Tercera Enmienda relativa a la imposibilidad de alojar soldados en las residencias particulares sin el previo consentimiento del propietario. A no ser que una norma así lo establezca en período de guerra[422]. En tercer lugar, en la salvaguarda que introduce la Cuarta Enmienda[423] ante registros arbitrarios (*unreasonable searches and*

---

[418] *Vid. Olmstead v. United States*, 277 U.S. 438 (1928).

[419] *Vid*., entre otras: *NAACP v. Alabama*, 357 U.S. 449 (1958); *Shelton v. Tucker*, 364 U.S. 479 (1960); *Buckley v. Valeo*, 424 U.S. 1 (1976); *Fisher v. United States*, 425 U.S. 391 (1976).

[420] *Vid. McIntyre v. Ohio Election Comm'n*, 514 U. S. 334 (1995).

[421] La Primera Enmienda de la Constitución de los Estados Unidos establece el siguiente tenor literal: "El Congreso no hará ley alguna por la que adopte una religión como oficial del Estado o se prohíba practicarla libremente, o que coarte la libertad de palabra o de imprenta, o el derecho del pueblo para reunirse pacíficamente y para pedir al gobierno la reparación de agravios". Consultado el 24.05.2020 desde: https://www.archives.gov/espanol/constitucion.

[422] *Vid*., entre otros: MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica…*, *op. cit.*, pp. 103-133.

[423] La Cuarta Enmienda de la Constitución de los Estados Unidos establece el siguiente tenor literal: "El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas". Consultado el 24.05.2020 desde: https://www.archives.gov/espanol/constitucion.

seizures)[424] efectuados por las autoridades administrativas sin disponer previamente de la debida autorización judicial, se considera que la garantía no ampara únicamente a los elementos materiales, sino que también, en los últimos tiempos, se han englobado aquellos inmateriales como sucede con las conversaciones telefónicas frente a la posible vigilancia electrónica sistematizada[425]. Así pues, será en 1967 en *Katz v. United States*, cuando el derecho a la privacidad logrará plantearse su alcance constitucional, como consecuencia de la influencia vertida por la opinión de Brandeis en 1928 sobre el mencionado caso de *Olmstead v. United States*[426].

En cuarto lugar, dentro del contenido previsto en la Quinta Enmienda, en lo relativo a la protección frente a la propia incriminación, así como sobre la protección frente a la facultad de las autoridades gubernamentales de forzar a los afectados a divulgar cierta información personal sobre ellos en contra de su propia voluntad[427]. En quinto lugar, se considera previsto en la enumeración de ciertos derechos que se incluye en la Novena Enmienda, cuyo redactado posibilita la realización de una interpretación extensiva en favor de aplicar garantías jurídicas sobre la privacidad en todos aquellos supuestos no regulados específicamente en las ocho primeras enmiendas[428].

---

[424] *Vid*., entre otras: *United States v. Miller*, 425 U.S. 435 (1976).

[425] Las garantías jurídicas efectuadas por parte de la Cuarta Enmienda fueron extendidas inicialmente a las conversaciones telefónicas, *vid*. *Katz v. United States*, 389 U.S. 347 (1967), y posteriormente limitado en aquellos supuestos en que el afectado voluntariamente cedía su información personal a terceros, *vid*. *United States v. Miller,* 425 U.S. 435 (1976). En cualquier caso, en la actualidad, la protección de la Cuarta Enmienda también se ha extendido a las comunicaciones electrónicas, en virtud de la Ley Privacidad de las Comunicaciones Electrónicas de 1986. Consultado el 24.05.2020 desde: https://it.ojp.gov/privacyliberty/authorities/statutes/1285; así como a los registros de los datos de ubicación que se generan mediante el uso de los dispositivos móviles, *vid*. *Carpenter v. United States*, 585 U.S. 84 (2018). Adicionalmente, *vid*., entre otras: *Olmstead v. United States*, 277 U.S. 438 (1928); *Goldman v. United States*, 316 U.S. 129 (1942); *Kyllo v. United States*, 533 U.S. 27 (2001).

[426] En el presente caso, el Tribunal Supremo de los Estados Unidos consideró que la Cuarta Enmienda no resultaba de aplicación sobre las intervenciones telefónicas por no implicar intromisión en la propiedad privada del hogar. Posteriormente, el Congreso daría luz verde la Sección 605 de la *Federal Communications Act* de 1934, que protegía el contenido de dichas comunicaciones mediante previa autorización, así como imponiendo la obligación de no revelar a terceros el contenido de estas.

[427] *Vid*. *Boyd v. United States*, 116 U.S. 616, 630 (1886); *Gouled v. United States*, 255 U.S. 298 (1921).

[428] *Vid*. *Griswold v. Connecticut*, 381 U.S. 479, 484-485 (1965).

En sexto y último lugar, en el concepto de libertad sustantiva previsto en la cláusula del debido proceso legal (*due process of law*)[429] de la Decimocuarta Enmienda, que, a partir del último tercio del siglo XX, la jurisprudencia menor[430] ha tomado como fundamento para considerar que el derecho a la privacidad informativa (*informational privacy*)[431] ostenta rango constitucional. Sin embargo, la totalidad de los Tribunales de Circuito no se han mostrado favorables a acoger el contenido de dicha interpretación[432], así como tampoco el Tribunal Supremo de los Estados Unidos se ha pronunciado sobre

[429] La cláusula de la Decimocuarta Enmienda que garantiza que ningún Estado "privará a ninguna persona de vida, libertad o propiedad, sin el debido proceso legal". El Tribunal Supremo de los Estados Unidos ha interpretado la cláusula del debido proceso para establecer la "incorporación selectiva" de enmiendas en los Estados, lo que significa que ni los Estados ni el propio gobierno federal pueden limitar los derechos individuales previstos por la Constitución mediante la promulgación de leyes estatales o federales. *Vid*., entre otros: *Roe v. Wade*, 410 U.S. 113 (1973); *Whalen v. Roe*, 429 U.S. 589 (1977).

[430] *Vid*., entre otros: *Barry v. City of New York*, 712 F. 2d 1554 (2d Cir. 1983); *Slayton v. Willingham*, 726 F. 2d 631 (10th Cir. 1984).

[431] Podemos referirnos al derecho a la privacidad informativa (*information privacy*) como aquella nueva vertiente del tradicional derecho a la privacidad desarrollado en Estados Unidos, que surge a tenor de un cambio en la jurisprudencia del Tribunal Supremo durante la década de 1960, como consecuencia de los tratamientos masivos que se realizan de información personal mediante el uso de las nuevas tecnologías desarrolladas bajo el acervo de internet. Su principal cometido radica en dotar a los afectados de las herramientas y los mecanismos necesarios que les permita disponer del control efectivo sobre sus datos personales, como parte integrante de una manifestación más del libre desarrollo de la personalidad contenido en el concepto de libertad sustantiva que se propugna en la cláusula del debido proceso establecida en la Decimocuarta Enmienda. *Vid*. WESTIN, A., *Privacy…*, *op. cit*., p. 7; FRIED, C., «Privacy», en *The Yale Law Journal*, nº 77 (1968), pp. 475-493; CATE, F. H., *Privacy in the Information Age*, Washington: Ed. Brookings Institution Press, 1997, p. 22; SCHWARTZ P. M., "Privacy and Democracy…", *op. cit*., pp. 1609-1701; KANG, J., "Information Privacy in Cyberspace Transactions", en *Stanford Law Review*, nº 50 (1998), pp. 1193-1294; SCHWARTZ, P. M., "Internet, Privacy…", *op. cit*., pp. 815-859.

[432] A este respecto, en palabras de Nieves Saldaña: "[t]odos los Tribunales de Circuito sostienen que el derecho a la *informational privacy* no es absoluto, ponderándose el interés individual en la protección de la información personal frente al interés estatal en la adquisición o divulgación de esa información, aunque difieren en cuanto a la relevancia que otorgan al interés estatal. Así, el Cuarto, Sexto y Décimo Circuitos aplican un examen judicial riguroso (*strict scrutiny*) a las invasiones estatales de la *informational privacy*, aunque el Sexto Circuito solo reconoce una violación de la información personal cuando afecta a derechos fundamentales, exigiendo demostrar un interés estatal esencial (*compelling state interest*) para invadir derechos fundamentales a través de la revelación de información personal, mientras que el Cuarto Circuito también aplica un escrutinio riguroso para evaluar la divulgación estatal de la información personal que no afecta a derechos fundamentales". *Cfr*. NIEVES SALDAÑA, M., "El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego", en *Teoría y Realidad Constitucional*, Universidad Nacional de Educación a Distancia (UNED), nº 28 (2011), Madrid, p. 306.

el alcance constitucional de este derecho, a pesar de las numerosas críticas que ha recibido por parte del sector doctrinal[433].

Nos encontramos entonces ante un escenario uniforme respecto de la aplicación del derecho a la privacidad informativa por parte de los diferentes Tribunales, que en la práctica se ha traducido en un escollo para que esta nueva manifestación integrante del derecho a la intimidad pueda ser efectivamente aplicada frente a las intromisiones arbitrarias efectuadas por parte de las autoridades gubernamentales[434]. Asimismo, también resulta evidente la falta de resiliencia del Tribunal Supremo de los Estados Unidos en adaptarse a los nuevos cambios tecnológicos y los riesgos que los mismos llevan aparejados, pues no se muestra proactivo al aprovechar las oportunidades de las que dispone para pronunciarse, como la mencionada en el caso *NASA v. Nelson* en 2011[435].

Una vez visto lo anterior, se puede afirmar que los Estados Unidos de América parten de un sistema que no reconoce la protección de la privacidad mediante una legislación específica, sino que ello se efectúa a través de diversas normativas federales de carácter sectorial que mediante su completitud con las autorregulaciones privadas de determinados sectores[436] propician un marco regulador singular —repleto de excepciones

---

[433] *Vid*., entre otros: FLAHERTY, D. H., "On the Utility of Constitutional Rights to Privacy and Data Protection", en *Case Western Reserve Law Review*, nº 41 (1991), pp. 831-855; CHLAPOWSKI, F. S., "The Constitutional Right to Informational Privacy", en *Boston University Law Review*, nº 71 (1991), pp. 133-136; TURKINGTON, R. C., "Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy", en *Northern Illinois University Law Review*, nº 10 (1990), pp. 496-503.

[434] Así de manifiesta es la preocupación frente a las injerencias de las autoridades gubernamentales que la primera norma aprobada en Estados Unidos a nivel federal que regula el derecho a la privacidad la encontramos en la *Data Privacy Act* de 1974, que regulaba el tratamiento de la información personal que realizaba el gobierno federal. Esta legislación ha sido complementada posteriormente con otras normas también aplicables al ámbito de actuación del sector público, como la *Electronic Communications Privacy Act (ECPA)* de 1986 o la *Driver's Privacy Protection Act (DPPA)* de 1994, que requiere la obtención del consentimiento del propietario del vehículo para comunicar los datos de este a terceras organizaciones.

[435] *Vid*. NIEVES SALDAÑA, M., "El derecho a la privacidad…", *op. cit.*, p. 307.

[436] Podemos citar, entre otras, a título ejemplificativo: la *Right to Financial Privacy Act (RFPA)* de 1978; la *Financial Services Modernization Act* de 1999, habitualmente conocida como la *Gramm-Leach-Bliley Act (GLBA)* de 1999; la *Fair and Accurate Credit Transactions Act (FACTA)* de 2003; por lo que hace referencia a datos médicos, la *Health Insurance Portability and Accountability Act (HIPAA)* de 1996; y con una relativa mayor actualidad, en lo relativo a la privacidad genética, podríamos citar la *Genetic Information Nondiscrimination Act (GINA)* de 2008, así como la *California Consumer Privacy Act (CCPA)* de 2018 relativa a la protección de la información personal de los consumidores residentes en California. Haciendo énfasis igualmente en la protección de la información personal en las comunicaciones electrónicas, cabe

y lagunas que dificultan su interpretación[437]—. Este escenario descrito difiere del preceptuado en el ámbito europeo, tendente a vehicular toda la regulación sobre una materia a través de un mismo cuerpo legal, como hemos tenido la oportunidad de ir advirtiendo, primero con la Directiva 95/46/CE y, más recientemente, con el Reglamento (UE) 2016/679, por citar únicamente algunos ejemplos.

En este contexto, se puede observar la reticencia del sector privado a someterse a las mismas restricciones que las apuntadas para el sector público, motivando los mecanismos de autorregulación como alternativa. Al respecto, Arribas Luque señala que: "La irrupción de las nuevas tecnologías y la escasa protección legislativa de la *privacy* motivó la pérdida de la confianza del consumidor norteamericano y forzó la autoimposición empresarial, voluntaria y como táctica comercial, de normas de conducta limitativas del libre uso de los datos personales, en la creencia de que una política, debidamente difundida, de protección de la privacidad de las personas frente a la intromisión generalizada en aquella que caracterizaba a la competencia redundaría en una mayor captación de clientela y en mayores beneficios"[438].

Pese a ello, podemos destacar, en términos generales, la existencia de ciertos mecanismos de protección frente a las vulneraciones del derecho a la privacidad en el ordenamiento jurídico norteamericano, pero que hasta el momento no se han considerado suficientes. Podemos destacar, en primera instancia, el *Second Restatement of the Law Torts* del *American Law Institute* de 1997, que establece la obligación para aquellas empresas que realicen fraudulentamente declaraciones de hechos, opiniones, intenciones o motivos de abonar aquellas pérdidas económicas que tal perjuicio hubiere causado sobre el afectado o tercero que hubiera confiado en ellas[439].

---

citar, en especial, la *Cable Communication Policy Act* (CCPA) de 1984; la *Electronic Communications Privacy Act* (ECPA) de 1986; la *Telecomunications Act* de 1996; la *Children's On-line Privacy Protection Act* (COPPA) de 1998 y la *E-Government Act* de 2002.

[437] *Vid*, entre otros: SCHWARTZ, P. M. y SOLOVE, D. J., *Information Privacy: Statutes and Regulations 2010-2011*, Ed. Wolters Kluwer (Aspen Publishing Co.), 2009; SOLOVE, D. J. y SCHWARTZ, P. M., *Information Privacy Law*, *op. cit.*

[438] *Cfr*. ARRIBAS LUQUE, J. M., "Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los EE. UU.: El sistema de principios de Puerto Seguro", en *Diario La Ley*, nº 5497 (Sección Doctrina) (2002), p. 3.

[439] *Ibidem*, p. 4.

En segunda instancia, bajo el acervo de la responsabilidad civil extracontractual derivada de la regla del precedente (*rule of precedent*) propia del derecho anglosajón, se prevén las acciones de reclamación por los daños y perjuicios ocasionados por vulneración del derecho a la intimidad. Su valoración, y en su caso, gradación económica se regirá por los supuestos que se hayan enjuiciado con anterioridad sobre situaciones similares por parte de los tribunales jerárquicamente superiores, dado que será entonces cuando se haya sentado precedente[440].

Y, en tercera y última instancia, encontramos aquellos mecanismos de protección previstos en las diferentes legislaciones federales o estatales que, con carácter sectorial, ayudadas de los mecanismos de autorregulación, posibilitan determinadas indemnizaciones de daños y perjuicios, como es el caso de, entre otras, la *Electronic Communications Privacy Act* de 1986, la *Telecommunications Act* de 1996 y la *Consumer Credit Reporting Reform Act* de 1996[441].

A modo de conclusión, resulta oportuno recordar que, por un lado, el desarrollo de esta materia está estrechamente vinculado a los avances tecnológicos que se van produciendo respecto de cada uno de los periodos históricos analizados. Así pues, las implicaciones varían en función de la tecnología utilizada para el tratamiento de los datos personales, siendo diferente el tratamiento de la información que se realizaba a finales del siglo XIX, con el que se realiza actualmente, por ejemplo, mediante las técnicas de análisis sobre cantidades masivas de datos personales provenientes de distintas fuentes de información[442].

Y que, por otro lado, resulta extremadamente dificultoso regular en tiempo real los desarrollos tecnológicos que se van sucediendo por parte de los poderes legislativos estatales. Esta circunstancia desencadena que, por más esfuerzos que se realicen para mitigar el riesgo de descontrol existente en lo relativo a la supervisión en la utilización de los datos e información personal por parte de los afectados[443], siempre exista un amplio

[440] *Ibidem*, pp. 5-6.

[441] *Ibidem.*

[442] *Vid*., entre otros: S. RUBINSTEIN, I., "The End of Privacy or a New Beginning?", en *International Privacy Law*, Vol. 3, nº 2 (2013), pp. 74-87.

[443] Siendo una de las máximas perseguidas por la referida doctrina de la privacidad informativa (*information privacy*), como hemos tenido ocasión de analizar brevemente.

margen de mejora. Incluso, en ocasiones, pese a la complejidad de la situación, nos encontramos adicionalmente con operadores económicos y entes privados que aúnan fuerzas en torpedear aún más esta difícil coyuntura.

2. Evolución de la Decisión de la Comisión, de 26 de julio de 2000, sobre los principios de Puerto Seguro ("*Safe Harbor*")

2.1. Antecedentes

La Unión Europea, desde la adopción del Convenio 108, ha realizado sendos esfuerzos en negociar acuerdos con todos aquellos terceros Estados que no formaban parte de esta. Se trata de territorios que, en la práctica, aglutinan la mayor parte de las transferencias internacionales de datos personales que se realizan fuera del territorio de la Unión Europea. Uno de los ejemplos más notorios de esta circunstancia lo encontramos con Estados Unidos, dado que, desde finales del siglo pasado, las autoridades norteamericanas y las pertenecientes a la Unión han entablado multitud de negociaciones tendentes a afianzar sus estrechos vínculos comerciales. No obstante, en los últimos años, la materia que estamos analizado se ha convertido en un escollo difícil de sortear, pues las distintas concepciones presentes en los respectivos territorios tendentes a garantizar la salvaguarda de este derecho considerado fundamental en el ámbito comunitario parecen resultar irreconciliables[444].

En este sentido, con la entrada en vigor de la Directiva 95/46/CE se planteó un nuevo escenario para el tratamiento de datos personales, dado que, tal y como se ha observado en el anterior Capítulo de la presente obra, entre otras cuestiones, su aplicación efectiva suponía la creación de unas nuevas reglas de juego para poder articular los movimientos de datos de manera transfronteriza. Recordemos que se partía de la premisa basada en que únicamente podían realizarse si existía un nivel de protección adecuado en el país de destino donde los mismos se pretendieran remitir, con la inclusión de un listado de excepciones para ciertos supuestos tasados.

Frente a estas nuevas obligaciones aprobadas, multitud de organizaciones norteamericanas mostraron su preocupación por las limitaciones que ello podía suponer respecto al tratamiento de los datos personales de ciudadanos de la Unión Europea, tanto por la propia prestación del servicio contratada como por el flujo de información personal que en consecuencia se derivaba de la relación comercial mantenida. Esta situación

[444] *Vid*. SUNOSKY, J. T., "Privacy Online: A Primer on the European Union's Directive and United States' Safe Harbor Privacy Principles", en *International Trade Law Journal*, nº 9 (2000), pp. 80-82; SOMA, J. T., RYNERSON, S. D. y BEALL-EDER, B. D., "An analysis of the Use of Bilateral Agreements Between Transnational Trading Groups: The U.S./EU E-Commerce Privacy Safe Harbor", en *Texas International Law Journal*, nº 39 (2004), pp. 194-207.

motivó que, a finales de 1998, el Departamento de Comercio de los Estados Unidos iniciara toda una serie de negociaciones con la Comisión Europea en aras de intentar llegar a un punto de consenso para permitir que los intercambios de datos personales no se vieran limitados o, en el peor de los casos —sobre todo para la economía norteamericana[445]—, paralizados.

Ambas partes partían de planteamientos diferentes dado que, por un lado, el Departamento de Comercio, representado a través de la *Federal Trade Commission* (FTC, por sus siglas en inglés)[446], de conformidad con las estipulaciones establecidas en el ordenamiento jurídico norteamericano, partía de una concepción ampliamente favorable de limitar el mecanismo a que ostentara carácter autorregulatorio, con la intención de que ello tuviera el menor impacto posible en la esfera económica[447]. Y, por otro lado, la Comisión defendía una posición más orientada al respeto de la protección de los datos personales, optando por legislaciones homogeneizadas, sin inclusión de aspectos que favorecieran a la dispersión normativa y, en consecuencia, a la correspondiente inseguridad jurídica.

Asimismo, y con el objetivo de articular un marco legislativo que hiciera efectivo el cumplimiento de los requisitos normativos que establecía la Directiva por parte de las organizaciones estadounidenses, el Departamento de Comercio de los Estados Unidos de América y la Comisión Europea destinaron casi dos años —aproximadamente desde junio

---

[445] Según palabras de la propia Comisión Europea, emitidas en 2014, se preveía que: "La tecnología y los servicios de los macrodatos representen un valor mundial de 16.900 millones de USD en 2015, con una tasa de crecimiento anual compuesta del 40 %, aproximadamente siete veces superior a la del mercado de tecnologías de información y comunicaciones (TIC) en general. Un estudio reciente predice que, solo en el Reino Unido, el número de personas especializadas en macrodatos que trabajará en las empresas de gran tamaño aumentará en más de un 240 % en los próximos cinco años". *Cfr*. COMISIÓN EUROPEA, "Hacia una economía de los datos próspera", Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones (COM/2014/0442 final), de fecha 2 de julio de 2014. Consultado el 20.08.2017 desde: https://ec.europa.eu/digital-single-market/en/news/communication-data-driven-economy.

[446] La Comisión Federal de Comercio de los Estados Unidos (FTC, por sus siglas en inglés), cuyas habilitaciones proceden de la Sección 5 de la *Federal Trade Commission Act*, puede definirse, tal y como se efectúa a través de su propio sitio web oficial, como una agencia independiente del gobierno estadounidense, centrada en la prevención de las prácticas comerciales anticompetitivas, engañosas o desleales hacia los consumidores; mejorar el nivel de información de las opciones disponibles para los consumidores y aumentar el grado de comprensión del proceso competitivo por parte del público; y cumplir con estos objetivos sin imponer una carga indebida sobre la actividad comercial legítima. Consultado el 24.08.2017 desde: https://www.ftc.gov/about-ftc.

[447] *Vid*. FEDERAL TRADE COMMISSION, *Self-Regulation and Privacy online: A report to Congress*, Estados Unidos, 1999.

de 1997 hasta julio de 2000[448]—, a mantener amplias negociaciones para desarrollar el contenido de la Decisión, lo cual posibilitó que finalmente el 26 de julio de 2000, se adoptara el texto[449]. A partir de entonces, se articulaba un mecanismo habilitante de las transferencias de datos personales de ciudadanos europeos a empresas que tenían su sede en Estados Unidos, siempre que las mismas, con carácter previo, hubieran aceptado respetar los principios de salvaguarda y protección a la privacidad contenidos en el Acuerdo de Puerto Seguro (en adelante, Acuerdo, o Decisión, respectivamente)[450].

En consecuencia, la Decisión de la Comisión, de 26 de julio de 2000, ya en sus iniciales considerandos, establecía ya ciertas reservas, propugnando que, aunque existiera un común acuerdo de voluntades para intentar articular mecanismos de cooperación y transparencia que permitieran una mejora de las relaciones comerciales y transaccionales entre los Estados Unidos de América y la Unión Europea, resultaba preciso manifestar que se partía de sistemas regulatorios antagónicamente diferentes. A pesar de intentar tutelar la protección del mismo bien jurídico, esto es, la privacidad —en el ámbito comunitario, acuñado bajo la denominación de protección de datos personales—, lo realizaban desde perspectivas y mecanismos diametralmente opuestos[451].

---

[448] Entre el lapso temporal que duraron las negociaciones —más de dos años—, el Departamento de Comercio de los Estados Unidos remitió numerosas propuestas de regulación a la Comisión Europea que, en su mayor parte, fueron rechazadas por parte de esta después de ser analizadas por parte del GT29. Este último organismo emitió varios pronunciamientos al respecto abordando el nivel de adecuación de los Estados Unidos de América respecto de las transferencias internacionales de datos con destino al referido territorio.

[449] *Vid*. Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (notificada con el número C [2000] 2441). Consultado el 20.08.2017 desde: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32000D0520.

[450] *Vid*. CHARLESWORTH, A., "Data Privacy in Cyberspace: Not National vs. International but Commercial vs. Individual", en EDWARDS, L. y C. WAELDE, C. (Coord.), *Law and the Internet*, Oxford: Ed. Hart, 2000, pp. 79-122; VACCA, J. R., "The European Data Protection Directive: A Roadblock to International Trade", en R. HEROLD, R. (Coord.), en *The Privacy Papers. Managing Technology, Consumer, Employee, and Legislative Actions*, Nueva York: Ed. Auerbach publications, 2000, pp. 569-581; RUBIN, P. H. y LENARD, T. M., *Privacy and the commercial use of personal information*, Boston: Ed. Wolters Kluwer, 2002, p. 100.

[451] *Vid*. N. LUGARESI, N., *Internet, Privacy e Pubblici Poteri negli Stati Uniti*, Milán: Ed. Giufrè, 2000, pp. 107-128; CAMP, L. J., *Trust and Risk in Internet Commerce*, Cambridge: Ed. Massachusetts Institute of Technology Press, 2000, pp. 99-114.

Como paso previo a entrar a examinar el contenido y estructura de la Decisión de la Comisión, de 26 de julio de 2000, que se ha apuntado. Conviene manifestar que nos encontramos ante un mecanismo de adhesión voluntaria para las organizaciones estadounidenses, que les permitía acogerse al cumplimiento de los principios consagrados en la Decisión mediante un mecanismo basado en la autocertificación y la autoevaluación[452]. Una vez superado este escollo, ello les posibilitaría valorar individualmente si cumplían con los referidos principios y obligaciones que les resultaban de aplicación, para que, posteriormente, pudieran comunicarlo al Departamento de Comercio de los Estados Unidos, dado que era el organismo regulador al que se le habían atribuido tales competencias[453].

En este sentido, cabe subrayar que la Decisión se componía de once considerandos iniciales, seis artículos que intentaban transmitir el contenido esencial del Acuerdo y una serie de Anexos, que pueden diferenciarse esencialmente en que el primero de ellos incluye los "Principios de Puerto Seguro (Protección de la vida privada)", y el segundo se refiere a las "Preguntas Frecuentes" (FAQ, por sus siglas en inglés). El resto de contenido que conforman los restantes Anexos, que avanzan hasta el número sexto, se orientan a intentar arrojar luz y facilitar la aplicabilidad práctica del texto de la Decisión y los correspondientes Principios y FAQ[454].

2.2. Contenido

2.2.1. Ámbito de aplicación e "irrealidad" sobre su viabilidad

En aras de realizar una evaluación crítica sobre las cuestiones sustantivas que integran el contenido del Acuerdo de Puerto Seguro, se formulará una enumeración

[452] Se trataba de un procedimiento que gozaba de un amplio margen de discrecionalidad y que no aportaba la suficiente seguridad jurídica en referencia a la protección de los datos de carácter personal. Ello fue puesto de manifiesto también por el GT29. *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 27): Dictamen 7/99, relativo al nivel de protección de datos previsto por los principios de «puerto seguro» hechos públicos, junto con las preguntas más frecuentes y otros documentos relacionados, el 15 y 16 de noviembre de 1999 por el Departamento de Comercio de los EE. UU.", aprobado por el Grupo de Trabajo, el 3 de diciembre de 1999, pp. 7-8

[453] Desde el año 2000, hasta su posterior invalidación, fueron alrededor de 3.000 organizaciones estadounidenses las que se adhirieron al acuerdo de forma voluntaria.

[454] Tal y como ha establecido al respecto el GT29, las Preguntas Frecuentes y el propio texto de la Decisión deberán entenderse como formantes de un mismo cuerpo jurídico unitario y con carácter vinculante. Consultado el 20.08.2017 desde: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp23_en.pdf.

sistemática de las mismas para facilitar su entendimiento. En primer lugar, respecto su *a priori* buen funcionamiento. Según lo preceptuado en su artículo 1.2, para que se pudieran efectuar los movimientos transfronterizos de los datos personales de ciudadanos comunitarios a los Estados Unidos, se tenían que cumplir dos condicionantes por parte de la entidad receptora de los datos. Uno basado en su compromiso de dar cumplimiento a los principios y FAQ consagradas en la Decisión. Y otro fundamentado en que la misma estuviera bajo la jurisdicción de alguno de los organismos que se relacionan en el Anexo VII del Acuerdo, esto es, el Departamento de Transporte o el Departamento de Comercio (a través de la FTC).

Para entender el contenido y alcance de este primer condicionante, cabe examinar los principios que se encontraban recogidos en el Acuerdo de Puerto Seguro —configurándose estos como una opción de mínimos para la garantía de los derechos y libertades de los afectados—. En primera instancia, encontrábamos el principio de notificación (*notification*), que establecía la obligación de informar a los afectados sobre las finalidades para las que se utilizaban sus datos personales, las posibles comunicaciones a terceros que se podían suceder, así como si les surgía cualquier duda o aclaración, a quién podían dirigirla. Todo ello debía de formularse a través de un lenguaje sencillo y transparente que no dificultase la comprensión por parte del interesado[455].

En segunda instancia, se posicionaba el principio de opción (*option*). Por un lado, incluía la posibilidad de solicitar a los afectados su consentimiento implícito (*opt-out*) para realizar comunicaciones de datos a terceros, así como para utilizar sus respectivos datos personales para finalidades distintas para las que inicialmente fueron recabados. Ello suponía una manifiesta contradicción de las consideraciones que el GT29 establecería unos años más tarde al respecto, en ocasión de analizar las comunicaciones con fines de venta directa[456]. Por otro lado, en aquellos supuestos en que la información

[455] *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 19): Dictamen 2/99, relativo a la idoneidad de los «Principios internacionales de puerto de seguro» que hizo públicos el Departamento estadounidense de Comercio el 19 de abril de 1999", aprobado por el Grupo de Trabajo, el 3 de mayo de 1999, p. 5.

[456] En relación con la utilización del consentimiento implícito, el GT29 ha manifestado su negativa en la utilización, estableciendo que: "[…] El consentimiento concedido con ocasión de la aceptación general de los términos y condiciones que regulan un contrato principal (p. ej. un contrato de suscripción en el que se solicita también el consentimiento para enviar comunicaciones con fines de venta directa) debe cumplir los requisitos, establecidos en la Directiva 95/46/CE, de ser libre, específico e informado. A condición de que se cumplan estas últimas condiciones, el interesado puede dar su consentimiento, por ejemplo, mediante la

facilitada tuviera la consideración de datos especialmente protegidos —como aquellos relativos al estado de salud, origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, vida sexual de la persona—, se debía prestar especial cautela, pues el consentimiento que debía solicitarse debía ser afirmativo y explícito (*opt-in*).

Las consideraciones reflejadas en este principio resultaron de vital importancia, pues en las mismas se fundamentaba la legitimación de las eventuales transferencias internacionales de datos que se pudieran suceder. Por lo que, a este respecto, el GT29 manifestó que el contenido de este principio adolecía de ciertas carencias, señalando que: "Los principios no regulan la legitimidad de los criterios de tratamiento, es necesario reforzar el principio de Opción. En su versión actual, la combinación de los principios de Notificación y Opción permite utilizar los datos para fines distintos de los notificados sin necesidad de ofrecer la posibilidad de opción (a menos que dichos fines sean incompatibles o que los datos sean delicados), lo que incumple las Directrices de la OCDE («Principio de limitación del uso»)"[457].

En tercera instancia, se establecía el principio de ulterior transferencia (*onward transfer*), cuyo contenido determinaba la necesidad de que, para que se pudiera articular una comunicación de datos personales a terceros —esto es, a otros responsables del tratamiento sitos en EE. UU.—, la empresa en cuestión destinataria debía de estar adherida a los principios de Puerto Seguro, en aras de respetar las vicisitudes establecidas en la Directiva 95/46/CE. Además, debía formalizar un contrato que le obligase a la adopción de las distintas medidas de seguridad y protección que resultasen aplicables en función de la tipología de datos personales objeto de tratamiento[458].

---

selección de una casilla. El consentimiento implícito para recibir tales mensajes no es compatible con la definición de consentimiento establecida en la Directiva 95/46/CE y, en particular, con el requisito de que el consentimiento sea manifestación de la voluntad de alguien, incluso en el caso en que se hiciera «salvo oposición» (listas de exclusión). De forma similar, las casillas preseleccionadas, p. ej. en sitios web, tampoco son compatibles con la definición de la Directiva". *Cfr*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 90): Dictamen 5/2004 sobre comunicaciones no solicitadas con fines de venta directa con arreglo al artículo 13 de la Directiva 2002/58/CE", aprobado por el Grupo de Trabajo, el 27 de febrero de 2004, p. 5.

[457] *Cfr*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 27): Dictamen 7/99 relativo…", cit., cit., pp. 4-5.

[458] Ante la ausencia de mecanismos de supervisión para garantizar la trazabilidad de los datos personales de los afectados en el marco de la realización de estas transferencias ulteriores, cabe remarcar las palabras

En cuarta y quinta instancia, se podían observar los principios de seguridad (*security*) e integridad de los datos (*data integrity*), respectivamente. El primero de ellos preceptuaba que las organizaciones que se encargasen de recabar datos de carácter personal debían aplicar todas las precauciones necesarias que permitiesen evitar su pérdida, uso indebido, acceso no autorizado, divulgación, alteración o destrucción. En consonancia, el segundo de los principios aludidos determinaba que las organizaciones únicamente podían utilizar los datos personales de acuerdo con las finalidades para las que fueron recabados, siendo pertinentes únicamente para el uso inicialmente previsto.

Por último, en sexta y séptima instancia, se recogían los principios de acceso (*access*) y cumplimiento (*enforcement*), respectivamente. El inicial reconocía el derecho de los interesados a obtener acceso a los datos personales de los que dispusieran las organizaciones sobre ellos mismos, así como a poder modificarlos, corregirlos o suprimirlos en caso de inexactitud. Y el posterior manifestaba la necesidad de que las organizaciones articulasen mecanismos para que los interesados, en el supuesto de que no se respetasen las vicisitudes contenidas en el Acuerdo de Puerto Seguro, pudieran disponer de vías de recurso que les ofrecieran y facilitaran una vía de tutela sobre sus derechos. Además de que, si resultaba procedente, se derivasen consecuencias en el supuesto de incumplimiento, como, por ejemplo, la imposición de indemnizaciones[459].

A este respecto, resulta oportuno reproducir a modo de sumario las palabras de Recio Gayo y Álvarez Caro cuando consideran que: "[l]os principios básicamente reconocen los derechos de los titulares de los datos personales, imponen obligaciones a los responsables del tratamiento, establecen principios aplicables al procesamiento de la información y responsabilidad para el caso de infracción. Asimismo, las entidades deben adoptar mecanismos para garantizar la efectiva aplicación de los citados principios, tales

---

que el GT29 había emitido al respecto, exponiendo que: "[p]ese a que este principio no se recoge en las directrices de la OCDE, es necesario para garantizar que las empresas estadounidenses que acatan los principios de puerto seguro no transfieran datos a otro responsable del tratamiento de datos en Estados Unidos o en otro lugar que no ofrezca la protección adecuada. Pero, tal como está formulado actualmente el principio, no está claro cuál es la norma aplicable. Consideramos que la persona debería tener la posibilidad de negarse a una transferencia de sus datos a un tercero. Para ello, como mínimo deberá estar informado de tal transferencia y de si dicho tercero se adhiere a los principios de puerto seguro, así como, si no es así, del grado de adecuación de la protección que se le ofrece. *Cfr*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 19): Dictamen 2/99…", cit., p. 6.

[459] Sin embargo, cabe advertir que, en la práctica, el régimen sancionador previsto ha adolecido de una ausencia de efectividad, dado que su formulación era tan generalista y poco concreta que ha evocado como resultado en su no aplicación de manera extensiva.

como recursos independientes, procedimientos de monitoreo, medidas de reparación o sanciones"[460].

Adicionalmente a lo anterior, se reconocían también una serie de FAQ —en total, quince— con la intención de que sirvieran de guía para aclarar o, en su caso, ayudar a aplicar algunos de los Principios que se han identificado. Ello resultaba necesario por ser su redacción algo confusa, dado que se efectuó de manera conjunta entre la industria y los representantes de la opinión pública en aras de facilitar y agilizar la consecución del libre intercambio de datos entre EE. UU. y la Unión Europea[461].

En relación con el segundo de los condicionantes que expresábamos al inicio del presente apartado, cabe entender que el ámbito de aplicación de la Decisión se encontraba limitado desde un inicio[462]. El texto adolecía de una exclusión expresa sobre aquellos tratamientos de datos personales que se produjesen por parte de organizaciones que no se encontrasen bajo el acervo competencial de las autoridades administrativas que se relacionaban en el Anexo VII del Acuerdo[463], esto es, el Departamento de Transporte y el Departamento de Comercio (a través de la FTC), siendo sobre esta última entidad a la que se refiere el documento de forma expresa.

A esta tesitura, hay que añadir que la Decisión partía de una perspectiva de futuro nada prometedora desde sus propios inicios. Si se recopilan las distintas observaciones que se han ido abordando, se recordará que el artículo 25.6 de la Directiva 95/46/CE abogaba por la consideración del "nivel de protección adecuado" que garantizase el país de destino de los datos personales, de acuerdo, conjuntamente con otros aspectos, a "su legislación interna […] a efectos de la protección de la vida privada o de las libertades o

---

[460] *Cfr*. RECIO GAYO, M. y ÁLVAREZ CARO, M., "Hacia un acuerdo Safe Harbor renovado para la transferencia internacional de datos entre EE. UU. y la UE", nº 25 (2015), en *Instituto de Derecho Europeo e Integración Regional (IDEIR)*, Madrid: Ed. Universidad Complutense, 2015, p. 7.

[461] *Vid*. RECIO GAYO, M. y ÁLVAREZ CARO, M., "Hacia un acuerdo…", *op. cit.*, p. 6.

[462] Sobre esta cuestión, el GT29 también manifestaba sus preocupaciones, señalando que: "[e]n lo que respecta al «puerto seguro», el Grupo de trabajo recomienda definir de manera clara y sin ambigüedad su alcance tanto para los beneficiarios como para las categorías de transferencias de datos". *Cfr*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 27): Dictamen 7/99, relativo…", cit., p. 4.

[463] Se reproduce, a continuación, el tenor literal del párrafo tercero del Anexo I de la Decisión de la Comisión de 26 de julio de 2000 en cuestión: "[l]as entidades sujetas a disposiciones de naturaleza legal, reglamentaria, administrativa u otra (o a reglamentaciones) que protejan con eficacia el secreto de los datos personales, podrán acogerse también a los beneficios del puerto seguro". Con lo que puede inferirse, como también ha puesto de relieve el GT29, que las autoridades públicas quedan exceptuadas del cumplimiento de la Decisión de la Comisión.

de los derechos fundamentales de las personas", como requisitos para poder articular una transferencia de datos personales con las suficientes garantías.

Ningún aspecto de los enumerados se ha tenido en cuenta en la redacción del Acuerdo, a pesar del claro mandato que efectuaba la Directiva. Si nos guiamos por la literalidad del contenido de la Decisión, en todo momento está haciendo alusión expresa al cumplimiento de lo que en la misma se contempla —principalmente, los Principios y las Preguntas Frecuentes—. No se presta atención alguna al mandato efectuado por el artículo 25.6 referido, así como tampoco se propone una solución ante las preocupaciones manifestadas por el GT29 sobre la situación de la legislación interna de los Estados Unidos en lo relativo a la protección de los datos de carácter personal[464].

En base a lo expuesto, se crea un contexto en el que fácilmente puede concluirse que la viabilidad de la Decisión era totalmente inexistente, así como también lo seria para la norma que vendrá a sustituirla, que correrá su misma suerte. Se puede apreciar entonces la elusión de distintas disposiciones normativas previstas en el ordenamiento comunitario —esto es, la Directiva 95/46/CE—, así como las propias advertencias dictaminadas por distintos operadores jurídicos de la Unión con competencias sobre la materia —como el GT29—. Esta circunstancia será puesta de relieve posteriormente por parte del Tribunal de Justicia de la Unión Europea[465].

2.2.2. Inaplicación

En segundo lugar, siguiendo con el análisis de las cuestiones sustantivas, conviene analizar la eficacia práctica del sistema de adhesión que preceptuaba el Acuerdo de Puerto Seguro. Se trataba de un sistema de carácter voluntario y autocertificable, en el que la propia entidad interesada valoraba a su íntegra discreción si daba cumplimiento a los

[464] Resulta oportuno traer a colación las palabras del GT29 pronunciadas al respecto: "[l]a protección de la intimidad y de los datos en Estados Unidos se enmarca en un complejo entramado de regulación sectorial, tanto a nivel federal como estatal, que se combina con la autorregulación industrial. Se han hecho considerables esfuerzos durante los últimos meses para mejorar la credibilidad y aplicabilidad de la autorregulación industrial, particularmente en el contexto de Internet y del comercio electrónico. Sin embargo, el Grupo de trabajo considera que actualmente no se puede confiar en el popurrí existente de leyes sectoriales muy segmentadas y en la autorregulación voluntaria para proporcionar protección adecuada en todos los casos a los datos personales transferidos desde la Unión Europea". *Cfr*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 15): Dictamen 1/99, relativo al nivel de protección de datos en Estados Unidos y a los debates en curso entre la Comisión Europea y el Gobierno de Estados Unidos", aprobado por el Grupo de Trabajo, el 26 de enero de 1999, p. 2.

[465] *Vid*. STJUE. Asunto C-362/14 (Schrems I), cit.

distintos condicionantes que se requerían por los Principios y las FAQ contenidos en la Decisión. Si el resultado era favorable, debía dar traslado de su idoneidad al Departamento de Comercio tanto de la propia adhesión como de la sujeción a su cumplimiento[466].

A este respecto, el GT29 ya manifestaba serias dudas respecto de la eficacia del mecanismo expuesto, pues indicaba que: "[e]l Departamento de Comercio no efectúa verificaciones previas para determinar si una entidad concreta cumple los criterios de adecuación (adhesión de su política de protección de la vida privada a los principios, jurisdicción de un órgano similar a la FTC para prácticas fraudulentas)". Por lo que, ante esta falta de control y supervisión advertida, añadía: "Dado que la renovación de dicha autocertificación no es obligatoria, una entidad podría adherirse a los principios durante un año y, a continuación, retirarse del «puerto seguro». Además, existe la posibilidad de que haya impostores no detectados que tarden un periodo significativo en desaparecer de la lista, periodo durante el cual los datos personales continuarían transfiriéndose con normalidad"[467].

Las advertencias reproducidas por el GT29 serían respaldadas posteriormente por parte de la Comisión Europea, en el informe que tuvo ocasión de emitir en fecha, 20 de octubre de 2004[468], donde alertaba sobre la constatación de que gran multitud de organizaciones norteamericanas no se sujetaban al cumplimiento de lo establecido en los

---

[466] Se reproduce, a continuación, el tenor literal de los párrafos segundo y tercero de la FAQ nº 6 incluida en la Decisión de la Comisión, de 26 de julio de 2000, en cuestión: "[l]os beneficios del puerto seguro se garantizan desde la fecha en que una entidad se autocertifica ante el Departamento de Comercio, o su representante, su adhesión a los principios de conformidad con las directrices que se indican a continuación. Para proceder a la autocertificación, las entidades pueden proporcionar al Departamento de Comercio (o a su representante) una carta firmada por uno de los responsables de la empresa en nombre de la entidad que se adhiere al puerto seguro […]".

[467] *Cfr*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 27): Dictamen 7/99, relativo…", cit., p. 9.

[468] La Comisión Europea, en su informe emitido en fecha 20 de octubre de 2004 (SEC [2004] 1323), se basa en el emitido con anterioridad, en la primera evaluación que se realizó sobre el Acuerdo de Puerto Seguro, reproducido en el Documento de Trabajo SEC (2002) 196, de fecha 13 de febrero de 2002, cuyo contenido fue respaldado posteriormente por sendos documentos de trabajo emitidos por parte del GT29. Consultado el 20.08.2017 desde: http://ec.europa.eu/transparency/regdoc/rep/2/2002/ES/2-2002-196-ES-1-1.Pdf. El informe emitido por parte de la Comisión, en fecha 20 de octubre de 2004, pone de relieve la falta de transparencia de las organizaciones estadounidenses que se adhieren al marco de cumplimiento, por lo que se refiere, en particular, al cumplimiento de los estándares fijados para las políticas de privacidad, que dificultan, a su vez, la tarea de supervisión de estas por parte de las autoridades de control de Estados Unidos que tienen competencias sobre este asunto. Consultado el 20.08.2017 desde: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf.

principios de Puerto Seguro para la protección de la privacidad. Dicho aspecto volvió a ponerse de manifiesto por el mismo órgano comunitario en fecha, 27 de noviembre de 2013[469], cuando volvió a manifestar: "[l]os progresos a este respecto han sido limitados. Desde el 1 de enero de 2009, el Departamento de Comercio evalúa la política de protección de la vida privada antes de renovar la certificación de puerto seguro de las entidades que deseen hacerlo —lo que debe hacerse anualmente—. Sin embargo, es una evaluación limitada, ya que no se evalúan plenamente las prácticas reales de las entidades autocertificadas, lo que haría mucho más fiable el procedimiento de autocertificación"[470].

De lo anterior, se desprende que los esfuerzos de supervisión llevados a término por parte de la FTC para revisar el cumplimiento de los Principios y FAQ contenidos en el Acuerdo de Puerto Seguro habían sido ínfimos, limitándose únicamente a revisiones de trámite, sin entrar a analizar el fondo de la cuestión. Una buena muestra de ello la encontramos en la referida comunicación emitida por parte de la Comisión, en que se manifiesta que tras solicitar al Departamento de Comercio que revisase todas las solicitudes con mayor detenimiento y rigurosidad, las solicitudes rechazadas habían incrementado el doble para las entidades que pretendían renovar el acuerdo y el triple para aquellas que pretendían adherirse por primera vez[471].

Asimismo, si a la ausencia de una supervisión efectiva que velase por la aplicación del contenido previsto en la propia Decisión, le añadimos la inclusión de una serie de excepciones contempladas en la misma que aún dificultan más su cumplimiento[472], se

---

469 *Vid*. COMISIÓN EUROPEA, "Comunicación al Parlamento Europeo y al Consejo, sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la Unión Europea y las empresas establecidas en la misma", de fecha 27 de noviembre de 2013 (COM [2013] 847 final). Consultado el 20.08.2017 desde: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com (2013)0847_es.pdf.

470 *Cfr*. COMISIÓN EUROPEA, "Comunicación al Parlamento… (COM [2013] 847 final)", cit., p. 9.

471 Según las estadísticas presentadas en septiembre de 2013 por el Departamento de Comercio, en 2010 el Departamento notificó a un 18 % (93) de las 512 entidades que pedían la certificación por primera vez y a un 16 % (231) de las 1.417 que deseaban renovarla que debían mejorar sus políticas de protección de la vida privada o sus solicitudes de adhesión al Acuerdo de Puerto Seguro. En cambio, tras la petición de la Comisión de una vigilancia más estricta, diligente y sistemática de todas las solicitudes, a mediados de septiembre de 2013 el Departamento había notificado a un 56 % (340) de las 602 entidades que pedían la certificación por primera vez y a un 27 % (493) de las 1.809 que deseaban renovarla que debían mejorar sus políticas de protección de la vida privada. *Ibidem*.

472 Las excepciones referenciadas eran añadidas a discreción por parte de las autoridades públicas norteamericanas. Se reproduce al respecto el tenor literal del párrafo cuarto del Anexo I de la Decisión de la Comisión de 26 de julio de 2000: "[l]a adhesión a estos principios puede limitarse: a) cuanto sea necesario

plantea un escenario de incertidumbre que dificulta su viabilidad. Estas mismas impresiones fueron recogidas por parte del GT29, considerando que el mecanismo proyectado no aportaba seguridad jurídica suficiente, pues consideraba preciso: "[e]liminar las generalizaciones y ambigüedades de las excepciones y exenciones permitidas, de manera que las excepciones sean precisamente eso, es decir, que se apliquen solamente cuando sea necesario y en la medida requerida, y que no sean invitaciones generales para hacer caso omiso de los principios"[473].

2.2.3. FAQ 7

En tercer lugar, los requisitos de verificación incluidos en el principio de aplicación previsto en la FAQ nº 7 permitían que aquellas organizaciones que se hubieran adherido al Acuerdo de Puerto Seguro pudieran demostrar el cumplimiento de su contenido a través de alguno de los distintos mecanismos que se articulaban para tal fin. Por un lado, encontrábamos el método de autoevaluación, en que un directivo u otro representante autorizado por parte de la empresa obligada debía firmar un informe de verificación de la autoevaluación como mínimo una vez al año. Dicho documento debía difundirse a petición de los consumidores o en el contexto de posibles investigaciones o quejas por incumplimiento[474].

Y, por otro lado, se recogía el método basado en la verificación por terceros que, a título meramente enunciativo, podía incluir auditorías, comprobaciones imprevistas, el uso de "señuelos" o de herramientas tecnológicas, según se considerase apropiado. Su utilización se contemplaba como una mera alternativa por la que podían optar las entidades. Como sucedía con el anterior mecanismo, también debía incluir la firma del revisor, del directivo u otro representante autorizado de la entidad obligada, elaborándose como mínimo una vez al año —para su entrega a la FTC—. De la misma manera,

---

para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley; b) por disposición legal o reglamentaria, o jurisprudencia que originen conflictos de obligaciones o autorizaciones explícitas, siempre que las entidades que recurran a tales autorizaciones puedan demostrar que el incumplimiento de los principios se limita a las medidas necesarias para garantizar los intereses legítimos esenciales contemplados por las mencionadas autorizaciones; c) por excepción o dispensa prevista en la Directiva o las normas de Derecho interno de los Estados miembros siempre que tal excepción o dispensa se aplique en contextos comparables".

[473] *Cfr.* COMISIÓN EUROPEA, "Comunicación al Parlamento… (COM [2013] 847 final)", cit., p. 15.

[474] *Cfr.* Párrafo tercero de la FAQ nº 7 incluida en el Anexo II de la Decisión de la Comisión de 26 de julio de 2000.

resultaba preciso garantizar su difusión bajo demanda de los consumidores o en el contexto de posibles investigaciones o quejas por incumplimiento[475].

En este sentido, una de los principales escollos que encontraba el sistema de autocertificación voluntaria propugnado por la Decisión radicaba en que las entidades norteamericanas incluidas bajo su acervo de protección podían seguir tratando datos personales de ciudadanos de la Unión Europea hasta que no se presentará una queja o se abriera una investigación por parte de las autoridades incluidas en el Anexo VII del Acuerdo —aunque las mismas no estuvieran dando cumplimiento a las garantías adecuadas—[476]. En consecuencia, nuevamente el GT29 alentó a la Comisión para buscar soluciones al respecto, por lo que recomendaba "considerar la eliminación o supresión de los datos transmitidos" a las entidades que previamente había identificado[477].

De entre las escasas opciones de recurso que se planteaban en el Anexo II del Acuerdo de Puerto Seguro, resulta especialmente curioso destacar lo dispuesto en la FAQ nº 11. En dicho punto, la FTC se comprometía a dar trámite sumario sobre aquellos recursos planteados directamente por ciertos organismos de autorregulación, así como por los propios Estados miembros de la Unión Europea que alegasen el incumplimiento de lo previsto en el artículo 5 de la *Federal Trade Commission Act*[478]. Ante estas situaciones, si el referido organismo competente norteamericano apreciaba indicios suficientes, podía optar por solucionar el asunto solicitando una decisión administrativa de cese de las prácticas denunciadas o presentando una denuncia ante un tribunal federal

---

[475] *Cfr*. Párrafo quinto de la FAQ nº 7 incluida en el Anexo II de la Decisión de la Comisión de 26 de julio de 2000.

[476] *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 27): Dictamen 7/99, relativo…", cit., p. 4.

[477] El GT29 introduce una clasificación de entidades de riesgo a las que aplicar la solución propuesta. A este respecto, reza el literal siguiente: "[t]eniendo en cuenta los ejemplos anteriores, el Grupo de trabajo insta a la Comisión a analizar métodos para garantizar la protección continua de los datos personales que puedan transmitirse a los siguientes tipos de entidades: 1. Entidades que nunca tendrían que haber aparecido en la lista porque no cumplen los criterios de aceptabilidad; 2. Entidades que, aunque aparecen en la lista, no cumplen los principios; 3. Entidades que, después de estar en la lista durante un año, dejan de estarlo el siguiente, porque no renuevan su autocertificación o porque dejan de ser aceptables en el «puerto seguro»; y 4. Entidades que, después de aparecer en la lista, son absorbidas por una empresa que no cumple los requisitos de «puerto seguro» (porque no puede o porque no desea adherirse a los principios)". *Cfr*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 27): Dictamen 7/99, relativo…", cit., pp. 4-5.

[478] El artículo 5 de la *Federal Trade Commission Act* establece la prohibición de llevar a cabo actos o prácticas desleales o fraudulentos en el comercio que, entre otros derechos, puedan afectar al relativo a la privacidad.

de primera instancia (*Federal District Court*). Si esta prosperaba, podía desencadenar una resolución al efecto de un tribunal federal[479].

Una vez citadas en grandes términos las escasas vías de resolución que planteaba la FAQ nº 11, resulta oportuno contrastar la efectividad práctica de estas, de la misma manera que también lo hemos observado con anterioridad respecto de la idoneidad de los esfuerzos de supervisión llevados a término por parte de la FTC para revisar el cumplimiento de los Principios y FAQ contenidas en el Acuerdo de Puerto Seguro. Nuevamente, no resulta nada sorprendente constatar que las vías de resolución de controversias propuestas no presentan apenas implementación práctica, así como que tampoco se daba curso a las peticiones cursadas por parte de los interesados.

Una prueba irrefutable de ello se encuentra en las consideraciones manifestadas por parte de la Comisión, cuando expresa que: "[l]a mayoría de las entidades retiradas de la lista de puerto seguro por el Departamento de Comercio lo fueron por petición propia (por ejemplo, entidades fusionadas o adquiridas por otras, que han cambiado su línea de negocio o que han cesado sus actividades). Asimismo, se ha eliminado un número más reducido de entidades extinguidas, cuando sus sitios web incluidos en los registros ya no estaban operativos y su certificación llevaba varios años sin renovarse. Es importante señalar que no parece haberse retirado de la lista ninguna entidad debido a problemas de cumplimiento detectados en la verificación del Departamento de Comercio"[480].

2.2.4. Limitaciones impuestas sobre los derechos de los afectados

En cuarto lugar, resulta oportuno recordar lo observado con anterioridad en relación con los principios de opción y acceso, respectivamente. Inicialmente se abordará el primero de ellos, cuyo contenido resulta complementado a su vez por lo dispuesto en la FAQ nº 1, que se encarga de introducir una serie de excepciones relacionadas con su cumplimiento, el cual quedaría exceptuado cuando "el tratamiento: 1) se realiza en función de intereses vitales de la persona afectada o de otra persona; 2) es necesario para

[479] Se reproduce, a continuación, el tenor literal del último párrafo incluido en la FAQ nº 11 del Anexo I de la Decisión de la Comisión de 26 de julio de 2000 en cuestión: "[l]a FTC puede tanto conseguir una sanción civil si se quebrantan las decisiones administrativas de cese como ejercer acciones civiles o penales en los casos de incumplimiento de las resoluciones de los tribunales federales de primera instancia. La FTC pondrá en conocimiento del Departamento de Comercio todas las acciones de este tipo que emprenda. El Departamento de Comercio alienta a otros organismos públicos a notificarle el resultado final de estos asuntos o cualquier otra resolución sobre la adhesión a los principios de puerto seguro".

[480] *Cfr.* COMISIÓN EUROPEA, "Comunicación al Parlamento… (COM [2013] 847 final)", cit., pp. 9-10.

preparar un recurso o acción en justicia; 3) se requiere para hacer un diagnóstico médico; 4) se lleva a cabo en el marco de las legítimas actividades de una fundación, asociación o cualquier otro organismo sin fines lucrativos que persiga un objetivo político, filosófico, religioso o sindical, a condición de que el tratamiento se refiera exclusivamente a los miembros del organismo o a las personas que tienen contactos habituales con él relacionados con sus fines, y a condición de que los datos no se revelen a terceros sin el consentimiento de los interesados; 5) es necesario para que la entidad cumpla sus obligaciones en materia de Derecho laboral; o 6) se refiere a información hecha pública de modo manifiesto por el particular"[481].

De entre todas las excepciones que se han apuntado, cabe hacer hincapié en la última de ellas, pues si la misma concurriese —así como de alguna de las restantes—, el afectado se vería privado de ejercer el derecho de opción previsto en el Acuerdo de Puerto Seguro[482]. Curiosamente, unos años más tarde, dicha excepción también tendrá encaje como una de las previstas en el artículo 9.2 del RGPD, respecto de la prohibición general de tratar categorías especiales de datos. En suma, se trata de un concepto homologable al previsto en la Directiva 95/46/CE. Concretamente en su letra e) se halla el siguiente literal: "El tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos".

Dicho concepto ha sido analizado activamente por parte del anterior Grupo de Trabajo del Artículo 29, estableciendo que: "[e]l GT29 quisiera hacer hincapié en que esta disposición debe entenderse en el sentido de que el interesado era consciente de que los datos iban a ponerse a disposición del público, es decir, de todas las personas e incluidas las autoridades. En caso de duda debe aplicarse una interpretación estricta, puesto que se supone que el interesado ha renunciado voluntariamente a la protección especial de datos sensibles al ponerlos a disposición del público, incluidas las autoridades"[483].

---

[481] *Cfr*. Párrafo segundo de la FAQ nº 1 incluida en el Anexo II de la Decisión de la Comisión de 26 de julio de 2000.

[482] A este respecto, el GT29 reitera que: "El hecho de que la información sea de dominio público no priva al sujeto de los datos de su derecho de acceso". *Cfr*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 27): Dictamen 7/99, relativo…", cit., p. 9.

[483] *Cfr*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 258): Dictamen sobre algunas cuestiones fundamentales de la Directiva sobre protección de datos en el ámbito penal (UE 2016/680)", aprobado por el Grupo de Trabajo, el 29 de noviembre de 2017, p. 10.

Sigue apuntado el referido GT29 que: "[e]n casos como la publicación de datos personales en una biografía, en la prensa o en un sitio web público, la intención está clara. En otros casos, resulta más difícil tomar una decisión. Por ejemplo, registrarse en una red social podría conllevar la aceptación de determinadas normas de protección de datos en las que se estipule que todos los asociados del proveedor (incluidas las autoridades policiales nacionales) tienen acceso a los datos personales. En estos casos, la mayoría de los usuarios probablemente no asimilan activamente esta información y realmente no son conscientes de que las autoridades policiales tienen acceso a sus datos"[484].

En relación con este concepto, en España fue inicialmente recogido en el Anteproyecto de la Ley Orgánica de Protección de Datos (artículo 13), siendo duramente criticado por parte del Consejo de Estado debido a la incertidumbre que el mismo generaba. Posteriormente, la AEPD tuvo ocasión de pronunciarse al respecto estableciendo el siguiente tenor literal: "[d]e este modo, se establece un principio general según el cual puede considerarse mínima la intromisión en la esfera privada de un interesado cuando el responsable procede al tratamiento de aquellos datos que él mismo ha hecho manifiestamente públicos, como podrían ser los que incorporase a perfiles abiertos de redes sociales, a los que se refiere la consultante"[485].

Sigue apuntado la referida autoridad de control: "[e]n este supuesto, el citado precepto del Anteproyecto establece una regla que consideraría amparado el tratamiento en el artículo 6.1 f) del Reglamento general de protección de datos, siempre que la divulgación se haya llevado a cabo directamente por el interesado y esa divulgación sea tan amplia que los datos puedan considerarse hechos "manifiestamente públicos". Entre los dos ejemplos mencionados podrán existir otros en que habrá de estarse a las circunstancias de cada supuesto. Así, por ejemplo, podría ser de aplicación el artículo 6.1 f) si el acceso a la fuente se encuentra amparado en una habilitación legal, como sucedería en los supuestos de sistemas de información crediticia o el acceso a determinados registros públicos, mientras que en otros supuestos, como por ejemplo los referentes a información divulgada por terceros distintos del afectado en fuentes de acceso más

[484] *Ibidem.*

[485] *Vid*. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Informe jurídico, con nº de referencia: 195/2017", pp. 19-20. Consultado el 20.08.2020 desde: https://www.aepd.es/es/documento/2017-0195.pdf.

restringido, la afectación al derecho fundamental sería mayor, no pudiéndose sin más amparar la recogida en el artículo 6.1 f) del reglamento general de protección de datos"[486].

Una vez expuesta la coyuntura descrita, con carácter posterior a analizar el principio de opción, debe reflexionarse en lo relativo al principio de acceso[487], que excluía el cumplimiento de la obligación de atender las peticiones de ejercicio de derechos de los afectados en dos supuestos tasados. Esto es, cuando ello suponía una carga o dispendio desproporcionado en relación con los riesgos que el asunto en cuestión conllevase para la vida privada de la persona, o bien cuando podían vulnerarse los derechos de otras personas[488].

De la misma forma que sucedía con el supuesto anterior, el principio de acceso se veía complementado con las disposiciones previstas en la FAQ nº 8, que además de establecer alguna aclaración sobre lo contenido en el Anexo I[489], se encargaba de estipular determinadas limitaciones que dificultaban aún más el ejercicio de este derecho por parte de los interesados. A este respecto, pueden enunciarse varios ejemplos. En un primer inciso, puede destacarse la propia contradicción manifiesta a la que llega el texto, en que, tras detallar una serie de directrices sobre la metodología a utilizar para atender correctamente las peticiones efectuadas por los afectados, se indica que "al responder a las peticiones de acceso de los afectados, las entidades deben guiarse por los motivos de

[486] *Ibidem.*

[487] Sobre el principio de acceso, que conlleva el reconocimiento de un derecho a favor del afectado, el GT29 considera que: "Es un principio fundamental para todo régimen de protección de datos que se precie, puesto que el Acceso es la raíz de la que se derivan todos los derechos del sujeto de los datos, y hace énfasis en que las excepciones a este principio fundamental solamente se permitan en circunstancias excepcionales, al tiempo que reitera la preocupación expresada en todos sus documentos anteriores sobre la amplitud y la ambigüedad de las excepciones y condiciones expresadas por los EE. UU. para el ejercicio de este derecho fundamental". *Cfr.* COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 27): Dictamen 7/99, relativo…", cit., p. 9.

[488] *Cfr.* Principio de acceso incluido en el Anexo I de la Decisión de la Comisión de 26 de julio de 2000.

[489] Una de las excepciones que establece el principio de acceso radica en considerar la petición como una "carga o dispendio desproporcionado", como hemos visto, pues haciendo gala nuevamente de la utilización de conceptos jurídicos indeterminados —sobre los que el GT29 ya había advertido sobre su peligrosidad—, la FAQ nº 8 pretendió, sin demasiado éxito, realizar alguna aclaración al respecto, manifestando en su segundo párrafo el siguiente tenor literal: "La obligación que tiene una entidad de proporcionar acceso a la información personal que posee sobre una persona está sujeta al principio de proporcionalidad o razonabilidad y debe suavizarse en determinados casos". *Cfr.* Principio de acceso incluido en el Anexo I de la Decisión de la Comisión de 26 de julio de 2000.

preocupación que provocaron inicialmente la petición"[490]. Posteriormente, se añade: "Los afectados no tienen que justificar las peticiones de acceso a sus propios datos"[491]. Difícilmente pueda guiarse una entidad en el momento de examinar una solicitud a través del contenido vertido en la misma, si esta no precisaba de la inclusión de justificación alguna.

En un segundo inciso, cabe citar los numerosos motivos que se habían previsto en el contenido de la FAQ nº 8 como posibles alternativas para limitar o no dar cumplimiento a las peticiones de acceso efectuadas por parte de los interesados[492]. Después de su análisis, difícilmente las autoridades administrativas de Estados Unidos encontrarían alguna de ellas como válida para poder acogerse, dado que la estructura de su construcción obedecía a un *numerus apertus*. Máxime, si consideramos la cláusula residual que se introducía a modo de "cajón de sastre", cuyo literal rezaba como sigue: "Otras circunstancias en que la carga o dispendio necesarios para facilitar el acceso sean desproporcionados o se vulneren los derechos o intereses legítimos de otras personas"[493].

Y en tercer y último inciso, pero no menos importante, resulta conveniente señalar, por un lado, la ausencia de inclusión de garantías en relación con el plazo de respuesta de las peticiones de ejercicio del derecho de acceso por parte de los interesados, no concretándose nada al respecto. Haciendo gala nuevamente de conceptos jurídicos indeterminados[494], pues únicamente se mencionaba que debían de atenderse "sin demoras

---

[490] *Cfr*. Párrafo tercero de la FAQ nº 8 incluida en el Anexo II de la Decisión de la Comisión de 26 de julio de 2000.

[491] *Ibidem*.

[492] Pese a enunciarse todo lo contrario al inicio de la quinta respuesta de la FAQ nº 8, pues manifiesta al respecto que: "[e]stas circunstancias son limitadas y las razones para denegar el acceso deben ser específicas". *Cfr*. Quinta respuesta de la FAQ nº 8 incluida en el Anexo II de la Decisión de la Comisión de 26 de julio de 2000.

[493] *Cfr*. Quinta respuesta de la FAQ nº 8 incluida en el Anexo II de la Decisión de la Comisión de 26 de julio de 2000.

[494] Resulta contradictorio que se incluyan expresiones imprecisas para referirse a los plazos de respuesta ante las peticiones de ejercicio de derechos por parte de los afectados. Máxime si tenemos en cuenta que también el GT29 ya había mostrado su rechazo ante este tipo de fórmulas, pues estableció respecto del principio de notificación que: "[e]l Grupo de trabajo también pide que se aclare el significado exacto de la expresión "o posteriormente lo antes posible", ya que considera que debería informarse a las personas en el momento de la recogida, y no cuando lo desee cada responsable del tratamiento". *Cfr*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 19): Dictamen 2/99…", cit., p. 5.

excesivas y en un plazo de tiempo razonable"[495]. Y, por otro lado, las previsiones injustificadas que se reproducían en relación con la imposición del cobro de cuotas a los afectados para atender las eventuales peticiones de ejercicio del derecho de acceso que realizaran, cuando las mismas fueran consideradas como excesivas, a sabiendas de que ello podía desencadenar en una vulneración de la tutela judicial efectiva sobre los interesados[496].

2.2.5. Papel de las autoridades de control

Por último, en quinto lugar, resulta oportuno examinar el papel que ostentaron las distintas autoridades de control en materia de protección de datos, tanto desde la perspectiva europea como norteamericana en lo relativo a las garantías y facultades que se reconocían en el Acuerdo de Puerto Seguro. Siguiendo el hilo de lo que se venía comentando, cabe dirigirnos a la FAQ nº 5 para encontrar las funciones que la Decisión reconocía a las referidas autoridades. Se centraban esencialmente en facultades de información y asesoramiento a entidades norteamericanas —a través de un panel informal de autoridades de protección de datos formado en el ámbito europeo—, en relación con quejas no resueltas de particulares relacionadas con el tratamiento de su respectiva información personal transferida desde la Unión Europea bajo el acervo del Acuerdo[497].

Para hacer más evidente la ausencia de garantías, a lo expuesto con anterioridad, se adiciona, por una parte, que el compromiso de colaboración con las autoridades competentes de los Estados miembros en materia de protección ostentaba carácter voluntario. Eran las propias entidades adheridas al Acuerdo las que decidían optar por

[495] *Cfr*. Decimoprimera respuesta de la FAQ nº 8 incluida en el Anexo II de la Decisión de la Comisión, de 26 de julio de 2000.

[496] Esta concepción ha sido nuevamente introducida en el RGPD, concretamente en su artículo 14, así como también se recoge en el artículo 13 de la LOPDGDD. Cabe reconocer qué perspectiva viene a contravenir el modelo tradicional de protección que se había seguido en la LOPD, pues a través de su artículo 15.1 se establecía que: "El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos".

[497] *Vid*. Primera respuesta de la FAQ nº 5 incluida en el Anexo II de la Decisión de la Comisión, de 26 de julio de 2000.

esta alternativa en el momento de su inscripción y notificación de adhesión ante el Departamento de Comercio[498].

Y por otra parte, de conformidad con lo que había advertido previamente el GT29, resultaba imposible proponer como alternativa que las organizaciones adheridas al Acuerdo de Puerto Seguro confiaran la supervisión del cumplimiento del mismo a las autoridades de los Estados miembros, pues estas carecían de competencias en terceros países y, por consiguiente, de toda capacidad de ejecución que les permitiera controlar eficazmente la aplicación de los principios por parte de las organizaciones estadounidenses[499]. Por ende, cabe considerar que las garantías de validez y solidez de la Decisión quedaron bastante diluidas por su ausencia de eficacia y aplicabilidad práctica.

En cualquier caso, debía de ser la Comisión el organismo comunitario encargado de decidir sobre la viabilidad de la Decisión, suspendiendo o limitando su ámbito de aplicación[500], teniendo en cuenta las cuestiones suscitadas durante su vigencia[501]. Como el propio ente reconocía: "[a]sí está previsto especialmente si se da un incumplimiento sistemático por parte estadounidense, por ejemplo, si un órgano responsable de velar por el cumplimiento de los principios de puerto seguro en Estados Unidos no está cumpliendo su función de manera efectiva, o si el nivel de protección que ofrecen los principios de puerto seguro es superado por los requisitos de la legislación estadounidense. Al igual

[498] Ello les comportaba principalmente un compromiso de colaboración centrado en colaborar con las autoridades comunitarias en materia de protección de datos en la investigación y resolución de las quejas que se formulasen, así como acatar las decisiones que estas pronunciaran, cuando se determinaba que la entidad debía tomar decisiones concretas para cumplir los principios de puerto seguro, y en particular el pago de indemnizaciones o compensaciones en beneficio de los afectados por el incumplimiento de los principios, para posteriormente notificar por escrito a las autoridades comunitarias sobre la adopción de dichas medidas. *Vid*. Primera respuesta de la FAQ nº 5 incluida en el Anexo II de la Decisión de la Comisión de 26 de julio de 2000.

[499] *Cfr*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 19): Dictamen 2/99…", cit., pp. 3-4.

[500] De conformidad con el procedimiento de examen expuesto en el Reglamento nº 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión.

[501] En cualquier caso, cabe apuntar que también se preveía en el artículo 3, apartado primero, de la propia Decisión de la Comisión de 26 de julio de 2000, de acuerdo con lo dispuesto en el artículo 25 de la Directiva 95/46/CE, que las autoridades de control de los Estados miembros en materia de protección de datos también pudieran ejercer la facultad de suspender los flujos de datos hacia una entidad que se hubiera adherido al Acuerdo de Puerto Seguro, a fin de proteger a los particulares contra el tratamiento de sus datos personales.

que todas las decisiones de la Comisión, la Decisión de puerto seguro también puede ser modificada, o incluso derogada, por otros motivos"[502].

Respecto del papel de las autoridades norteamericanas, cabe manifestar que, durante los aproximadamente diez primeros años de vigencia de la Decisión, no se produjeron quejas en relación con el cumplimiento del Acuerdo de Puerto Seguro, no siendo hasta el año 2009 cuando se iniciaron las primeras actuaciones por infracción de las obligaciones previstas en el mismo. Concretamente, se trató de diez actuaciones sucedidas entre 2009 y 2012[503], que se vieron complementadas a su vez por una serie de medidas de carácter administrativo contra entidades que, de manera fraudulenta, habían manifestado estar adheridas a la Decisión y cumplir con los respectivos principios que en la misma se preceptuaban.

Todo ello fue como consecuencia de las reiteradas peticiones efectuadas al respecto por parte de la Comisión Europea sobre la necesidad de reforzar los mecanismos de supervisión y control que incluía el Acuerdo de Puerto Seguro, así como, entre otros, la importancia de que se intensificaran los controles periódicos realizados sobre sitios web y se revisaran las nuevas solicitudes con mayor atención y detenimiento[504]. Asimismo, la Comisión manifestó la necesidad de articular un mayor número de investigaciones y comprobaciones de oficio sobre el cumplimiento de las obligaciones

[502] *Cfr.* COMISIÓN EUROPEA, "Comunicación al Parlamento… (COM [2013] 847 final)", cit., p. 5.

[503] Se siguen a continuación: *Javian Karnani, and Balls of Kryptonite, LLC.* (Consultado el 20.08.2020 desde: https://www.ftc.gov/enforce-ment/cases-proceedings/092-3081/best-priced-brands-llc-et-al); *World Innovators, Inc.* (Consultado el 20.08.2020 desde: https://www.ftc.gov/enforcement/cases-proceedings/0923137/world-innovators-inc-matter); *ExpatEdge Partners, LLC.* (Consultado el 20.08.2020 desde: https://www.ftc.gov/enforcement/cases-proceedings/0923138/expatedge-partners-ll); *Onyx Graphics, Inc.* (Consultado el 20.08.2020 desde: https://www.ftc.gov/enforcement/cases-proceedings/0923139/onyx-graphics-inc); *Directors Desk, LLC* (Consultado el 20.08.2020 desde: https://www.ftc.gov/enforcement/cases-proceedings/0923140/directors-desk-ll); Progressive Gaitways, LLC. (Consultado el 20.08.2020 desde: https://www.ftc.gov/enforcement/cases-proceedings/0923141/progressive-gaitways-ll); *Collectify, LLC.* (Consultado el 20.08.2020 desde: https://www.ftc.gov/enforcement/cases-proceedings/092-3142/collectify-ll); Google, Inc. (Consultado el 20.08.2020 desde: https://www.ftc.gov/enforcement/cases-proceed- ings/102-3136/google-inc-matter); Facebook, Inc. (Consultado el 20.08.2020 desde: https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc); y, Myspace, LLC. (Consultado el 20.08.2020 desde: https://www.ftc.gov/enforcement/cases-proceedi-ngs/102-3058/myspace-llc-matter). *Cfr.* RECIO GAYO, M. y ÁLVAREZ CARO, M., "Hacia un acuerdo…", *op. cit.*, pp. 11-12.

[504] *Vid.* COMISIÓN EUROPEA, "Comunicación al Parlamento… (COM [2013] 847 final)", cit., pp. 9-10.

establecidas en la Decisión respecto de aquellas entidades norteamericanas que estuvieran adheridas a la misma[505].

Ante esta tesitura, se considera oportuno traer a colación las palabras de Recio Gayo y Álvarez Caro como respuesta a la actividad de la FTC, cuando afirman que: "[r]esulta claro que, a pesar de que durante los primeros años no hubo acción alguna, lo importante ahora no es plantear excusas si hubo incumplimientos y a quién le correspondía identificarlos o conocer de los mismos, en su caso. Todos los esfuerzos se deben poner en pensar qué medidas concretas son necesarias para buscar y conseguir la protección efectiva de la persona cuyos datos personales son objeto de tratamiento. Al mismo tiempo, la posibilidad de recurrir a mecanismos de resolución extrajudicial de litigios es una oportunidad que debe considerarse en términos que permita generar confianza para todas las partes implicadas, debiendo ser razonablemente accesible y, en cualquier caso, efectiva para los titulares de los datos personales"[506].

2.3. Consideraciones

2.3.1. Imposibilidad de supervivencia. Cuestiones que imposibilitaron su vigencia

Ahora que se ha podido analizar el contenido de la Decisión de la Comisión de 26 de julio de 2000, cabe reseñar las principales implicaciones que se sucedieron desde su aplicación práctica. En suma, la primera y más notoria recae en el incremento del flujo de movimientos de datos personales desde la Unión Europea hacia los Estados Unidos, cuya sucesión repercutió en un notable incremento de los beneficios económicos para ambos territorios citados, dado que desde 2003 a 2017 se calcula que el comercio total entre ambos socios comerciales aumentó de 594.000 millones a 1.2 billones de dólares[507].

Del mismo modo, podemos constatar que las transferencias internacionales de datos que se producen como consecuencia de esta alianza transatlántica se posicionan como las más elevadas en el mundo. Una estimación estableció que Estados Unidos exportó ciento cuarenta mil millones de dólares en servicios a la Unión Europea en 2012,

---

[505] *Ibidem*, p. 13.

[506] *Cfr*. RECIO GAYO, M. y ÁLVAREZ CARO, M., "Hacia un acuerdo…", *op. cit.*, pp. 13-14.

[507] *Vid*. PATEL, O. y LEA, N., *EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows*, Londres: Ed. UCL European Institute, 2020, p. 11.

representando el 72 % del total de las exportaciones estadounidenses al citado territorio, sirviendo muchas de estas exportaciones como base para articular las cadenas de valor mundiales[508]. *A sensu contrario*, Estados Unidos únicamente importó ochenta y seis mil millones de dólares en servicios de la Unión Europea, el 62 % de los cuales fue integrado únicamente en las cadenas de valor norteamericanas[509].

Por lo tanto, estas cifras constatan la evidencia de la importancia económica que tiene para ambos territorios el mantenimiento de un canal fluido de intercambio de datos, así como que el mismo no se vea interrumpido o suspendido por cuestiones como las que en las siguientes líneas se tendrá ocasión de examinar. Adicionalmente, si traemos a colación datos facilitados por la propia Comisión Europea[510], no hacemos más que seguir ratificando la importancia de la Decisión mediante el incremento exponencial de la cantidad de organizaciones estadounidenses que decidieron adherirse al Acuerdo de Puerto Seguro durante el período que concierne de 2004 a 2013, pasando de 400 en ese primer año a 3.246 en la última de las anualidades indicadas.

Así pues, la Comisión también recalca el valor del dato, concretamente, el relativo a los ciudadanos sitos en la UE, que pasó de trecientos quince millones de euros en 2011 a una previsión de un billón de euros en 2020[511], constatándose un repunte de la importancia de ciertos sectores de actividad como el tecnológico, sobre todo a través del mercado relativo al análisis de grandes cantidades de datos. Este sector, en fecha de 2013, estaba incrementándose en un 40 % anual a nivel mundial[512], cuando los intercambios de

---

[508] *Vid*. GRIMM, A. N., "Trends in U.S. Trade in Information and Communications Technology (ICT) Services and in ICT-Enabled Services", Ed. Bureau of Economic Analysis, U.S. Department of Commerce, 2015; MANYIKA, J. y LUND, S., "How Digital Trade is Transforming Globalisation", California: Ed. McKinsey & Company, 2016. Consultado el 20.08.2020 desde: http://e15initiative.org/publications/how-digital-trade-is-transforming-globalisation.

[509] *Vid*. MELTZER, J. P., "The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment", Ed. Brookings, 2014, pp. 12-17. Consultado el 20.08.2020 desde: https://www.brookings.edu/research/the-importance-of-the-internet-and-transatlantic-data-flows-for-u-s-and-eu-trade-and-investment/.

[510] *Vid*. COMISIÓN EUROPEA, "Comunicación al Parlamento… (COM [2013] 847 final)", cit., p. 3.

[511] *Vid*. COMISIÓN EUROPEA, "Comunicación al Parlamento Europeo y al Consejo, Restablecer la confianza en los flujos de datos entre la UE y EE. UU.", de fecha 27 de noviembre de 2013 (COM [2013] 846 final), p. 3. Consultado el 20.08.2017 desde: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2013%3A0846%3AFIN.

[512] *Vid*. MANYIKA, J., CHUI, M. y VV. AA., "Big data: The next frontier for innovation, competition, and productivity", California: Ed. McKinsey & Company, 2011. Consultado el 20.08.2020 desde:

datos transfronterizos se estaban convirtiendo en una cotidianeidad, como en el caso de los servicios de computación en la nube[513]. Por lo que se requería de nuevas soluciones adaptadas a las necesidades tecnológicas del momento, a las que —como se verá— el Acuerdo de Puerto Seguro no daba cobertura suficiente.

2.3.2. Inefectividad manifiesta

En segundo lugar, conviene destacar las manifiestas carencias de efectividad y omisiones de control a las que el Acuerdo de Puerto Seguro se había visto abocado por la falta de diligencia de las autoridades de control encargadas de su supervisión en el ámbito norteamericano, evidenciadas esencialmente por parte del Departamento de Comercio de los Estados Unidos a través de la FTC. Lo anterior puede sustentarse adecuadamente a través de dos documentos emitidos por parte de la Comisión Europea en los que se analizan las repercusiones de la Decisión en dos momentos cronológicos diferenciados.

Por un lado, se puede citar el documento de trabajo elaborado en 2004 sobre la aplicación de la Decisión[514], en el que se ponían de relieve ciertas deficiencias que no se solventarían incluso hasta años más tarde en la segunda revisión de 2013. De entre las mismas, puede citarse la ausencia de transparencia o claridad en las políticas de privacidad de las entidades adheridas, la elevada utilización de conceptos jurídicos indeterminados como el de "tercero", la inclusión de advertencias sobre la peligrosidad del mecanismo de "ulterior transferencia" que hemos analizado, así como una vaga e imprecisa explicación sobre los distintos derechos de los que disponían los afectados para hacer valer sus pretensiones.

Y, por otro lado, en 2013, la Comisión publicó la comunicación sobre la que hemos venido trabajando, en la que advirtió nuevamente serias dudas sobre la idoneidad

---

https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation.

[513] A este respecto, conviene recordar las palabras manifestadas por el GT29 respecto a la utilización de la tecnología basada en la computación en la nube, cuando señala que: "La autocertificación con puerto seguro por sí sola no puede considerarse suficiente en ausencia de una sólida aplicación de los principios de protección de datos en la computación en nube. Asimismo, el artículo 17 de la Directiva de la UE requiere la firma de un contrato entre el responsable y el encargado del tratamiento a efectos del tratamiento de datos, lo que se confirma en la FAQ 10 de la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000". *Cfr*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 195): Dictamen 05/2012 sobre la computación en nube", aprobado por el Grupo de Trabajo el 1 de julio de 2012, p. 20.

[514] *Cfr*. COMISIÓN EUROPEA, "Documento de trabajo del personal de la Comisión sobre la aplicación de la Decisión 520/2000/CE de la Comisión… (SEC [2004] 1323)", cit., p. 3.

del Acuerdo, que iban en el mismo sentido de lo ya había advertido en 2004. Pero esta vez se introducían una serie de datos actualizados, tales como que un elevado número de empresas autocertificadas no había hecho pública su política de protección de datos o no habían publicado su adhesión a la Decisión[515], así como que aquellas que sí lo habían hecho introducían un redactado demasiado complejo que no favorecía la lectura y comprensibilidad por parte del afectado, pues incluso los hipervínculos que en las mismas se contenían no funcionaban correctamente[516].

Las recomendaciones se centraron principalmente en cuatro grandes líneas de trabajo. La primera de ellas se centraba en la transparencia, estableciendo que las políticas de privacidad de las organizaciones norteamericanas adheridas al marco de cumplimiento deberían de ser públicas en sus correspondientes sitios web, redactadas con un lenguaje claro y sencillo. Además, debían incluirse hipervínculos al sitio web del Departamento de Comercio para poder constatar que la entidad en cuestión se encontraba incluida en el listado de todas las organizaciones adheridas y, al mismo tiempo, era preciso establecer las condiciones en las cuales se efectuaban las subcontrataciones para la prestación de determinados servicios que involucrasen el tratamiento de datos personales.

La segunda de las líneas de trabajo contenida en las recomendaciones estaba orientada a los recursos, pues las políticas de privacidad debían incluir enlaces a cualesquiera terceros que se encargasen de la solución extrajudicial de litigios, los cuales, deberían ser asequibles y fácilmente disponibles, dado que el Departamento de Comercio velaría por su cumplimiento. Paralelamente a esta línea de trabajo, en tercer lugar se encontraba aquella vinculada con su efectiva aplicación, pues para poder proceder a su constatación se proponía articular inspecciones de oficio orientadas a verificar el nivel de cumplimiento de las entidades adheridas al Acuerdo sobre Puerto Seguro, así como realizar investigaciones cuando se hubieran manifestado indicios de incumplimientos o se hubieran recibido denuncias al respecto, debiendo informar a las autoridades comunitarias siempre que resultase oportuno.

En cuarto lugar, siguiendo el orden de las líneas de trabajo expuestas en las recomendaciones, encontramos la cuestión relativa al acceso por parte de las autoridades estadounidenses a los datos de carácter personal. En este punto, se establecía la obligación

[515] *Vid.* COMISIÓN EUROPEA, "Comunicación al Parlamento… (COM [2013] 847 final)", cit., p. 7.

[516] *Ibidem.*

de que las políticas de privacidad incluyeran de manera detallada, el marco jurídico norteamericano que permitía el acceso a los datos personales transferidos en el marco del Acuerdo de Puerto Seguro. Teniendo en cuenta que, en todo caso, se trataría de una actividad rutinaria, no únicamente con carácter excepcional.

Por último, la Comisión también apuntaba en esta última revisión efectuada que se había puesto de manifiesto que un 10 % de las entidades que afirmaban ser miembros del Acuerdo no figuraban en la lista actualizada del Departamento de Comercio, siendo las mismas tanto entidades que no habían participado nunca antes en el marco de la Decisión como aquellas que no habían renovado analmente su compromiso[517]. Asimismo, entre otras cuestiones, se identificaron una serie de mecanismos que posibilitarían una mejor defensa de los derechos de los afectados, en garantía de su derecho a una tutela judicial efectiva[518].

2.4. La vigilancia masiva efectuada por los EE. UU. El impacto sustancial de las revelaciones de Snowden

La tercera de las cuestiones que imposibilitaron su supervivencia fue motivada por las revelaciones desencadenadas por Edward Snowden, un exagente de la CIA que trabajaba para una empresa subcontratada por parte del gobierno de los Estados Unidos —llamada Booz Allen Hamilton— que, con la ayuda de un joven soldado, Bradley Manning, el 9 de junio de 2013, afirmaron ser el origen de las diversas filtraciones que se habían producido escasos días antes a través del portal WikiLeaks. Lo anterior se publicó en el marco de unas declaraciones efectuadas en el periódico británico *The Guardian*[519], mediante las cuales se desvelaron las prácticas de vigilancia masiva e indiscriminada llevadas a cabo por la National Security Agency de los EE. UU. (NSA, por sus siglas en inglés[520]), en colaboración con otras agencias de inteligencia, incluidas las europeas como la Government Communications Headquarters, perteneciente al Reino Unido.

[517] *Vid.* COMISIÓN EUROPEA, "Comunicación al Parlamento… (COM [2013] 847 final)", cit., p. 8.

[518] *Ibidem*, p. 16.

[519] Consultado el 20.08.2017 desde: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

[520] La *National Security Agency* se podría definir como un órgano de inteligencia creado por parte del gobierno de los Estados Unidos de América, dependiente del Departamento de Defensa, que tiene como principal objetivo el análisis masivo de las comunicaciones, entendido el concepto en un sentido extensivo con la intención de garantizar la protección y salvaguarda de los intereses gubernamentales de los Estados Unidos de América.

Constatándose así, que no se trataba exclusivamente de una práctica efectuada por el país norteamericano, sino que la misma estaba extendida a varios territorios.

Estas actuaciones de vigilancia masiva —que se venían efectuando desde hacía años de manera rutinaria por parte de varios gobiernos como el norteamericano—, intentaron encontrar su legitimación pública como respuesta a los atentados sucedidos el 11 de septiembre de 2001[521], permitiendo que bajo este pretexto pudieran obtenerse millones de datos personales de manera masiva de los distintos usuarios de servicios de telecomunicaciones a escala mundial. De esta manera, una vez más, se ponían de manifiesto las deficiencias normativas de las que adolecía el marco regulatorio vigente en los Estados Unidos por lo que se refiere a la protección de los datos personales, en este caso, en relación con la protección de los derechos de los ciudadanos sitos en la Unión Europea[522].

2.4.1. Contexto legislativo de vigilancia en los Estados Unidos

Con antelación a proseguir con el análisis que venimos efectuando, resulta preciso detenerse unos instantes para analizar el contexto legislativo de Estados Unidos en lo relativo a los efectos de la vigilancia y obtención de información en aras de la seguridad nacional. Para ello, cabe remontarnos al año 1972 para encontrar el caso *Keith*[523], abordado por el Tribunal Supremo de los Estados Unidos, en el que se juzgaban las

[521] Como apunta Dworkin a este respecto, además de los efectos internos del 11-S (básicamente, en el plano jurídico, los derivados de la aplicación de la *USA Patriot Act*) y dada la condición de superpotencia global de EE. UU., la nueva doctrina promovida por parte de las autoridades de Washington a partir de 2001 tuvo proyección más allá de los límites territoriales de los Estados Unidos. Es obligado reseñar, a este respecto, el tratamiento dispensado a los detenidos calificados como "combatientes ilegales" y las prácticas de tortura llevadas a cabo en establecimientos localizados fuera del territorio norteamericano, pues hay que puntualizar que no se trata de actividades ocasionales como consecuencia de la acción de incontrolados, sino de situaciones previstas, e incluso teorizadas, por las propias autoridades estadounidenses (en particular, por los Departamentos de Defensa y de Justicia) en su encrucijada contra el terrorismo. *Cfr.* DWORKIN, R., "Terror and the Attack on Civil Liberties", en *The New York Review of Books*, Vol. 50, nº 17 (2003).

[522] *Vid.* MILANOVIC, M., "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age", en *Harvard International Law Journal*, nº 56 (2015), p. 86; BOWDEN, C., "The US Surveillance Programmes and their Impact on EU Citizens' Fundamental Rights", Bruselas: Ed. Parlamento Europeo, 2013, pp. 12-15. Consultado el 15.08.2020 desde: https://op.europa.eu/es/publication-detail/-/publication/0a3aa9b5-1fe9-4f85-aaae-cc515408cf97.

[523] *Vid. United States v. United States District Court*, 407 U.S. 297 (1972).

potestades de las agencias de inteligencia respecto de los ciudadanos norteamericanos[524]. Se trataba de un supuesto en que se habían intervenido las comunicaciones telefónicas de uno de los integrantes de un partido político que formaba parte de la izquierda radical denominado *White Phanters*, que finalmente sería procesado por accionar una bomba ante una oficina de la CIA[525].

En este supuesto de hecho que venimos comentando, se juzgaba la viabilidad de que una autoridad gubernamental pudiera intervenir las comunicaciones telefónicas de un ciudadano de los Estados Unidos sin que previamente mediara una orden judicial que las habilitara, legitimándose dicha actuación en el marco de lo preceptuado por la Cuarta Enmienda, cuyo contenido hemos tenido la oportunidad de revisar sumariamente con anterioridad. El Alto Tribunal, entre otras cuestiones, manifestó una clara distinción entre la vigilancia orientada a la delincuencia común y la relacionada con finalidades relativas a la seguridad nacional, afirmando a su vez que esta última gozaba de dos vertientes: por un lado, los aspectos domésticos de la seguridad nacional (*domestic aspects of national security*) y, por otro, las actividades de potencias extranjeras y sus agentes (*activities of foreign powers or their agents*)[526].

El Tribunal concluyó que el supuesto quedaba amparado en la protección conferida por la Cuarta Enmienda, considerándose como una actuación encuadrada en el marco del concepto de los aspectos domésticos de la seguridad nacional, y que, en consecuencia, requería que las autoridades de inteligencia recabaran la previa autorización judicial con antelación a efectuar las escuchas telefónicas[527]. En este sentido,

---

[524] Por "servicios" o "agencias de inteligencia" (en inglés, "*Intelligence Community*") se entenderán los detallados en la Sección 3.5.h) de la EO 12333, tal como se indica en la nota 1 de la PPD-28. *Cfr.* Decisión de Ejecución (UE) nº 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. [notificada con el número C (2016) 4176.], nota 61. Consultado el 15.08.2020 desde: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32010D0087.

[525] *Vid*. MORRISON, T. W., *The Story of United States v. United States District Court (Keith): The Surveillance Power*, Nueva York (Estados Unidos): Ed. Schroeder C.H. & Bradley C.A., Presidential Power Stories, 2008.

[526] *Vid*. BIGNAMI, F., "The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens", en *George Washington Law School Public Law and Legal Theory Paper*, nº 2015-54 (2015), Washington (Estados Unidos), p. 20.

[527] *Vid*. RAUSTIALA, K., *Does the Constitution Follow the Flag? The Evolution of Territoriality in American Law*, Ed. Oxford University Press, 2009, pp. 157-186; ATKINSON, L. R., "The Fourth Amendment's National Security Exception: Its History and Limits", en *Vanderbilt Law Review*, Vol. 66,

nada se abordaba para aquellos supuestos en que se juzgaban cuestiones vinculadas a las potencias extranjeras y a sus respectivos agentes, en las que, como afirmaba Bignami, difícilmente pudiera extenderse la protección que confiere la Constitución de los Estados Unidos a ciudadanos que no dispongan de la nacionalidad estadounidense[528].

Una vez expuesto lo anterior, se puede contextualizar a grandes rasgos la situación normativa existente en Estados Unidos sobre la cuestión, en la que se diferencia claramente la protección ofrecida a ciudadanos norteamericanos respecto de aquellos ciudadanos que no poseen dicha nacionalidad, pues estos últimos apenas disponen de mecanismos de protección. Ante esta tesitura, podemos distinguir principalmente dos instrumentos regulatorios que dan cobertura a las situaciones de obtención de información personal sobre ciudadanos extranjeros —sobre todo, antes de las revelaciones efectuadas por E. Snowden—. Encontramos la *Foreign Intelligence Surveillance Act*[529] de 1978, complementada a su vez por la *Patriot Act* de 2001 y la *Executive Order 12333* de 1981[530]. Respecto de estas normas complementarias, cabe añadir que pese a aplicarse ambas en lo relativo a la protección de la seguridad nacional, suele acogerse la última con mayor aceptación para efectuar la vigilancia fuera de los Estados Unidos[531].

nº 5 (2009), pp. 1343-1353; SCHULHOFER, S. F., "An International Right to Privacy? Be Careful What You Wish For", *Working paper nº 15-15*, Ed. New York University. School of Law, 2015, pp. 238-258.

528 *Vid*. BIGNAMI, F., "The US Legal…", *op. cit.*, p. 20.

529 *Vid*. Estados Unidos. *50 U.S. Code, Chapter 36, Foreign Intelligence Surveillance Act*.

530 *Vid*. *Memorandum opinion of United States District Court for the District of Columbia*, de 16 de diciembre de 2013 (*Civil Action No.* 13-0851), p. 9.

531 A este respecto, Bignami apunta que además de la distinción entre amenazas a la seguridad nacional y aquellas consideradas extranjeras, existe otra distinción importante que conviene destacar para comprender las actividades de inteligencia, esto es: la inteligencia afirmativa respecto de la inteligencia protectora. Mientras que, por un lado, la inteligencia protectora (también llamada "contrainteligencia" en la *Executive Order 12333, 3.5 (a)* se puede considerar como un sinónimo de la seguridad nacional. Por otro lado, la inteligencia afirmativa (también llamada "inteligencia extranjera", en la *Executive Order 12333, 3.5 (e)* se refiere a aquellas actividades generales de recopilación de inteligencia necesarias para llevar a cabo los asuntos exteriores y la defensa nacional. En contraste con la inteligencia protectora —es decir, la seguridad nacional—, resulta menos probable que la inteligencia afirmativa esté asociada con la aplicación de la ley. Con base en estas distinciones, las Directrices del Fiscal General para las operaciones nacionales del FBI distinguen tres grandes áreas de actuación: delitos federales, amenazas a la seguridad nacional e inteligencia extranjera. Sin embargo, las Directrices también señalan que es probable que exista una superposición significativa entre estas áreas temáticas. *Cfr*. BIGNAMI, F., "The US Legal…", *op. cit.*, p. 20.

2.4.2. Contexto antes de las filtraciones efectuadas por Snowden

La *Foreign Intelligence Surveillance Act* (FISA, por sus siglas en inglés) fue promulgada por el Congreso de los Estados Unidos en 1978, con el principal objetivo de crear una estructura jurídica que permitiera dar respaldo a las prácticas de vigilancia electrónica llevadas a cabo por las agencias de inteligencia del gobierno de los Estados Unidos. Hasta la fecha, dichas actuaciones de recopilación de información se habían ido realizado sin contar con la correspondiente autorización judicial, produciéndose un menoscabo de la protección conferida por la Cuarta Enmienda, en detrimento de preservar la seguridad nacional[532].

La FISA vino a establecer un procedimiento específico para que las autoridades gubernamentales norteamericanas pudieran obtener órdenes judiciales con carácter sumario[533] que les permitieran intervenir las comunicaciones electrónicas de una potencia extranjera o de sus respectivos colaboradores, siempre que, con carácter previo, mediaran sospechas fundadas de que ello podía suponer una amenaza para la seguridad nacional[534]. A tal fin, se articularon dos tipologías de organismos judiciales: por un lado, la *Foreign Intelligence Surveillance Court* (FISC, por sus siglas en inglés), compuesta por once jueces de distrito con jurisdicción para atender solicitudes y emitir las autorizaciones judiciales; y, por otro lado, la *FISC Court of Review*, formada por tres jueces de distrito o provenientes de tribunales de apelación que tendrían potestad para revisar las solicitudes

[532] *Vid*. *Memorandum opinion of United States District Court for the District of Columbia*, de 16 de diciembre de 2013 (*Civil Action No.* 13-0851), p. 10.

[533] En el supuesto de autorización previa, los servicios solicitantes (FBI, NSA, CIA, etc.) presentaban un proyecto de solicitud a los juristas de la División de Seguridad Nacional del Departamento de Justicia para que lo estudiarán y, cuando procediera, solicitar información complementaria. Una vez finalizada la solicitud, resultaba preciso obtener el visto bueno del fiscal general, el vicefiscal general o el fiscal general adjunto de Seguridad Nacional. A continuación, el Departamento de Justicia presentaba la solicitud ante la *Foreign Intelligence Surveillance Court*, para que la evaluará y determinará de manera preliminar el modo de proceder. En caso de celebrarse una vista, el FISC estaba facultado para tomar declaración, incluso a expertos en la materia. *Vid*. Decisión de Ejecución (UE) nº 2016/1250 de la Comisión, cit., apdo. 105.

[534] En el último informe publicado por la *Administrative Office of the United States Courts*, el pasado 25 de abril de 2019, se indica que se atendieron durante 2018 un total de 1.318 solicitudes amparadas en la FISA por parte del FISC, unas 300 menos aproximadamente que durante 2017. Respecto de las cuales, se concedieron 985 órdenes, se modificaron 261 órdenes y se denegaron en su totalidad 30 solicitudes. Consultado el 20.08.2017 desde: https://www.uscourts.gov/sites/default/files/fisc_annual_report_2018_0.pdf.

denegadas por la FISC[535]. La última instancia se encontraba en el Tribunal Supremo de los Estados Unidos[536].

La FISA se ha ido modificando con posterioridad para su adecuación a las nuevas necesidades de vigilancia del gobierno de los EE. UU., pero una de sus reformas más notables se produjo con los cambios que introdujo la *Patriot Act* de 2001, aprobada como consecuencia inmediata de los atentados sucedidos el 11 de septiembre de 2001 por parte del gobierno liderado por George W. Bush. La reforma, además de dotar de mayores competencias de vigilancia a las referidas agencias federales de inteligencia, introdujo una serie de modificaciones en el propio contenido de la FISA y otras normas complementarias. Asimismo, entre otros aspectos, también tipificó nuevos delitos y reforzó los existentes con penas de mayor calado[537].

Una de las reformas sustanciales que introdujo esta norma se contenía en su Sección 215, que modificaba la FISA —en su Sección 501—[538], permitiendo que las agencias de inteligencia solicitasen una orden judicial a través de los tribunales creados bajo el acervo de la FISA, con la intención de obtener datos personales de terceros mediante la realización de requerimientos a distintas empresas que gestionan grandes volúmenes de información —como organizaciones empresariales del sector de las telecomunicaciones—. Cuando estas recibían el requerimiento, se veían obligadas a atenderlo inmediatamente facilitando cualquier registro o "cosa tangible" —como registros telefónicos, documentos o libros, esto es, todo lo que no estuviera incluido en

[535] *Vid*. RUGER, T. W., "Chief Justice Rehnquist's Appointments to the FISA Court: An Empirical Perspective", en *Northwestern University Law Review*, Vol. 101, nº 1 (2007), pp. 239-244.

[536] *Vid*. Decisión de Ejecución (UE) nº 2016/1250 de la Comisión, cit., apdo. 105.

[537] *Vid*. GOITEIN, E. y PATEL, F., "What Went Wrong with the FISA Court", Ed. Brennan Center for Justice, New York University School of Law, 2015. Consultado el 20.08.2017 desde: https://www.brennancenter.org/our-work/research-reports/what-went-wrong-fisa-court; DONOHUE, L. K., "Section 702 and the Collection of International Telephone and Internet Content", en *Harvard Journal of Law & Public Policy*, Vol 38, nº 1 (2015), pp. 119-246; DONOHUE, L. K., "Bulk Metadata Collection: Statutory and Constitutional Considerations", en *Harvard Journal of Law & Public Policy*, Vol 37, nº 3 (2014), pp. 757-900.

[538] Consultado el 20.08.2017 desde: https://www.justice.gov/archive/ll/what_is_the_ patriot_act.pdf.

las comunicaciones electrónicas[539]—, si esta era considerada necesaria para el curso de cualquier investigación centrada en la salvaguarda de la seguridad nacional[540].

Pese a que una orden judicial obtenida bajo el amparo de la FISA se emitía siempre que la vigilancia en cuestión se refiriese a ciudadanos extranjeros vinculados con la inteligencia extranjera, o en el caso de ciudadanos americanos que estuvieran relacionados con cuestiones de terrorismo internacional o actividades clandestinas de inteligencia extranjera[541], en el momento de solicitar la expedición de la autorización judicial, si ésta implicaba el acceso a "cosas tangibles", debía argumentarse ante las autoridades gubernamentales. La justificación en cuestión debía consistir en una exposición de hechos que demostraran que las sospechas eran razonables y estaban suficientemente fundadas, pues las mismas debían ser corroboradas por parte del FISC[542], debido a que este Tribunal disponía de un rol de supervisión más activo en relación con esta tipología de autorizaciones judiciales avaladas por la FISA[543].

Otra de las cuestiones que merece la pena destacar radican en las Secciones introducidas por la *FISA Amendments Act* de 2008, que ampliaron la cobertura legislativa de la norma. Por un lado, la Sección 702 habilitaba que, en idénticos términos como sucedía en los anteriores supuestos, el gobierno de los EE. UU. recopilara información sobre los servicios de inteligencia extranjeros, a través de cualquier medio de vigilancia electrónica, en aras de proteger nuevamente la seguridad nacional frente a amenazas extranjeras, así como información que pudiera perjudicar en el exterior los intereses de

---

[539] *Vid*. BIGNAMI, F., "The US Legal…", *op. cit.*, p. 24; KERR, O. S., *Computer Crime Law*, Ed. West Academic Publishing, 2ª Edición, 2013, p. 813.

[540] *Vid*. DONOHUE, L. K., "Bulk Metadata Collection…", *op. cit.*, pp. 757-776; KRIS, D. S., "On the Bulk Collection of Tangible Things", en *Journal of National Security Law & Policy*, Vol. 7, nº 209 (2014), pp. 209-295.

[541] *Vid*. BIGNAMI, F., "The US Legal…", *op. cit.*, p. 24. Adicionalmente sobre esta cuestión, KRIS y WILSON señalan que: "*FISA authorizes the federal government to engage in four types of investigative activity [in the United States]: electronic surveillance targeting foreign powers and agents of foreign powers; physical searches targeting foreign powers and agents of foreign powers; the use of pen registers and trap-and-trace devices…; and court orders compelling the production of tangible things in connection with certain national security investigations*". *Cfr*. KRIS, D. S. y WILSON, J. D., *National Security Investigations and Prosecutions*, Ed. Thomson-Reuters, 2019.

[542] Así como la solicitud debía contener un listado de los procedimientos de minimización adoptados por el fiscal general en lo referente a la conservación y difusión de la inteligencia recabada. *Vid*. Decisión de Ejecución (UE) nº 2016/1250 de la Comisión, cit., apdo. 108.

[543] *Ibidem.*

los Estados Unidos. En estos supuestos, resultaba obligatorio seguir con el mandado de los procedimientos descritos respecto de la obtención de la correspondiente orden judicial por parte de los tribunales especiales originados por la FISA[544].

Las facultades que se preveían en la Sección 702[545] pese a que eran limitadas, también fueron duramente criticadas por su contenido[546]. De esta manera, únicamente disponía de competencias sobre la aprobación de solicitudes relativas a información extranjera que se obtenía por parte de las agencias de inteligencia, en relación con posibles amenazas contra la seguridad nacional, dado que en ningún caso se revisaban solicitudes de vigilancia sobre personas físicas determinadas. Asimismo, las peticiones que se remitían para recabar la oportuna orden judicial debían completarse con la fundamentación suficiente para que pudieras prosperar, de conformidad con lo que ocurría también en relación con el supuesto analizado relativo a la aplicación de la Sección 215 de la *Patriot Act.*

En cualquier caso, las organizaciones destinatarias de la orden judicial debían cooperar en todo momento con las agencias de inteligencia que hubieran obtenido la autorización judicial conforme a la FISA; aunque en caso de no estar conforme con la petición recibida, podían optar a su apelación ante los tribunales creados también por la propia norma aludida[547]. En este punto, nos encontramos que, al tratarse de cuestiones amparadas en la confidencialidad, resultaba imposible que los afectados pudieran ejercer derecho alguno en relación con el tratamiento de sus datos personales, pues no eran informados en ningún momento de las acciones o actuaciones que se estaban produciendo[548].

---

544 *Vid*. BIGNAMI, F. y RESTA, G., "Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance", en *George Washington Law School Public Law and Legal Theory Paper*, nº 2016-67 (2017), pp. 10-11; KRIS, D. S. y WILSON, J. D., "National Security…", *op. cit.*

545 Estados Unidos. *50 U.S. Code, §1881a, Foreign Intelligence Surveillance Act.*

546 *Vid*. BIGNAMI, F. y RESTA, G., "Human Rights…", *op. cit.* p. 11; GOITEIN, E. y PATEL, F., "What Went Wrong…", *op. cit.*

547 *Vid*., entre otros: BIGNAMI, F. y RESTA, G., "Transatlantic Privacy Regulation: Conflict and Cooperation", en *Law and Contemporary Problems*, nº 78 (2015), p. 252; RICHARDS, N. M., "The Dangers of Surveillance", en *Harvard Law Review*, Vol. 126, No. 7 (2013), pp. 1934-1935; THE WHITE HOUSE, "Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies Recommendation", Recommendation 12, 2013, pp. 145-46.

548 *Vid*. KRIS, D. S. y WILSON, J. D., "National Security…", *op. cit.*

A este respecto, como afirman Bignami y Resta, la dificultad de obtener un recurso judicial, en ausencia de un proceso penal basado en pruebas adquiridas ilegalmente, se constató en el caso *Clapper v. Amnesty International USA*[549], en el que el Tribunal Supremo de los EE. UU. entendió que los peticionarios —abogados de derechos humanos y otras personas que se comunicaron con afectados situados en el extranjero— no tenían legitimación suficiente para que el asunto prosperarse. Los demandantes no pudieron probar que las comunicaciones efectuadas a través de sus propios dispositivos hubieran sido interceptadas por la NSA, cuya afirmación se consideró demasiado especulativa[550].

Por otro lado, prosiguiendo con la enumeración de novedades introducidas por la *FISA Amendments Act* de 2008, cabe citar brevemente que las Secciones 703 —prevista en 50 USC §1881b— y 704 —prevista en 50 USC §1881c— de la FISA, respectivamente, propiciaron que determinadas cuestiones relativas a la vigilancia de ciudadanos norteamericanos situados en el extranjero que se efectuaba mediante la *Executive Order 12333* de 1981[551] (EO 12333, por sus siglas en inglés) promulgada por el presidente Ronald Reagan pasaran a regularse directamente por la FISA[552]. Esta última norma se consideraba más garantista en relación con el respeto de los derechos sobre la privacidad de los ciudadanos norteamericanos al tratar cuestiones de seguridad nacional circunscritas al ámbito interno de los Estados Unidos, a pesar de que su ámbito de aplicación no estuviera limitado a ningún alcance geográfico[553].

Siguiendo con el orden de exposición que se venía efectuando, resulta preciso avanzar con el análisis del contenido previsto en la aludida *Executive Order 12333* de 1981, que, pese a ser susceptible de numerosas modificaciones[554], se preceptuaba como

---

[549] *Vid*. 133 S. Ct. 1138 (2013).

[550] *Cfr*. BIGNAMI, F. y RESTA, G., "Transatlantic Privacy…", *op. cit.*, p. 252.

[551] *Vid*. Estados Unidos. *Executive Order 12333*. Consultado el 20.08.2020 desde: http://fas.org/irp/offdocs/eo/eo-12333-2008.pdf.

[552] *Vid*. BIGNAMI, F. y RESTA, G., "Human Rights…", *op. cit.* p. 11; DONOHUE, L. K., "Section 702…", *op. cit.*, pp. 138-140.

[553] *Vid*. BIGNAMI, F. y RESTA, G., "Transatlantic Privacy…", *op. cit.*, p. 251; DONOHUE, L. K., "Section 702…", *op. cit.*, pp. 138-140.

[554] Fue enmendada en tres ocasiones, el 23 de enero de 2003 por la *Executive Order 13284*, el 27 de agosto de 2004 por la *Executive Order 13555* y el 30 de julio de 2008 por la *Executive Order 13470*, bajo el mandato del que fuera el presidente de los Estados Unidos, George W. Bush. A este respecto, conviene

el marco normativo que regulaba la actividad de las agencias de inteligencia ubicadas en Estados Unidos. La norma se encargaba de configurar las potestades que estos organismos ostentaban, así como los límites que debían respetar en la ejecución de sus respectivas actuaciones, garantizando el respeto de los derechos reconocidos en la Constitución de los EE. UU. en relación con sus respectivos ciudadanos[555]. Las competencias que se preceptúan en esta norma sobre la vigilancia se concentran básicamente en tres dimensiones: (i) cuestiones de inteligencia suscitadas fuera del territorio norteamericano; (ii) vigilancia de inteligencia extranjera —dentro y fuera de los EE. UU.—, siempre que ello no esté cubierto por la FISA; (iii) datos personales recabados de manera accidental sobre ciudadanos estadounidenses en el marco de actuaciones de investigación de inteligencia extranjera[556].

A diferencia de lo que se ha ido detallando respecto de la FISA, en que su aplicación y supervisión dependía directamente de unos tribunales creados específicamente para atender las cuestiones que se suscitaban al amparo de esta —esto es, a través de un mecanismo propio del poder judicial—, las actuaciones que se contemplan en el marco de la EO 12333 deben estar desarrolladas de conformidad con las directrices departamentales y los criterios propiciados por el Fiscal General —esto es, a través de un mecanismo interno del poder ejecutivo—, cuyas garantías que se contienen resultan aplicables únicamente sobre ciudadanos norteamericanos. En determinadas circunstancias se aplican una serie de limitaciones sobre las técnicas de recolección de información —en la mayoría de las ocasiones intrusivas—, que incluso pueden requerir que sean previamente habilitadas por parte del fiscal general[557].

---

recordar también, como señala la Comisión Europea, que el presidente de los Estados Unidos podrá dirigir dentro de los límites que el Congreso le reconoce las actividades de los servicios de inteligencia estadounidenses, en particular mediante *executive orders* (decretos) o *presidential directives* (directivas presidenciales). *Vid*. Decisión de Ejecución (UE) nº 2016/1250 de la Comisión, cit., apdo. 69.

[555] Asimismo, como la nota 59 de la Decisión de Ejecución (UE) nº 2016/1250 de la Comisión afirma, la EO 12333 determina los objetivos, las orientaciones, las obligaciones y las responsabilidades de las misiones estadounidenses de inteligencia (incluido el cometido de los distintos servicios de inteligencia) y establece los parámetros generales para llevar a cabo actividades de inteligencia (concretamente, la necesidad de promulgar normas de procedimiento específicas). En virtud del artículo 3.2 del EO 12333, el presidente, respaldado por el Consejo Nacional de Seguridad y por el director de Inteligencia Nacional, adoptará las directivas, los procedimientos y las orientaciones pertinentes y necesarios para la aplicación de este acto. *Vid*. BIGNAMI, F., "The US Legal…", *op. cit.*, p. 21.

[556] *Vid*. DONOHUE, L. K., "Section 702…", *op. cit.*, pp. 144-145.

[557] *Vid*. BIGNAMI, F., "The US Legal…", *op. cit.*, p. 27.

En este sentido, podemos afirmar que, en comparación con la FISA, la EO 12333 resulta menos garantista para la protección de los derechos de los ciudadanos de los EE. UU., pues tanto su supervisión como su aplicación práctica se contempla con mayor laxitud[558]. Asimismo, cabe destacar que, en determinados supuestos, la EO 12333 faculta a las agencias de inteligencia para que puedan colaborar con las autoridades policiales en la recopilación de información en ciertas actividades, como supuestos de terrorismo o armas de destrucción masiva, que pueden poner en peligro la seguridad nacional de los Estados Unidos. Ante estas casuísticas excepcionales, las referenciadas agencias podían incluso extender sus competencias más allá del propio territorio norteamericano[559], pero teniendo en cuenta que las garantías que se contemplan en esta norma excluyen a todos aquellos ciudadanos no estadounidenses[560].

2.4.3. Principales programas de vigilancia revelados por las filtraciones de E. Snowden

Una vez realizada la contextualización legislativa relativa a la vigilancia de las comunicaciones electrónicas a efectos de inteligencia y seguridad nacional existente durante las filtraciones efectuadas por Edward Snowden, resulta oportuno mencionar los principales programas utilizados por las agencias de inteligencia de los Estados Unidos para llevar a cabo tal cometido. Por un lado, podemos destacar el programa dedicado a la lucha contra el terrorismo denominado "*Bulk Telephony Metadata Program*", que fue diseñado para crear un histórico completo sobre registros telefónicos que proporcionase una ayuda complementaria en las investigaciones relativas a la prevención de actividades terroristas efectuadas por parte del *Federal Bureau of Investigation* (FBI, por sus siglas en inglés)[561].

---

[558] *Vid*. KRIS, D. S. y WILSON, J. D., "National Security…", *op. cit.*

[559] *Vid*. BIGNAMI, F., "The US Legal…", *op. cit.*, pp. 27-28.

[560] *Vid*. BIGNAMI, F. y RESTA, G., "Human Rights…", *op. cit.* p. 10.

[561] *Vid*., entre otros: MARGULIES, P., "The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism International Counterterrorism", en *Fordham Law Review*, Vol. 82, nº 5 (2014), pp. 2140-2141, DONOHUE, L. K., "Bulk Metadata Collection…", *op. cit.*, pp. 757-900; BRADBURY, S. G., "Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata Under Section 215 and Foreign-Targeted Collection Under Section 702", en *Lawfare Research Paper Series*, nº 1 (2013); KRIS, D. S., "On the Bulk Collection of Tangible Things", en *Lawfare Research Paper Series*, nº 1 (2013); MARGULIES, P., "Evolving Relevance: The Metadata Program and the Delicate Balance of Secrecy, Deliberation, and National Security", en *Legal Studies Research Paper Series*, nº 146 (2014), Roger Williams Univ. Sch. of Law.

El programa en cuestión que estamos exponiendo encontraba su legitimación en la Sección 1861 de la FISA, en base a su redacción original que data de 1998, siendo posteriormente enmendada en 2001 por la Sección 215 de la *Patriot Act*, así como en 2006 como consecuencia de la Ley de Reautorización *(Reauthorization Act)*. Esta última reforma propició que el Congreso, entre otras modificaciones, dotará de un derecho de revisión judicial a aquellos destinatarios de las órdenes de presentación emitidas bajo dicha Sección 1861 ante la FISC, pues dicha posibilidad no quedaba contemplada en el ordenamiento jurídico estadounidense con antelación a la existencia de la enmienda[562].

En general, los registros que se obtenían mediante la utilización de este programa se categorizaban como metadatos[563], recogiéndose una serie de datos personales como números de teléfono, franjas horarias de las llamadas, duración de estas, la identificación de sesión del terminal, el *International Mobile Subscriber Identity* (IMSI, por sus siglas en inglés) o el *International Mobile Equipment Identity* (IMEI, por sus siglas en inglés), excluyendo cualquier información sobre el contenido de las llamadas, así como los nombres, direcciones o información financiera de las partes implicadas en la llamada. En todo caso, el Gobierno de los EE. UU. siempre ha manifestado que nunca se han llevado a cabo estas actuaciones de una manera indiscriminada[564].

El programa se inició a partir de 2006, extendiéndose su duración durante más de siete años[565], propiciando que el FBI obtuviera diariamente los metadatos de ciertas

---

[562] *Vid*. *Memorandum opinion of United States District Court for the District of Columbia*, de 16 de diciembre de 2013 (*Civil Action No.* 13-0851), pp. 6-7.

[563] A este respecto, resulta preciso traer a colación la definición que el GT29 contempla respecto a los metadatos, pues los define como: "Todos los datos sobre una comunicación en curso, excepto el contenido de la conversación. Pueden incluir el número de teléfono o dirección IP de la persona que hace una llamada o envía un correo electrónico, el tiempo y la información relativa a la ubicación, el asunto, el destinatario, etc. Sus análisis pueden revelar datos delicados sobre las personas, debido a las llamadas a determinados números de información médica o centros religiosos, por ejemplo". Asimismo, el GT29 considera que, aunque *a priori* parece que la recogida de metadatos pueda considerarse menos gravosa para los derechos y libertades de los afectados, ello no es así, pues con su tratamiento masivo mediante la utilización de instrumentos informáticos pueden obtenerse conjuntos de datos personales estructurados más fácilmente que analizando el contenido de las comunicaciones, cuyo trabajo resultaría más arduo. *Cfr.* COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 215): Dictamen 04/2014 del Grupo de Trabajo del Artículo 29, sobre la vigilancia de las comunicaciones a efectos de inteligencia y seguridad nacional", aprobado por el Grupo de Trabajo, el 10 de abril de 2014, pp. 4-5.

[564] *Ibidem.*

[565] Teniendo en cuenta lo anterior, resulta ilustrativo apuntar a título anecdótico el artículo publicado en el diario británico *The Economist*, en fecha 15 de junio de 2013, titulado *"Surveillance: Look who's listening"*, el cual comentaba sarcásticamente que las autoridades estadounidenses parecían creer que la

compañías de telecomunicaciones bajo el acervo de las órdenes judiciales emitidas por parte de la FISC. Una vez que se obtenían dichos datos por parte de las agencias de inteligencia, la NSA consolidaba toda la información recabada en una base de datos centralizada, permitiendo que sus analistas dispusieran de un repositorio que contenía el histórico de las comunicaciones que les permitía vincular rápidamente diferentes números de teléfono ante la búsqueda de potenciales amenazas terroristas contra los Estados Unidos[566].

Así pues, el programa que se viene comentado tuvo que asumir su examen judicial en los años venideros, pues en 2009 fue el FISC quien determinó que la NSA había incurrido en un "sistemático incumplimiento" con el desarrollo y utilización del "Bulk Telephony Metadata Program" y, posteriormente, la *U. S. District & Bankruptcy Court* del Distrito de Columbia, mediante el *Memorandum Opinion* sobre la *Civil Action Nº 13-0851 (RJL),* de fecha 16 de diciembre de 2013, también tuvo ocasión de pronunciarse al respecto. En este sentido, tal y como detalla el memorándum, tras las revelaciones efectuadas por E. Snowden, se plantearon dos procedimientos durante el mandato de Barack H. Obama —los asuntos *Klayman I* y *Klayman II*, de fechas 2 y 12 de junio, respectivamente—, en los que se constataba el empleo de prácticas de vigilancia masiva e indiscriminada por parte de las agencias de inteligencia y ciertas empresas de telecomunicaciones y servicios digitales[567].

Las partes demandantes hicieron valer sus pretensiones basándose en que los usuarios de los referidos servicios habían visto vulnerados sus derechos individuales recogidos en la Primera, Cuarta y Quinta Enmienda de la Constitución, así como las garantías recogidas en la *Administrative Procedure Act* por las prácticas abusivas de vigilancia llevadas a cabo por las autoridades gubernamentales, excediéndose de las potestades y competencias autorizadas por la FISA[568].

---

obtención de registros de cada llamada telefónica efectuada en Estados Unidos resultaba susceptible de ser considerada relevante para una investigación o un baluarte esencial de la lucha que efectuaba el referido país contra el terrorismo internacional. Consultado el 20.08.2020 desde: https://www.economist.com/briefing/2013/06/15/look-whos-listening.

566 *Vid*. *Memorandum opinion of United States District Court for the District of Columbia*, de 16 de diciembre de 2013 (*Civil Action No.* 13-0851), p. 8.

567 *Ibidem*, pp. 20-21.

568 *Ibidem*, p. 24.

Así pues, el juez Richard J. Leon que suscribe el memorándum mantiene que la situación que se analiza en este caso concreto —relativa al "Bulk Telephony Metadata Program"—, no podía ser susceptible de realizar un ejercicio de analogía con el caso *Smith v. Maryland*[569] como solicitaban las autoridades gubernamentales, pues los paradigmas de los que se partía resultaban ser antagónicamente diferentes. En este supuesto, se planteaban dos escenarios diferentes por lo que a los avances tecnológicos y sociales se refiere, dado que en 2013 se planteaba un nuevo paradigma en el que las tecnologías que se utilizaban para llevar a cabo la actividad de vigilancia eran más invasivas que antaño. Así entonces, el juez Leon sostiene que el programa en cuestión viola la expectativa razonable de privacidad amparada por la Cuarta Enmienda[570].

Y, por otro lado, relacionado con el análisis que se viene efectuando sobre los programas utilizados por las agencias de inteligencia de los Estados Unidos que fueron objeto de revelación, podemos mencionar también PRISM y Upstream, ambos amparados bajo la Sección 702 de la FISA[571]. En este caso, nuevamente vemos como las autoridades gubernamentales norteamericanas podían llevar a término actividades de vigilancia sobre el contenido de las comunicaciones de personas que no ostentaran la nacionalidad estadounidense, sobre las cuales existieran sospechas razonables de que se encontrasen fuera de Estados Unidos para adquirir información clasificada de inteligencia extranjera que pudiera poner en peligro la seguridad nacional.

---

[569] En el asunto *Smith v. Maryland*, 442 US 73 5 (1979), el Tribunal Supremo de los Estados Unidos dictaminó que no se otorgaba una expectativa razonable de privacidad respecto de los datos personales que se transmiten a las operadoras de telecomunicaciones.

[570] *Vid. Memorandum opinion of United States District Court for the District of Columbia*, de 16 de diciembre de 2013 (*Civil Action No.* 13-0851), p. 45.

[571] En virtud de la Sección 702 de la FISA, el FISC no autoriza medidas de vigilancia individuales, sino programas de vigilancia (como PRISM o Upstream) sobre la base de certificaciones anuales elaboradas por el Fiscal General y el Director de Inteligencia Nacional. El artículo 702 de la FISA permite fijar como objetivos de la adquisición de información de inteligencia exterior a personas de las que se tengan motivos fundados para pensar que se encuentran ubicadas fuera de los Estados Unidos. Estos objetivos son fijados por la NSA en dos fases: en primer lugar, los analistas de la NSA identificarán a los ciudadanos no estadounidenses ubicados en el extranjero cuya vigilancia vaya a conducir, con arreglo a la valoración de los analistas, a la obtención de la inteligencia exterior pertinente especificada en la certificación; en segundo lugar, una vez que estas personas específicas han sido identificadas y aprobadas como objetivos a través de un amplio mecanismo de examen dentro de la NSA, se asignan (es decir, se desarrollan y aplican) una serie de selectores que identifican los recursos de comunicación (por ejemplo, direcciones de correo electrónico) utilizados por dichas personas. Según se indica, las certificaciones que han de recibir el visto bueno del FISC no contienen información sobre las personas objetivo propiamente dichas, sino que identifican categorías de información de inteligencia exterior. *Cfr.* Decisión de Ejecución (UE) nº 2016/1250 de la Comisión, cit., apdo. 109.

Sobre el funcionamiento de los dos programas informáticos que se vienen indicando, Bignami y Resta afirman que la NSA en primera instancia obtiene el contenido y los metadatos de un sector de empresas prestadoras de servicios de Internet que previamente ha sido delimitado en base a un "término de selección". De esta forma, la tipología de información recabada variará en función del prestador de servicios escogido, pudiendo ir desde correos electrónicos hasta videos o detalles que se encontrasen publicados en redes sociales, entre muchos otros. En segunda instancia, y en función del "término de selección" por el que se hubiera optado, mediante Upstream, las autoridades gubernamentales obligan a los prestadores que controlan las comunicaciones a interceptarlas directamente para acceder a su contenido[572].

En suma, respecto de estos programas de vigilancia, cabe citar dos cuestiones. Inicialmente en cuanto al programa Upstream, que con arreglo a un dictamen desclasificado del FISC de 2011, se apuntaba que más del 90 % de las comunicaciones electrónicas recabadas en virtud del artículo 702 de la FISA procedían del programa PRISM, mientras que menos del 10 % provenían del programa Upstream[573]. Y, posteriormente, con respecto a la información personal recopilada en virtud de la Sección 702 de la FISA, los procedimientos de minimización de la NSA aprobados por el FISC preveían como norma general que los metadatos y los contenidos no evaluados del programa PRISM no pudieran conservarse más de cinco años y, en el caso de los datos de Upstream, no más de dos años.

2.4.4. Contexto posterior de las filtraciones efectuadas por Snowden

Las revelaciones efectuadas por Snowden propiciaron que se sucedieran algunos instrumentos legislativos en el ordenamiento jurídico estadounidense, pretendiendo reaccionar ante las acusaciones que se habían vertido sobre las prácticas abusivas que se llevaban a cabo en materia de vigilancia y obtención de información por parte de los EE. UU. en virtud de garantizar la protección de la seguridad nacional. En este sentido, emergieron dos iniciativas legislativas que conviene citar. Por un lado, el 17 de enero de 2014, se aprobó la *Presidential Policy Directive 28* (PPD-28, por sus siglas en inglés) que

[572] *Vid*. BIGNAMI, F. y RESTA, G., "Transatlantic Privacy…", *op. cit*., p. 249.

[573] *Vid*. FISC: Dictamen 2011 WL 10945618 (FISA Ct. [FISA Court], 03.10.2011), nota 21. Consultado el 20.08.2020 desde: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.

establecía una serie de limitaciones en las operaciones de inteligencia de señales[574] —que están a cargo del Director de la NSA—, cuyo contenido resulta vinculante para todas las agencias de inteligencia de los Estados Unidos, independientemente de los cambios que puedan producirse en el Gobierno norteamericano[575].

La PPD-28 contiene diversas disposiciones dirigidas a los ciudadanos que no ostentan la nacionalidad estadounidense[576], pues, entre otras, puede destacarse en un primer término que, para poder llevar a cabo una recopilación de inteligencia de señales, debe mediar un previo acto legislativo o una autorización presidencial. En un segundo término, se preceptúa un principio de igualdad y dignidad para todas las personas investigadas, independientemente de su nacionalidad o lugar de residencia, así como también una expectativa de privacidad respecto de su información personal. Y en un tercer término, se prevé una obligación que preceptúa que todas las actividades de inteligencia de señales deben de realizarse de forma adecuada, en aras de no menoscabar los derechos y libertades de los afectados[577].

El contenido de la PPD-28 también establece que deberán priorizarse técnicas de recogida de información que resulten lo menos intrusivas posibles, optando por búsquedas selectivas de términos antes que proceder a recabar datos de forma masiva e indiscriminada —aunque esta última opción está prevista en supuestos en los que se pretenda identificar a nuevas amenazas—. Así como *a priori* las declaraciones efectuadas por el gobierno estadounidense aseguran que las decisiones acerca de la recogida de información no constituyen una facultad discrecional de cada agente de inteligencia, sino

---

[574] La inteligencia de señales SIGINT, bajo sus siglas en inglés) consiste en la obtención de información técnica y de inteligencia a partir de las emisiones realizadas por sistemas de comunicaciones y aquellos que no tienen tal consideración, como radares o perturbadores. *Vid*. "Monografías del SOPT. La Guerra electrónica en España. Ministerio de Defensa". Consultado el 20.08.2020 desde: https://www.tecnologiaeinnovacion.defensa.gob.es/Lists/Publicaciones/Attachments/13/monografia_sopt_2.pdf.

[575] *Vid*. Decisión de Ejecución (UE) nº 2016/1250 de la Comisión, cit., apdo. 68.

[576] A este respecto, la Comisión apunta que: "[A]l estar contenidos en una directiva adoptada por el presidente en calidad de Jefe de Gobierno, estos requisitos vinculan a la totalidad de los servicios de inteligencia y se han aplicado asimismo a través de una serie de normas y procedimientos institucionales que incorporan los principios generales a las instrucciones específicas aplicables a sus operaciones cotidianas. Por otro lado, aunque el Congreso no está directamente vinculado por la PPD-28, también ha adoptado medidas para garantizar que la recopilación de datos personales y el acceso a los mismos en los Estados Unidos sean de carácter selectivo en lugar de «generalizados»". *Cfr*. Decisión de Ejecución (UE) nº 2016/1250 de la Comisión, cit., apdo. 77.

[577] *Vid*. Decisión de Ejecución (UE) nº 2016/1250 de la Comisión, cit., apdo. 69.

que han de basarse en las políticas y procedimientos que los servicios de inteligencia norteamericanos deben adoptar para aplicar la PPD-28[578].

A este respecto, resulta oportuno traer a colación las consideraciones efectuadas por Bignami y Resta[579], dado que con posterioridad a afirmar que las garantías que se contienen en la PPD-28 se componen de una estructura de protección de datos clásica, en la que se contiene un compromiso general de proporcionalidad, garantías sobre la limitación del uso, la difusión y la retención, además de cuestiones de seguridad y supervisión. En consonancia con lo que una parte de la doctrina sobre la materia ha tenido ocasión de manifestar[580], también constatan que su contenido no ha conllevado un cambio significativo sobre el marco normativo al que están sujetas las agencias de inteligencia, sino que se ha optado por una operación simbólica que apenas ha tenido una eficacia práctica.

Y, por otro lado, en junio de 2015 se aprobó la *USA Freedom Act*, que vino a modificar las competencias de vigilancia y seguridad nacional de los Estados Unidos de América, en aras de propiciar una mayor transparencia sobre las prácticas llevadas a cabo por las agencias de inteligencia y los tribunales amparados bajo la FISA. Concretamente, el texto aboga por el mantenimiento de la prohibición de recopilar de forma masiva e indiscriminada registros sobre ciudadanos estadounidenses y no estadounidenses —según la Sección 501 de la FISA—. Esta casuística que había quedado debidamente acreditada a partir de las revelaciones efectuadas por Snowden ante distintos medios de comunicación.

La prohibición recaía sobre las disposiciones que se contienen en la FISA o en las *National Security Letter* (NSL, por sus siglas en inglés)[581], que habilitan, entre otras

[578] *Ibidem*, apdo. 70.

[579] *Vid*. BIGNAMI, F. y RESTA, G., "Human Rights…", *op. cit*. pp. 10-11.

[580] *Vid*., entre otros: KRIS, D. S., "On the Bulk Collection…", en *Journal of National…*, *op. cit*., pp. 209-289; SEVERSON, D., "American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change", en *Harvard International Law Journal*, Vol. 56, nº 2 (2015), pp. 465-514.

[581] A pesar de que ya existían con anterioridad a los atentados sucedidos el 11 de septiembre de 2001, se empezaron a utilizar con mayor asiduidad a partir de dicha fecha las denominadas "*National Security Letters*", que, como indica la Oficina del Director de Inteligencia Nacional (ODNI, por sus siglas en inglés) en la nota nº 38 del Anexo VI de la Decisión de Ejecución (UE) 2016/1250 de la Comisión, "están autorizadas por varias leyes y permiten que el FBI obtenga información contenida en informes crediticios, registros financieros y registros electrónicos de abonados y de operaciones de determinados tipos de

cuestiones, la recopilación en bloque de metadatos a partir de la realización de escuchas telefónicas o registros de llamadas salientes fuera de los Estados Unidos. Su utilización impone la obligatoriedad de adoptar un "criterio de selección específico" en la búsqueda de información para garantizar los derechos y libertades de los afectados. Este aspecto pone en duda que teóricamente estas prácticas no se vinieran efectuando, pues, como hemos visto mediante los distintos programas de inteligencia publicados, las garantías que debían adoptarse en su ejecución no se respetaban de manera habitual[582].

Adicionalmente, también se aumentaron las prácticas de transparencia y de garantía de la privacidad, designándose un panel permanente de abogados expertos en privacidad, libertades colectivas, recopilación de inteligencia o tecnología. Estos podían ser consultados por parte de los tribunales de la FISA en calidad de *amicus curiae*[583] en aquellos supuestos en los que se planteasen interpretaciones novedosas o de relevancia sobre determinadas normas previstas en el ordenamiento jurídico norteamericano y se encontraban investidos de competencia suficiente para exponer los argumentos que considerasen necesarios en aras de garantizar la salvaguarda de los derechos y libertades de los afectados[584].

Respecto de lo anterior, cabe citar que un análisis efectuado al respecto por parte del *Brennan Center for Justice* en 2020 destaca que desde la promulgación de la *USA Freedom Act* de 2015, únicamente se tiene constancia de que se hayan utilizado en 11 ocasiones —estando disponibles las decisiones solo para 8 de esos casos—, pues la

---

empresas, con el único propósito de protegerse contra el terrorismo internacional o las actividades de inteligencia clandestinas. Las cartas de seguridad nacional son utilizadas normalmente por el FBI para reunir información de contenido no crítico en las primeras fases de las investigaciones antiterroristas y de contraespionaje, como la identidad del abonado a una cuenta que se haya puesto en comunicación con agentes de un grupo terrorista como ISIL. Los destinatarios de la Carta Nacional de Seguridad tienen derecho a impugnarla ante un tribunal". Al respecto, la Comisión Europea sigue apuntado en la nota nº 79 de la Decisión que "[E]l principal fundamento jurídico existente parece ser la *Electronic Communications Privacy Act* (Ley de Privacidad de las Comunicaciones Electrónicas, codificada en el título 18, artículo 2709, del USC), que dispone que toda solicitud de información sobre los abonados o registros de operaciones utilice un término que identifique específicamente a una persona, una entidad, un número de teléfono o una cuenta". *Vid*. Decisión de Ejecución (UE) nº 2016/1250 de la Comisión, cit.

582 *Vid*. Punto III del Anexo IV de la Decisión de Ejecución (UE) nº 2016/1250 de la Comisión, cit.

583 Expresión de origen latino utilizada con frecuencia para referirse a una persona o grupo que no es parte de un litigio, pero que, por tener un interés en el asunto, o por resultar de un mandato normativo, facilitará al tribunal un escrito sobre una cuestión específica de la acción con la intención de influir en la decisión y resolución del proceso judicial del que se trate.

584 *Ibidem.*

capacidad de influencia de la que disponían los *amicus curiae* sobre los tribunales amparados bajo la FISA para que impusieran restricciones a los programas de vigilancia efectuados por la NSA había sido previamente limitada. Sin contar además con que la mayoría de los miembros que forman parte de este cuerpo habían ostentado con anterioridad cargos vinculados a la salvaguarda de la seguridad nacional. Este aspecto en la práctica se traduce en una ausencia de independencia en el momento de valorar decisiones vinculadas a la protección de los derechos y libertades de los afectados. Por este motivo, el referido Centro aboga por una mayor implicación de estos actores y que su intervención esté respaldada por parte del Congreso de los EE. UU.[585]

Así pues, como última cuestión a destacar vinculada a las novedades sobre transparencia introducidas por la *USA Freedom Act* de 2015, podemos afirmar que —tal y como se indica en la Decisión 2016/1250 de la Comisión—, el Gobierno de los Estados Unidos debe facilitar cada año al Congreso (y al público) el número de mandamientos y directivas solicitados o recibidos en virtud de la FISA, así como estimaciones del número de ciudadanos estadounidenses y no estadounidenses sometidos a vigilancia, entre otros datos. La citada Ley impone asimismo la obligación de divulgar el número de NSL emitidas tanto con respecto a los ciudadanos estadounidenses como a aquellos no estadounidenses (si bien, al mismo tiempo, permite a los destinatarios de mandamientos y certificaciones, en virtud de la FISA y de solicitudes en forma de NSL, presentar informes de transparencia en determinadas circunstancias)[586].

Una vez observado el desconcierto generado en Estados Unidos —y, por ende, en la comunidad internacional—, a tenor de las ya referidas revelaciones efectuadas por E. Snowden, así como esbozado el escenario regulatorio afectado por ellas, tanto en su perspectiva anterior como posterior a la divulgación, en el contexto comunitario la Comisión Europea, el 27 de noviembre de 2013, tomó una serie de iniciativas para reabrir el diálogo con las autoridades de Estados Unidos mediante una serie de comunicaciones efectuadas en el Parlamento Europeo y en el Consejo de la Unión Europea. Estas tenían como principal objetivo reafirmar la alianza estratégica que unía a ambos territorios, así

[585] PATEL, F. y KOREH, R., "Enhancing Civil Liberties Protections in Surveillance Law", en *New York University – Annual Survey of American Law*, Nueva York, 2020. Consultado el 20.08.2020 desde: https://www.brennancenter.org/our-work/analysis-opinion/enhancing-civil-liberties-protections-surveillance-law.

[586] *Cfr.* Decisión de Ejecución (UE) nº 2016/1250 de la Comisión, cit., apdo. 104.

como destacar la importancia fundamental de los flujos de datos transatlánticos para el comercio, la aplicación de la legislación vigente y las políticas nacionales.

Todo ello reconociendo a su vez que las revelaciones efectuadas por el E. Snowden habían dañado la confianza de la Unión Europea en el Acuerdo de Puerto Seguro y que la misma debería de ser reconstruida y fortalecida[587]. En las mencionadas comunicaciones, la Comisión efectuó trece recomendaciones que tenían como principal objetivo subsanar las debilidades que se habían puesto de manifiesto sobre el Acuerdo de Puerto Seguro, para que el mismo pudiera seguir siendo un mecanismo eficaz que permitiera el intercambio transatlántico de datos personales[588].

En los meses venideros, las autoridades comunitarias realizarían sendos esfuerzos en consensuar posiciones y articular negociaciones, que serían dadas a conocer públicamente en junio de 2014, momento en el que la entonces vicepresidenta de la Comisión Europea, Viviane Reding, aprovechó para efectuar unas declaraciones que actualizaban el estado de las negociaciones, así como para exponer que el Departamento de Comercio de los Estados Unidos había aceptado doce de las trece recomendaciones que se le habían trasladado. Sin embargo, manifestó que el único punto de fricción se encontraba en la necesidad de mantener la excepción vinculada a la seguridad nacional, pues la Comisión no la entendía como tal, sino más bien como una cláusula residual que servía para amparar multitud de acciones que, en la mayoría de las ocasiones, comportaban un menoscabo de los derechos y libertades de los afectados[589].

Ante esta tesitura y teniendo en cuenta que se sucedieron una serie de demandas provenientes de varios sectores sociales, así como de las propias autoridades de control

[587] Concretamente, la Comisión Europea expone el siguiente tenor literal: "El acceso a gran escala por parte de las agencias de inteligencia a los datos transferidos a Estados Unidos por entidades con certificación de puerto seguro suscita serias cuestiones adicionales en lo que respecta al derecho de los europeos a que sus datos sigan estando protegidos cuando se transfieren a ese país". *Cfr*. COMISIÓN EUROPEA, "Comunicación al Parlamento… (COM [2013] 847 final)", cit., pp. 19.

[588] *Vid*. COMISIÓN EUROPEA, "Comunicación al Parlamento… (COM [2013] 847 final)", cit., pp. 19-21.

[589] *Vid*. Nota de prensa efectuada por la entonces vicepresidenta de la Comisión Europea, Viviane Reding, en fecha 6 de junio 2014, sobre las negociaciones del Acuerdo de Puerto Seguro, a la luz de las revelaciones sobre la vigilancia masiva realizadas por E. Snowden. Consultado el 20.08.2017 desde: http://europa.eu/rapid/press-release_SPEECH-14-431_en.htm.

de algunos Estados miembros[590], que abogaban por la supresión del Acuerdo de Puerto Seguro, el gobierno de los Estados Unidos —en aquellos momentos liderado por el presidente Barack Obama— se vio obligado a admitir las filtraciones que se habían producido. Esto puso de manifiesto la existencia de varios "programas" de vigilancia masiva, como por ejemplo sucedió, entre otros, con el programa acuñado bajo la denominación "PRISM" que hemos tenido la ocasión de examinar, cuya existencia incluso había sido ya anunciada por la propia Comisión Europea[591].

[590] *Vid*. Resolución del Parlamento Europeo nº 2016/C075/14 de fecha 4 de julio de 2013, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de Estados Unidos, los organismos de vigilancia en varios Estados miembros y su impacto en la vida privada de los ciudadanos de la Unión Europea (2013/2682 [RSP]).Consultado el 20.08.2017 desde: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//NONSGML+TA+P7-TA-2013 0322+0+DOC +PDF+V0//EN.

[591] A este respecto, la Comisión había apuntado que "[A] lo largo de 2013, la información sobre la escala y el alcance de los programas estadounidenses de vigilancia han suscitado inquietudes sobre la continuidad de la protección de los datos personales transferidos a Estados Unidos con arreglo al marco de puerto seguro. Por ejemplo, aparentemente todas las empresas involucradas en el programa PRISM, y que conceden a las autoridades estadounidenses acceso a los datos almacenados y tratados en Estados Unidos, tienen el certificado de puerto seguro. Esto ha hecho de puerto seguro uno de los conductos a través de los cuales se da acceso a las autoridades de inteligencia estadounidenses para recopilar datos personales que han sido tratados inicialmente en la Unión Europea". *Cfr*. COMISIÓN EUROPEA. (2013). "Comunicación al Parlamento… (COM [2013] 847 final)", cit., p. 17.

3. Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015, asunto C-362/14 ("Schrems I")

3.1. Antecedentes de hecho

Para iniciar correctamente la explicación, resulta oportuno efectuar una breve introducción sobre el supuesto de hecho que antecede la presente decisión judicial[592]. El Sr. Maximilian Schrems, un jurista austríaco con residencia habitual en Irlanda, en fecha 25 de junio de 2013 decide instar una denuncia ante el *Data Protection Comissioner* —autoridad nacional de protección de datos de Irlanda— solicitando la suspensión de las transferencias internacionales de sus datos personales de *Facebook Ireland*[593] a los Estados Unidos. En dicha petición afirma que esta última mercantil citada —bajo su posición de responsable del tratamiento— no disponía de los mecanismos habilitantes necesarios que la legitimasen para articular transferencias transatlánticas de sus datos de carácter personal a territorio norteamericano debido a que había quedado totalmente acreditado el acceso indiscriminado que estaban realizando las agencias de inteligencia estadounidenses respecto de los datos personales de ciudadanos europeos en base a las revelaciones efectuadas por E. Snowden.

Sin embargo, el Comisionario irlandés, desestimó la denuncia sobre la base de que no existían pruebas sustanciales que permitieran acreditar los hechos expuestos, así como declaró que cualquier cuestión relativa a la validez de la Decisión debía sustanciarse procesalmente por los cauces adecuados previstos en el contenido de la norma. En este sentido, también se indicó que la Comisión Europea ya había tenido la oportunidad de determinar con anterioridad a la denuncia presentada, la viabilidad del Acuerdo de Puerto Seguro y que, por lo tanto, no podía impugnarse la validez de la Decisión adoptada por parte del susodicho organismo europeo.

Lo anterior no convenció al Sr. Schrems, por lo que optó por la posibilidad de acudir a la vía jurisdiccional, interponiendo un recurso contra la decisión de la autoridad irlandesa ante el Tribunal Supremo de Irlanda, con la intención de que la decisión

[592] *Vid*. STJUE. Asunto C-362/14 (Schrems I), cit.

[593] Facebook, del mismo modo que también lo han realizado otras compañías multinacionales, ha ubicado su sede principal de actividades de Europa en Irlanda por una cuestión de carácter tributario, pues el nivel de carga impositiva que se impone en dicho territorio resulta menor que en el resto de los países de la Unión Europea. *Vid.* DARCY, S., "Battling for the Rights to Privacy and Data Protection in the Irish Courts", en *Utrecht Journal of International and European Law*, Vol. 31, nº 80 (2015), p. 131.

adoptada por el Comisionario irlandés fuera objeto de revisión, y a su vez, sirviera como base para pronunciarse sobre la viabilidad del nivel de protección adecuado del que hasta la fecha gozaban los EE. UU.

En este contexto, el Tribunal Supremo de Irlanda consideró que la *quaestio litis* concernía a una materia que debía de sustanciarse mediante los órdenes jurisdiccionales comunitarios. Por este motivo, decidió suspender el procedimiento nacional para plantear una cuestión prejudicial ante el organismo judicial competente, esto es el Tribunal de Justicia de la Unión Europea, sobre dos puntos en concreto. Por un lado, sobre si una autoridad de control nacional en materia de protección de datos, aunque hubiera constatado que un tercer país no garantiza un nivel de protección adecuado de los datos personales recabados, estaría vinculada, en su totalidad, por las decisiones que hubiera emitido la Comisión Europea —en el presente caso, respecto de la Decisión, de 26 de julio de 2000, analizada y comentada con anterioridad—.

Y, por otro lado, en el supuesto de que no existiera una vinculación directa, se planteó la cuestión sobre si una autoridad de control nacional en materia de protección de datos personales podría realizar sus propias investigaciones sobre un asunto en particular, como consecuencia de la aparición de nuevos hechos noticiables que recomendasen la revisión de la Decisión.

Ante esta situación, el Tribunal de Justicia de la Unión Europea celebró su primera y única audiencia pública sobre este asunto el 24 de marzo de 2015, para posteriormente, en fecha 6 de octubre de 2015, hacer público su pronunciamiento mediante un análisis conjunto de ambas cuestiones planteadas. Como señala Uría Gavilán a este respecto: "Las conclusiones que alcanza el Tribunal coinciden con las del abogado general Bot, que fueron presentadas tan solo dos semanas antes de que el TJUE dictara su sentencia[594]. Tanto el Tribunal como el abogado general deciden sobre dos elementos cardinales: uno de tipo procedimental, relativo a los poderes de las autoridades nacionales de protección

[594] Resulta poco usual que se presentasen las conclusiones del abogado general, Yves Bot, escasamente dos semanas antes del pronunciamiento del TJUE, cuando estaban previstas inicialmente para el 24 de junio de 2015.

de datos y otro de tipo sustantivo, referente a la validez de la Decisión de puerto seguro"[595].

3.2. Contenido de la Sentencia "Schrems I"

Una vez analizado el supuesto de hecho que precede el pronunciamiento efectuado por parte del TJUE, conviene examinar el contenido de este. En primer lugar, se manifiesta la obligatoriedad a la que están sometidos los Estados miembros, y, por ende, sus respectivas autoridades nacionales, a dar cumplimiento a los pronunciamientos que se emitan por parte de las instituciones comunitarias. En este caso, las decisiones emitidas por parte de la Comisión Europea, al amparo de las facultades reconocidas por el artículo 25.6 de la Directiva 95/46/CE, dado que, como consecuencia del mandato efectuado por el artículo 28.4 del Tratado de Funcionamiento de la Unión Europea[596], las mismas tendrán carácter vinculante para los Estados miembros, quienes deberán articular los medios que resulten necesarios para darle el debido cumplimiento, siempre que las decisiones no hayan sido previamente declaradas inválidas por parte de los órganos jurisdiccionales correspondientes[597].

Sin perjuicio de lo anterior, el Tribunal también admite que ello no puede suponer que no se examinen las pretensiones que se efectúen por parte de un interesado respecto de la protección de sus datos de carácter personal. Máxime cuando estos pueden ser transferidos a un tercer país que no garantiza un nivel de protección adecuado[598]. La Decisión no pretendía limitar las competencias propias que ostenta una autoridad de control nacional de un Estado miembro que, en todo momento, debía atender las solicitudes que le fueran dirigidas con la máxima diligencia. Pero recuerda que quien

---

[595] *Cfr*. URÍA GAVILÁN, E., "Derechos fundamentales versus vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 (Schrems I)", en *Revista de Derecho Comunitario Europeo*, nº 53 (2016), pp. 267-268.

[596] *Vid*. Artículo 28 del Tratado de Funcionamiento de la Unión Europea. Consultado el 20.08.2017 desde: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:12012E291.

[597] *Vid*., entre otros: CRESPI, S., "The Applicability of Schrems Principles to the Member States: National Security and Data Protection within the EU Context", en *European Law Review*, nº 5 (2018), pp. 669-686; KUNER, C., "Reality and Illusion in EU Data Transfer Regulation Post Schrems", *German Law Journal*, Vol. 18, nº 14 (2017), pp. 881-918.

[598] *Vid*. STJUE. Asunto C-362/14 (Schrems I), cit., apdo. 56.

decide en última instancia sobre la validez de un acto normativo de esta índole es el Tribunal de Justicia de la Unión Europea[599].

En segundo lugar, el Tribunal entra a valorar la validez de la Decisión de la Comisión, de fecha 26 de julio de 2000, exponiendo en primera instancia la ausencia de efectividad del mecanismo de autocertificación que propugnaba el artículo 1, dado que los principios establecidos en el referido Acuerdo de Puerto Seguro eran únicamente aplicables ante aquellas entidades que hubieran decidido voluntariamente someterse a ellos. En ningún caso los propios poderes públicos estadounidenses habían optado por la sumisión a dichos principios, y aún el problema se intensifica si tenemos en cuenta que no se habían articulado procedimientos legislativos efectivos que garantizasen su cumplimiento[600].

A este respecto, el propio texto de la Sentencia, en su apartado 81, afirma que: "[a]unque el recurso por un tercer país a un sistema de autocertificación no es por sí mismo contrario a la exigencia enunciada en el artículo 25, apartado 6, de la Directiva 95/46 de que el tercer país considerado garantice un nivel de protección adecuado «a la vista de su legislación interna o de sus compromisos internacionales», la fiabilidad de ese sistema en relación con dicha exigencia descansa, en esencia, en el establecimiento de mecanismos eficaces de detección y de control que permitan identificar y sancionar en la práctica las posibles infracciones de las reglas que garantizan la protección de los derechos fundamentales, en especial del derecho al respeto de la vida privada y del derecho a la protección de los datos personales".

En segunda instancia, conviene señalar que, según el Tribunal de Justicia de la Unión Europea, la Decisión de la Comisión, de fecha 26 de julio de 2000, propugna la primacía de determinados aspectos consagrados por el ordenamiento jurídico de Estados Unidos, tales como las "exigencias de seguridad nacional, interés público y el cumplimiento de la ley estadounidense"[601] sobre los principios reflejados en el Acuerdo de Puerto Seguro. Ello produce una injerencia directa en el derecho fundamental a la protección de los datos personales por la inobservancia de las debidas garantías[602], tal y

[599] *Ibidem*, apdos. 63-65.

[600] *Ibidem*, apdos. 82-83.

[601] *Ibidem*, apdo. 75.

[602] *Ibidem*, apdo. 81, 90-91.

como había quedado evidenciado a través del análisis efectuado por la Comisión sobre la aplicación de las disposiciones contenidas en el susodicho marco normativo[603].

En este mismo sentido, la protección del derecho fundamental a la privacidad y la intimidad, y por ende, a los datos de carácter personal, únicamente puede soportar excepciones cuando estas no excedan de lo estrictamente necesario, por lo que la Sentencia recuerda que: "No se limita a lo estrictamente necesario una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización […]. En particular, se debe considerar que una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta"[604].

Ante esta tesitura, el Tribunal concluye que las instituciones comunitarias con competencias sobre la materia —especialmente, la Comisión Europea— no efectuaron las comprobaciones necesarias que hubieran permitido determinar con exactitud que los Estados Unidos de América no gozaban de un nivel de protección adecuado para ser el destinatario de los datos personales de ciudadanos de la Unión[605]. Máxime si tenemos en cuenta que, además de dotar de mecanismos de tutela ineficaces para los afectados[606], se

---

603 *Vid*. COMISIÓN EUROPEA, "Comunicación al Parlamento… (COM [2013] 847 final)", cit., p. 19.

604 *Vid*. STJUE. Asunto C-362/14 (Schrems I), cit., apdos. 93-94.

605 A este respecto, resulta oportuno traer a colación las contundentes manifestaciones efectuadas por parte del abogado general Yves Bot en sus conclusiones, cuando afirma inicialmente en el apartado 234 que: "[S]i bien tenía conocimiento de la existencia de disfunciones en la aplicación de la Decisión 2000/520, la Comisión ni la suspendió ni la adaptó, lo que dio lugar a la violación continuada de los derechos fundamentales de las personas cuyos datos de carácter personal fueron y siguen siendo transferidos en el marco del régimen de puerto seguro". Y, posteriormente, en el apartado 236: "[T]al inacción de la Comisión, que atenta directamente contra los derechos fundamentales protegidos por los artículos 7, 8 y 47 de la Carta, constituye, a mi parecer, un motivo complementario para declarar inválida la Decisión 2000/520 en el marco de la presente remisión prejudicial". *Vid*. Conclusiones del abogado general Yves Bot en el asunto C-362/14 (Schrems I), presentadas el 23 de septiembre de 2015. Consultado el 20.08.2017 desde: http://curia.europa.eu/juris/document/document.jsf?docid=168421&doclang=ES.

606 *Vid*. STJUE. Asunto C-362/14 (Schrems I), cit., apdos. 95-96.

optó por dificultar el ejercicio de ciertas facultades a las autoridades nacionales de los Estados miembros, imposibilitando el cumplimiento de las vicisitudes contenidas en el artículo 25.6 de la Directiva 95/46/CE[607], comportando en definitiva la invalidez del Acuerdo de Puerto Seguro remarcado *ut supra*[608].

A modo de conclusión, resulta oportuno traer a colación las palabras de Uría Gavilán cuando indica que resulta sorprendente que en un caso de relevancia como el que se está analizando, en el que los derechos fundamentales juegan un papel transcendental en toda la interpretación efectuada por el Tribunal, no se cite en ningún momento el Convenio Europeo de Derechos Humanos, así como tampoco la jurisprudencia imperante al respecto por parte del Tribunal de Estrasburgo. Confirmándose así la tendencia de la que alerta cierto sector doctrinal[609] sobre la "autonomización" del TJUE respecto del Tribunal Europeo de Derechos Humanos, propiciado por la entrada en vigor del Tratado de Lisboa en 2009, momento en que la Carta comenzó a ser jurídicamente vinculante[610].

3.3. Implicaciones de la Sentencia "Schrems I" para las transferencias internacionales de datos personales a los Estados Unidos de América

El contexto propiciado y la inseguridad jurídica[611] generada por la invalidez de la Decisión de la Comisión, que hasta la fecha había posibilitado las transferencias internacionales de datos desde la Unión Europea a Estados Unidos, forzó que el Grupo

607 *Ibidem*, apdos. 99-104.

608 *Ibidem*, apdos. 97-98.

609 *Vid*., entre otros: CALLEWAERT, J., "To accede or not to accede: European protection of fundamental rights at the crossroads", en *Journal européen des droits de l'homme*, Vol. 2014, nº 4 (2014), pp. 500-510; DE BURCA, G., "After the EU Charter of Fundamental Rights: the Court of Justice as a Human Rights Adjudicator?", en *Maastricht Journal of European and Comparative Law*, Vol. 20, nº 2 (2013), p. 174.

610 *Vid*. URÍA GAVILÁN, E., "Derechos fundamentales…", *op. cit*., pp. 277-278; ŠKRINJAR, M., "Schrems v. Data Protection Commissioner (Case C-362/14): Empowering National Data Protection Authorities", en *Croatian Yearbook of European Law and Policy*, nº 11 (2015), p. 265.

611 Como señala DAVARA RODRÍGUEZ: "[I]nmediatamente se crea una inseguridad jurídica que hace que los órganos de control de los diferentes Estados (en España, la Agencia Española de Protección de Datos) muevan ficha ante la avalancha de consultas que realizan los responsables de ficheros y tratamientos en protección de datos y los propios interesados sobre la legalidad de las transferencias que están realizando y que, hasta el momento, tenían su soporte jurídico en la referida Decisión 2000/520 que acababa de anular el TJUE". *Cfr*. DAVARA RODRÍGUEZ, A., "El escudo de privacidad", en *El Consultor de los Ayuntamientos*, nº 19 (2016), Madrid: Wolters Kluwer, 2016, p. 7.

de Trabajo del Artículo 29 se viera obligado a pronunciarse desde un primer momento[612]. El referido organismo puso de manifiesto, por un lado, la necesidad de realizar un llamamiento, en primer término, a los Estados miembros y a sus respectivas autoridades nacionales de protección de datos para que encontraran una posición unánime en la aplicación de la Sentencia "Schrems I"[613]. Y, por otro lado, a las autoridades comunitarias para que retomaran las negociaciones con las autoridades estadounidenses, en aras de encontrar una alternativa que permitiera seguir operando con los flujos de datos personales transfronterizos, pero esta vez con la adopción de mecanismos claros y vinculantes que asegurasen la salvaguarda de los derechos y libertades de los afectados respecto de sus datos de carácter personal.

Adicionalmente, el GT29 también aprovechó la ocasión para hacer hincapié en la necesidad de encontrar soluciones alternativas factibles para realizar los movimientos transatlánticos de datos personales a los Estados Unidos, pues el marco jurídico que las sustentaba hasta la fecha había sido declarado inválido. Ello comportó que algunas autoridades de control, como sucedió en España, a través de la Agencia Española de Protección de Datos, indicasen que no se llevarían a cabo actuaciones inspectoras y sancionadoras en este sentido[614]. Se optó por recomendar que se adoptaran los mecanismos alternativos previstos para seguir con la operativa de negocio que hasta la fecha se venía efectuando, tales como las Cláusulas Contractuales Tipo adoptadas por la Comisión Europea, las Normas Corporativas Vinculantes o, en su defecto, optar puntualmente a que la transferencia en cuestión se ajustase a alguna de las excepciones

---

612 *Vid*. COMISIÓN EUROPEA. Declaración del GT29, de fecha 16 de octubre de 2015, relativa a las implicaciones de la Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 6 de octubre de 2015, en el asunto C- 362/14, reseñada con anterioridad. Consultado el 24.08.2017 desde: http://ec.europa.eu/justice/data-protection/article-29/press-material/pressrelease/art29press_material/2015/20151016_wp29_statement_o n_schrems_judgement.pdf.

613 A este respecto, resulta recomendable consultar la nota de prensa publicada en la página web oficial de la Agencia Española de Protección de Datos, en fecha 19 de octubre de 2015, donde se anuncia que: "Las Autoridades europeas de Protección de Datos publican una declaración conjunta en relación con la aplicación de la sentencia del TJUE sobre el Puerto Seguro". Consultado el 24.08.2017 desde: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas_prensa/news/2015_10_19-ides-idphp.php#Actuaci%C3%B3n%20conjunta.

614 *Vid*. En este punto, resulta oportuno citar la necesidad de revisar la comunicación efectuada por parte de la Agencia Española de Protección de Datos a los responsables, publicada a través de su página web, en fecha 29 de octubre de 2015. Consultado el 24.08.2017 desde: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/Comunicacion_responsables_-_Puerto_Seguro.pdf.

contenidas en el artículo 26.1 de la Directiva 95/46/CE —o, en el caso español, recogidas en el artículo 34 de la LOPD—.

Con posterioridad a las declaraciones efectuadas por parte del GT29, la Comisión Europea también reaccionó ante la situación generada por la Sentencia del TJUE en el mismo sentido, pero con mayor especificidad[615], pues realizó una exposición sobre las distintas alternativas que existían para articular las transferencias internacionales de datos a los Estados Unidos, animado a que los responsables del tratamiento apostaran por las mismas, colaborando estrechamente con sus respectivas autoridades de control nacionales. Aprovechó la ocasión también para reiterar los esfuerzos que venía efectuando desde 2013 respecto de las negociaciones existentes con los EE. UU., encaminadas a encontrar un nuevo régimen para regular los movimientos de datos personales transfronterizos entre los dos territorios, respecto del cual se habían alcanzado supuestas mejoras basadas en las trece recomendaciones que se han analizado con anterioridad.

[615] *Vid*. COMISIÓN EUROPEA, "Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre la transferencia de datos personales de la UE a los Estados Unidos de América con arreglo a la Directiva 95/46/CE de forma consiguiente a la sentencia del Tribunal de Justicia en el asunto C-362/14 (Schrems I)", de fecha 6 de noviembre de 2015 (COM [2015] 566 final). Consultado el 24.08.2017 desde: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52015DC0566&from=EN.

4. Nuevo paradigma para las transferencias internacionales de datos a Estados Unidos. El novedoso "*EU–U.S. Privacy Shield framework*"

4.1. Antecedentes

Tras más de dos años de intensas negociaciones entre las autoridades europeas y norteamericanas, a principios de 2016, concretamente el 2 de febrero de ese mismo año, se alcanzó un acuerdo político entre la Comisión Europea y el Departamento de Comercio de los Estados Unidos que debía de convertirse en el nuevo marco regulador de las transferencias internacionales de datos personales entre ambos territorios. Asimismo, el 29 de febrero, se hizo público el nuevo proyecto de decisión que fue acuñado, bajo la denominación *"EU–U.S. Privacy Shield framework"* —cuyo contenido incluía siete anexos, con los principios sobre los que se sustentaba, así como numerosas declaraciones de compromiso efectuadas por parte de organismos del gobierno estadounidense—.

Con posterioridad, entre los meses de marzo y julio de 2016, se dio traslado del texto a las instituciones europeas con competencias sobre la materia para que evaluaran su contenido y realizaran las apreciaciones que considerasen oportunas. En concreto, el GT29[616], el Parlamento Europeo[617] y el Supervisor Europeo de Protección de Datos (en adelante, SEPD)[618] realizaron una serie de pronunciamientos que se examinarán. La totalidad de los organismos coincidieron en manifestar que se habían introducido diversas mejoras, las cuales posibilitaron que de manera prudencial se avalara el contenido del texto propuesto, que sería formalmente adoptado en fecha 16 julio de ese mismo año, a través de la Decisión de Ejecución (UE) nº 2016/1250, emitida por parte de la Comisión Europea.

En primer lugar, respecto a los pronunciamientos efectuados por parte del GT29, cabe reseñar uno inicial efectuado el 13 abril de 2016, en el que a pesar de reconocer la

---

[616] *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 238): Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision", aprobado por el Grupo de Trabajo el 13 de abril de 2016, pp. 7-8. Consultado el 24.08.2017 desde: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

[617] *Vid*. Resolución del Parlamento Europeo nº 2016/2727(RSP), de 26 de mayo de 2016, sobre los flujos transatlánticos de datos. Consultado el 24.08.2017 desde: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52016IP0233.

[618] *Vid*. SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, "Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision", de fecha 30 de mayo de 2016. Consultado el 24.08.2017 desde: https://SEPD.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf.

introducción de una serie de mejoras para la protección de los derechos y libertades de los afectados respecto de lo preceptuado por el acuerdo predecesor, manifestaba la necesidad de seguir mejorando sobre el régimen de garantías previstas para efectuar transferencias internacionales de datos a Estados Unidos, por resultar aun manifiestamente insuficiente. Por un lado, se indicaba la necesidad de introducir aclaraciones sobre el principio de limitación en la conservación de los datos personales recabados, así como la obligación de evaluar si la legislación nacional de un tercer país resulta suficiente bajo el principio de ulterior transferencia y la dificultad de garantizar la tutela judicial efectiva de los afectados mediante el complejo sistema de recursos previsto[619].

Por otro lado, el GT29 expresó cuatro garantías esenciales a las que se deberían dar cumplimiento en cualquier supuesto —en base a la jurisprudencia del TJUE y del TEDH—, las cuales pueden detallarse brevemente en que: (i) el tratamiento de los datos personales se sustentará bajo los principios de claridad, precisión y accesibilidad; (ii) se respetarán los principios de necesidad y proporcionalidad cuando se accediera a datos personales; (iii) resultará necesario preservar la existencia de mecanismos de supervisión independientes; y, (iv) se facilitarán a los interesados mecanismos que ofrezcan una correcta tutela de sus derechos y libertades[620].

En conclusión, como indica Davara Rodriguez, "el GT29 destaca las grandes mejoras que ofrece el Escudo de Privacidad comparado con la decisión de Puerto Seguro invalidada. Dadas las preocupaciones expresadas y las aclaraciones pedidas, el GT29 urge a la Comisión a despejar estas preocupaciones, señalar las soluciones adecuadas y proporcionar las aclaraciones solicitadas para mejorar la propuesta de decisión de adecuación y garantizar que la protección ofrecida por el Escudo de Privacidad sea esencialmente equivalente a la ofrecida por la UE"[621].

En segundo lugar, cabe mencionar el pronunciamiento llevado a cabo por parte del Parlamento Europeo, que, siguiendo el modelo instaurado por parte del GT29, agradece el esfuerzo llevado a cabo por las partes implicadas durante todo el proceso de

---

[619] *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 27): Opinion 01/2016…", cit., pp. 15-33.

[620] *Ibidem*, pp. 33-51.

[621] *Cfr*. DAVARA RODRÍGUEZ, A., "El escudo de…", *op. cit.*, p. 5.

negociación del Acuerdo. Pero sigue insistiendo en la necesidad de dotar de seguridad jurídica suficiente al régimen de transferencias de datos personales que se articule entre la Unión y EE. UU., por lo que solicita a la Comisión que aplique en su completitud las recomendaciones que había efectuado con anterioridad el GT29, así como que se comprometiera bajo su responsabilidad a revisar de manera sólida y periódica el cumplimiento de la aplicación del contenido previsto en la Decisión de Ejecución (UE) nº 2016/1250[622].

En tercer lugar, resulta preciso mencionar las aseveraciones que sobre esta cuestión realizaba el SEPD, que siguiendo el hilo de agradecimientos efectuado por sus predecesores —esto es, el GT29 y el propio Parlamento Europeo—, en relación con las implicaciones de las instituciones comunitarias y norteamericanas, destaca especialmente la relevancia del compromiso adoptado por primera vez por parte del Departamento de Justicia, del Departamento de Estado y de la Oficina del Director de Inteligencia Nacional durante las negociaciones sucedidas.

Sin embargo, el SEPD seguía manifestando que el proceso resultante no era suficiente en sí mismo, pues la necesidad temporal de encontrar un nuevo marco jurídico no puede ir en detrimento de poner en jaque los derechos y libertades de los afectados, dado que el acuerdo resultante debería tener vocación de permanencia de futuro[623]. Sobre todo, este organismo hacía hincapié en la necesidad de regular las prácticas llevadas a cabo por los servicios de inteligencia, alentando a la Comisión a velar por que esta tipología de actividades se realizase con estricto cumplimiento de las vicisitudes contenidas en la legislación europea que regulaba la materia[624], a pesar de que las

---

[622] *Vid*. "Resolución del Parlamento… (2016/2727[RSP])", cit., apdos. 10-13.

[623] A este respecto, el SEPD manifiesta el tenor literal siguiente: "[…] Acogería con agrado una solución general para las transmisiones de datos de la UE a los EE. UU., una solución que debería ser suficientemente sólida e integral. Esto requiere la introducción de importantes mejoras para garantizar que, a largo plazo, se respeten nuestros derechos y libertades fundamentales. Una vez adoptada y tras la primera evaluación de la Comisión Europea, la Comisión deberá ser revisada oportunamente con el fin de identificar las medidas pertinentes para alcanzar soluciones a más largo plazo y sustituir el escudo protector de la intimidad por un marco jurídico más estable y robusto que impulse las relaciones transatlánticas". *Vid*. SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, "Resumen ejecutivo del dictamen sobre el proyecto de decisión relativo a la adecuación del escudo protector de la intimidad entre la UE y los EE. UU (2016/C 257/05)", de fecha 15 de julio de 2016, p. 3.

[624] Respecto a la necesidad de que la Comisión Europea adopte una postura de mayor rigor, el SEPD señala que: "[…] Alienta a la Comisión Europea a enviar una señal más firme: dadas las obligaciones que emanan del Tratado de Lisboa para la UE, las autoridades públicas únicamente deberían poder acceder a los datos

autoridades gubernamentales norteamericanas habían expresado su compromiso de reducir esta tipología de actuaciones.

Como cuestión final, el SEPD abogaba también por reforzar los mismos puntos que había indicado con anterioridad el GT29, pero adicionalmente enfatizaba específicamente sobre la necesidad de reforzar los mecanismos de tutela para los afectados —sobre todo en lo relativo a la figura del Defensor del Pueblo—. En el contexto de la vocación de permanencia que se ha apuntado en el párrafo anterior, debía entenderse incluida la adecuación del contenido del nuevo Acuerdo a los requerimientos que vendría a desplegar el RGPD en el momento de su aplicación efectiva —que se produciría el 25 de mayo de 2018—[625].

Finalmente, en fecha, 12 de julio de 2016, la Comisión Europea, mediante nota de prensa[626], hizo pública la adopción del Acuerdo sobre el Escudo de Privacidad UE-EE. UU., constituyendo el nuevo marco normativo para las transferencias internacionales de datos personales de ciudadanos entre los distintos territorios. Con posterioridad, en fecha 26 de julio de 2016, el GT29 emitió una declaración[627] sobre la Decisión de Ejecución (UE) nº 2016/1250 elogiando a la Comisión y a las autoridades estadounidenses por reflejar en el texto definitivo las consideraciones que había trasladado con anterioridad durante el periodo de consulta del texto. Sin perjuicio de ello, el referido grupo de expertos seguía señalando ciertos defectos que no se habían solventado, centrados básicamente en la ausencia de normas específicas en relación con las decisiones automatizadas —respecto a las cuales el RGPD había realizado especial énfasis en su regulación—, la inexistencia de un derecho general de oposición y la insuficiencia de garantías de independencia y potestades sobre la figura del Defensor del Pueblo (*Ombudsperson*).

---

transmitidos con fines comerciales y utilizarlos, incluso durante su tránsito, con carácter excepcional y solo cuando sea indispensable por motivos específicos relacionados con el interés público". *Ibidem.*

625 *Vid*. SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, "Opinion 4/2016…", cit., pp. 9-12.

626 *Vid*. Nota de prensa efectuada por la Comisión Europea sobre la adopción del Acuerdo sobre Escudo de Privacidad UE-EE. UU., en fecha 12 de julio 2016. Consultado el 24.08.2017 desde: http://europa.eu/rapid/press-release_IP-16-2461_es.htm.

627 *Vid*. Declaración del GT29 sobre sobre la decisión de la Comisión Europea sobre Escudo de privacidad UE-EE. UU, efectuada en fecha 26 de julio de 2016. Consultado el 24.08.2017 desde: http://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf.

4.2. Contenido

El objetivo que centró las negociaciones de la Decisión de Ejecución (UE), nº 2016/1250, de la Comisión recayó en la subsanación de los defectos que se habían puesto de manifiesto por parte del TJUE respecto del anterior Acuerdo de Puerto Seguro, por lo que supuestamente se partía de una nueva concepción para su construcción. En aras de fortalecer los derechos fundamentales de los ciudadanos de la Unión Europea, se articularon una serie de novedades que ponían su foco de atención en su ámbito de aplicación, pues aparte de regular los propios flujos de información que se sucediesen entre los destinitos territorios, el texto también se preocupaba de delimitar las competencias de las autoridades gubernamentales de los EE. UU. —aunque en la práctica, eso no implicara que siguiera prevaleciendo la legislación estadounidense frente a la comunitaria—[628].

En este sentido, su contenido y estructura se componía inicialmente por ciento cincuenta y cinco considerandos, seguidos por seis artículos que intentaban plasmar el calado jurídico de la norma. En los mismos se admitía que el territorio norteamericano garantizaba un nivel de protección adecuado respecto de los datos personales de los ciudadanos europeos que les fuesen transferidos bajo el acervo del Acuerdo. Todo ello sin perjuicio de que pudieran detectarse defectos por parte de las autoridades de control nacionales de los EE.MM. que aconsejasen una reevaluación de las consideraciones aducidas en el contenido de la Decisión.

Como indica Pérez Cambero, la Decisión "instaura el deber de realizar un seguimiento continuo del funcionamiento del Escudo de la privacidad y de la obligación de los Estados miembros de la Unión Europea y la Comisión de informarse recíprocamente de incumplimientos por parte de los organismos públicos de los Estados Unidos que afecten a los principios del Escudo, así como los compromisos y declaraciones oficiales. Recoge también la revisión anual que se realizará sobre el cumplimiento del Escudo de la privacidad y enumera los supuestos en los que la Comisión podrá incoar un procedimiento de suspensión o derogación de la Decisión 2016/1250"[629].

---

[628] *Vid*. SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, "Opinion 4/2016…", cit., p. 20.

[629] *Cfr*. PÉREZ CAMBERO, R., "Aspectos más destacables de la Decisión de Ejecución 2016/1250 de la Comisión Europea, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU.", en *Actualidad Administrativa*, nº 4 (2017), Wolters Kluwer, p. 19.

Para, finalmente, en el último tramo de la Norma, incorporar una serie de Anexos, que llegan hasta el número séptimo y que tienen como principal objetivo intentar arrojar luz y facilitar la aplicabilidad práctica del texto que compone la Decisión. En suma, y siguiendo con los precedentes sentados por el anterior Acuerdo, el marco normativo sobre el Escudo de Privacidad partía también de un mecanismo de autocertificación que debía notificarse ante el Departamento de Comercio de los Estados Unidos mediante la adhesión al cumplimiento de una serie de principios que vinían consagrados en el Anexo II de la Decisión. Estos se estructuraban, a grandes rasgos, en siete principios generales y dieciséis que tenían carácter complementario[630].

En primer lugar, se encontraba el principio de notificación, que requería que las organizaciones estadounidenses que se adhiriesen al nuevo marco normativo proporcionasen información más específica en sus respectivas políticas de privacidad. En la práctica[631], ello ya venía sucediendo con el anterior Acuerdo de Puerto Seguro, pero a muy alto nivel. En este caso, se había optado por detallar específicamente los requisitos que esa concreta política debería de cumplir, introduciendo novedades tales como la necesidad de incluir un enlace electrónico al formulario de presentación de quejas y reclamaciones para la resolución extrajudicial de controversias, así como la obligatoriedad de reconocer la responsabilidad en los supuestos de transferencias ulteriores a terceros[632].

En segundo lugar, el principio de opción no introducía novedades significativas respecto de lo que se venía manteniendo en el anterior texto de la Comisión, que venía a ofrecer a los interesados la posibilidad de decidir si sus datos personales podían ser cedidos a terceros o, en su caso, ser utilizados para finalidades distintas a las que originaron su recogida[633]. Resulta importante destacar la introducción de una excepción

[630] *Vid*. Decisión de Ejecución (UE) nº 2016/1250 de la Comisión, cit., apdo. 14.

[631] En relación con lo anterior, desde un punto de vista práctico, sería conveniente advertir que puede resultar contraproducente incurrir por el contrario en un exceso de detalle, dado que ello podría entrar en conflicto con los principios generales por los que aboga el propio texto de la Decisión, centrados en la utilización de un lenguaje sencillo, claro y visible. Es por ello que las organizaciones, en el momento que opten por su redacción, deberán tener en cuenta estas consideraciones, para no entrar en colisión con otros puntos esenciales del texto objeto de comentario.

[632] *Vid*. Apartado segundo del Anexo II de la Decisión de Ejecución (UE) nº 2016/1250 de la Comisión, cit.

[633] A este respecto, como indica Álvarez Hernando parafraseando a la Comisión, por ejemplo, si la empresa para la que trabaja una persona ha transferido sus datos a los EE. UU. para su tratamiento, la empresa de

ante el cumplimiento de este principio general, que radicaba en que cuando ese tercero actuase como agente —es decir, bajo la condición de encargado del tratamiento—, no sería preciso ofrecer a los interesados ese derecho de opción. Sin embargo, la organización quedaba obligada a suscribir un contrato con ese tercero, en el que se delimitasen las instrucciones que le trasladaría al respecto como responsable del tratamiento[634].

En tercer lugar, cabe identificar el denominado principio de responsabilidad por una transferencia ulterior que, pese a estar previsto en el Acuerdo de Puerto Seguro, incorporaba nuevas obligaciones para las organizaciones en detrimento de lo que establecía su predecesor. Su contenido se centraba en la protección de cualquier transferencia o comunicación de datos personales que se efectuase con posterioridad a la recogida de los datos personales a otro responsable o encargado del tratamiento. Únicamente se contemplaba como alternativa si mediaba la existencia de un vínculo contractual previo que estipulase expresamente el cumplimiento de todos los principios reflejados en el marco normativo sobre el Escudo de Privacidad, especialmente el de proporcionar un nivel de protección adecuado[635].

La obligación contractual a la que se refiere este principio toma su inspiración de las diversas obligaciones estipuladas en el RGPD respecto a la necesidad de garantizar la protección adecuada de los datos personales durante todo el ciclo de vida que pueda durar su gestión. El responsable del tratamiento debía mantener un deber de diligencia en la elección de su encargado del tratamiento, con la intención de que éste último ofreciera garantías suficientes respecto de la implementación y el mantenimiento de las medidas técnicas y organizativas apropiadas, así como la correcta tutela de los derechos de los interesados[636].

---

los EE. UU. podrá ser autorizada para utilizar esos datos con el fin de ofrecer al afectado una póliza de seguros o un plan de pensiones, siempre que el interesado no se oponga a dicho tratamiento. Por el contrario, no podrá ceder o comunicar los datos a terceros que le ofrezcan bienes o servicios carentes de relación con dicho empleo. *Cfr*. ÁLVAREZ HERNANDO, J., *Prácticum Protección de Datos 2018*, Navarra: Ed. Aranzadi, 2017.

634 *Vid*. Apartado segundo del Anexo II de la Decisión de Ejecución (UE) nº 2016/1250 de la Comisión, cit.

635 *Ibidem.*

636 En particular, el Considerando 81 del RGPD señala al respecto el siguiente tenor literal: "[e]l tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable, que fije el objeto y la duración del

En cuarto lugar, se establecía el principio de seguridad, que mantenía el mismo redactado que el introducido en el anterior Acuerdo de Puerto Seguro, abogando por que las organizaciones que se encargaban de la recogida de datos de carácter personal aplicasen todas las precauciones necesarias que permitiesen evitar su pérdida, uso indebido, acceso no autorizado, divulgación, alteración o destrucción. Sin embargo, resulta sorprendente que se optara por un redactado tan amplio en comparación con los restantes principios que se han examinado a lo largo de los anteriores párrafos, caracterizados particularmente por la especificación y exactitud de las obligaciones que en los mismos se contempla[637].

Puede compararse este punto con la mención que se contiene al respecto en el RGPD, cuando el mismo se hace eco de las medidas técnicas y organizativas que se deberán implementar para la correcta protección y salvaguarda de los datos personales de los afectados, en que casi reproduciendo el mismo tenor literal enuncia idénticas obligaciones, pero con un nuevo enfoque respecto del que veníamos acostumbrados —sobre todo en España, donde existía un catálogo cerrado de medidas de seguridad a aplicar por parte de los responsables y/o encargados del tratamiento—. El mismo pone énfasis en la realización de una evaluación de riesgos que, una vez concluida, debería permitir determinar con exactitud los riesgos a los que estarían expuestos unos determinados datos personales para poder implementar así las medidas de seguridad que puedan resultar de aplicación y trazar un plan de acción al respecto, primando por una gestión continua del riesgo.

En quinto lugar, se identificaba el principio de integridad de los datos y la limitación de la finalidad para la que habían sido obtenidos, que mantenía las mismas obligaciones que el ya reiterado Acuerdo de Puerto Seguro. Hacía hincapié en la necesidad de que las organizaciones que se adhiriesen al nuevo marco normativo debían adoptar medidas razonables que asegurasen la utilización de los datos personales de

tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado. El responsable y el encargado pueden optar por basarse en un contrato individual o en cláusulas contractuales tipo que adopte directamente la Comisión o que primero adopte una autoridad de control de conformidad con el mecanismo de coherencia y posteriormente la Comisión. Una vez finalizado el tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos".

[637] *Vid*. Apartado segundo del Anexo II de la Decisión de Ejecución (UE) nº 2016/1250 de la Comisión, cit.

conformidad con las finalidades para las que fueron recabados, es decir, su tratamiento debía ser pertinente para el uso previsto y la información debía ser precisa, completa y actualizada durante el período que comprendiese su conservación[638].

A este respecto, se añadía explícitamente que cualquier organización que tuviera acceso a estos datos personales debía adherirse al cumplimiento de los principios reflejados en el Acuerdo sobre el Escudo de Privacidad, independientemente de que, una vez que dejase de intervenir en su tratamiento, decidiese retirarse del mismo. Ello va en consonancia con el espíritu de redacción del texto de la Decisión, que abogaba por la protección de los datos de carácter personal durante todo el ciclo de su gestión, en especial, cuando los mismos eran destinados a terceros. Ello obedecía a las reiteradas quejas que se habían sucedido tradicionalmente sobre la cuestión y que también el RGPD tomaba especialmente en consideración.

En sexto lugar, se apreciaba el principio de acceso, cuyo contenido era similar al que había sido objeto de introducción en la anterior Decisión de la Comisión. En concreto, se establecía al respecto el siguiente tenor literal: "[l]os particulares deberán tener acceso a la información personal que las entidades tengan sobre ellos y poder corregir, modificar o suprimir dicha información si resultase inexacta, o haya sido tratada infringiendo los principios, excepto en dos casos: cuando permitir el acceso suponga una carga o dispendio desproporcionado en relación con los riesgos que el asunto en cuestión conlleve para la vida privada de la persona, o cuando puedan vulnerarse los derechos de otras personas"[639].

A este respecto, no resultaba preciso que el afectado justificase los motivos que le llevaban a ejercer sus correspondientes derechos sobre los datos personales que le concernían, salvo en aquellos casos donde la petición en cuestión careciese de precisión o resultase demasiado genérica. Hay que tener en cuenta que, como principio general, el responsable del tratamiento que fuera destinatario de la petición debía atender las peticiones que le fuesen dirigidas de manera correcta y siempre dentro de un plazo razonable.

Y, por último, en séptimo lugar, cabe apuntar la existencia del principio de recurso, aplicación y responsabilidad, cuyo ámbito de aplicación se había visto ampliado

[638] *Ibidem.*

[639] *Ibidem.*

significativamente respecto de lo establecido con anterioridad por el Acuerdo de Puerto Seguro. Dicho principio se encargaba de preceptuar para las organizaciones adheridas la obligatoriedad de implementar mecanismos para los interesados que garantizasen la correcta y efectiva tutela de los derechos y libertades que se les reconocía en el ámbito legislativo comunitario.

Para ello, se optó por articular una multiplicidad de procedimientos, tales como: (i) la asunción de responsabilidad por la propia organización afectada y adherida al Acuerdo, que debía responder la reclamación correspondiente en un plazo máximo de 45 días, así como en su caso, dar cumplimiento al mandato establecido por la autoridad de control competente del Estado miembro donde residiera el afectado; (ii) la posibilidad de presentación de quejas y reclamaciones ante las propias autoridades nacionales de protección de datos de los Estados miembros donde los interesados residieran, pues serían éstas las que a su vez darían traslado al Departamento de Comercio estadounidense (mediante las distintas instituciones designadas a tal efecto, a priori, ello se realizaría a través de la *Federal Trade Comission*, debido a que era la principal autoridad encargada de colaborar en la investigación y resolución de las quejas o reclamaciones que pudiesen interponerse por parte de los ciudadanos europeos; (iii) la opción de acudir a un sistema extrajudicial de resolución de litigios, que debía ostentar carácter gratuito; y (iv) con carácter subsidiario, en el supuesto de que no se hubiera resuelto la controversia por ninguna de las anteriores vías, se dejaba abierta la posibilidad de acudir ante un procedimiento arbitral[640].

En este contexto, cabe reconocer que el nuevo marco normativo parecía comportar un avance en detrimento de los efectos desplegados por su predecesor, aunque seguía careciendo de aquellos elementos indispensables que equipararían su protección a la que realizaba la legislación comunitaria —aunque se partía de ordenamientos jurídicos antagónicamente diferentes—. Es por ello que, a grandes rasgos, podría alabarse su positividad, puesto que pretendía poner fin a gran parte de la situación de inseguridad jurídica que se había venido sucediendo hasta su entrada en vigor y que perjudicaba tanto a las organizaciones como a los propios interesados. Pero cabía recordar en todo momento que el mismo venía siguiendo el mismo modelo deficiente que el utilizado por parte del Acuerdo de Puerto Seguro.

[640] *Ibidem.*

Otra de las novedades importantes que traía consigo el nuevo Acuerdo radicaba en la figura del Defensor del Pueblo, que venía a preceptuarse como uno de los recursos puestos a disposición de los ciudadanos europeos afectados por la recogida de sus datos personales para que pudieran tutelar sus respectivos derechos[641]. Esta figura también fue objeto de comentario por parte del GT29, manifestando al respecto que, aunque podía constituir una medida significante de mejora para la tutela de los derechos de los interesados, existía una preocupación razonable por el hecho de que el órgano gozase de la independencia suficiente y de las competencias necesarias que le permitiesen desarrollar las funciones que tenía encomendadas de manera efectiva[642].

Como última cuestión a indicar, debe recordarse que, con carácter adicional, la Decisión incorpora siete anexos que recogen las consideraciones y los compromisos adoptados por parte de las autoridades norteamericanas respecto de las garantías existentes en su respectivo ordenamiento jurídico para todos aquellos individuos que no ostentasen la nacionalidad estadounidense. El Anexo I incorporaba una Carta de la Secretaria de Comercio estadounidense, Penny Pritzker, dirigida a la Comisión Europea en la que se detallaban los compromisos adoptados por parte del Departamento de Comercio para garantizar el cumplimiento de las disposiciones previstas en el Acuerdo sobre el Escudo de Privacidad, con mención específica sobre el nuevo modelo de arbitraje establecido. El Anexo II, cuyo contenido se ha tenido la oportunidad de analizar con anterioridad, incorporaba el listado de principios a los que debían adherirse las empresas norteamericanas que pretendiesen operar bajo el acervo de la Decisión.

El Anexo III se circunscribe a una carta del Departamento de Estado en la que se asumían una serie de compromisos en relación con la figura del Defensor del Pueblo que hemos tenido la oportunidad abordar. En el mismo sentido, el Anexo IV se trata de otra carta de la FTC, en la que, como indica Pérez Cambero, se describen los compromisos de este organismo en torno al cumplimiento de las vicisitudes de la Decisión en cuatro áreas clave: (i) priorización de las remisiones e investigaciones; (ii) tratamiento de las declaraciones falsas o fraudulentas de adhesión al Escudo de la privacidad; (iii)

[641] Todo ello, debería de ser interpretado en su conjunto, a través de los restantes principios complementarios y preguntas frecuentes que formaban parte del Anexo II de la Decisión de ejecución (UE) nº 2016/1250, y que tenían como objetivo principal intentar ayudar y orientar la aplicación de los principios generales enumerados con anterioridad.

[642] *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 27): Opinion 01/2016…", cit., p. 4.

supervisión continua de las órdenes; y, (iv) mayor compromiso y colaboración en lo que respecta a la ejecución, con las autoridades de protección de datos de la Unión Europea.[643]

Los restantes documentos, esto es el Anexo V, VI y VII, se componen también de tres cartas del Departamento de Transporte, de la Oficina del Director de Inteligencia Nacional y del Departamento de Justicia, respectivamente. En la primera de ellas se asumen una serie de compromisos en relación con el cumplimiento del Acuerdo[644]. Posteriormente, en las dos restantes se suministra información a las instituciones comunitarias sobre el funcionamiento de las actividades realizadas por parte de las agencias de inteligencia de los EE. UU., así como sobre ciertas cuestiones sobre el acceso de las autoridades gubernamentales del país a la información necesaria para garantizar el cumplimiento de la legislación aplicable y garantizar la protección de la seguridad nacional.

4.3. Cuestiones prácticas sucedidas durante su vigencia

Una vez llegados a este punto, en que se han abordado las principales cuestiones que se enmarcan en el contenido del Acuerdo sobre el Escudo de Privacidad, cabe analizar la efectividad de su posterior aplicación práctica. Su herencia histórica ha venido marcada por una serie de deficiencias respecto de la tutela de los derechos fundamentales vinculados a la protección de los datos personales, que fueron nuevamente reseñadas en 2015 por parte del Tribunal de Justicia de la Unión Europea en la invalidación del Acuerdo de Puerto Seguro. Posteriormente, las mismas se intentarían paliar sin éxito con la elaboración de un nuevo marco normativo que tampoco cumpliría con las expectativas que inicialmente en él se habían depositado.

Para observar sus implicaciones prácticas, en primera instancia, resulta oportuno detenerse en la primera revisión anual conjunta que se produjo entre las instituciones comunitarias y las autoridades norteamericanas sobre la efectividad práctica del Acuerdo

[643] *Cfr.* PÉREZ CAMBERO, R., "Aspectos más destacables…", *op. cit.*, p. 20.

[644] De conformidad con lo comentado por Pérez Cambero, el documento en cuestión "ofrece la información detallada sobre cada uno de los compromisos en cuatro áreas clave: 1) priorización de las remisiones e investigaciones; 2) tratamiento de las declaraciones falsas o fraudulentas de adhesión al Escudo de la privacidad; 3) supervisión continua de las órdenes; y 4) mayor compromiso y colaboración en lo que respecta a la ejecución, con las autoridades de protección de datos de la Unión Europea". *Ibidem.*

sobre el Escudo de Privacidad[645]. Por un lado, la Comisión Europea efectuó una serie de recomendaciones para que se tuvieran en cuenta, de entre las que cabe destacar: (i) la llevanza de controles periódicos por parte del Departamento de Comercio de los EE. UU. sobre el cumplimiento de los principios previstos en el Acuerdo, pues se detectaron serios incumplimientos por parte de las empresas que se encontraban adheridas al mismo; (ii) una mayor cooperación entre las autoridades de control nacionales de los EE. MM. y el Departamento de Comercio, que permitiera a su vez fortalecer la sensibilización respecto de la protección de los datos personales entre los distintos agentes que convergían en su posterior tratamiento; y (iii) un esclarecimiento sobre determinadas cuestiones relacionadas con la legislación relativa a la seguridad nacional de los EE. UU., así como un mayor compromiso en promover mecanismos que dotasen de protección a los ciudadanos no estadounidenses, como la designación del Defensor del Pueblo[646].

Por otro lado, el GT29 también tuvo ocasión de pronunciarse al respecto, dividiendo sus consideraciones en dos partes diferenciadas. Una relativa a los aspectos comerciales del Acuerdo, en la que, en consonancia con lo que también había expresado la Comisión, puso de relieve la necesidad de fortalecer los controles sobre el funcionamiento del Escudo de Privacidad. En particular, abogó por la necesidad de articular una eficaz supervisión sobre el cumplimiento de sus principios por parte de las autoridades norteamericanas competentes, así como por implementar una serie de

[645] La primera revisión conjunta anual se llevó a cabo los días 18 y 19 de septiembre de 2017 en Washington, DC. Fue inaugurado por la Comisaria de Justicia, Consumidores e Igualdad de Género, Věra Jourová, y el secretario de Comercio de Estados Unidos, Wilbur Ross. La revisión anual se realizó para la UE por representantes de la Dirección General de Justicia y Consumidores de la Comisión Europea. La delegación de la UE también incluyó a ocho representantes designados por el artículo 29, el órgano consultivo que reúne a las autoridades nacionales de protección de datos de los Estados miembros, así como el Supervisor Europeo de Protección de Datos. Del lado estadounidense, representantes del Departamento de Comercio, la Comisión Federal de Comercio (FTC), el Departamento de Transporte, el Departamento de Estado, la Oficina del Director Nacional Inteligencia y el Departamento de Justicia participaron en la revisión, así como la actuación de Ombudsperson, miembros de la Junta de Supervisión de Privacidad y Libertades Civiles y la Oficina del Inspector General de la Comunidad de Inteligencia. Además, representantes de organizaciones que ofrecen mecanismos de resolución de disputas bajo el Escudo de Privacidad, la Asociación Americana de Arbitraje como administrador del Panel de Arbitraje del Escudo de Privacidad y algunas empresas certificadas por el Escudo de la privacidad proporcionaron información durante la revisión anual. *Cfr.* COMISIÓN EUROPEA, "Informe al Parlamento Europeo y al Consejo sobre la primera revisión anual del funcionamiento del Escudo de la privacidad UE - EE. UU. (SWD [2017] 344 final)", de fecha 18 de octubre de 2017, p. 3Consultado el 15.08.2020 desde: https://ec.europa.eu/info/sites/info/files/report_on_the_first_annual_review_of_the_eu-us_privacy_shield_2017.pdf.

[646] *Vid.* COMISIÓN EUROPEA, "Informe al Parlamento… (SWD [2017] 344 final)", cit., pp. 4-7.

mejoras para la gestión de datos personales en el ámbito de RR. HH. y en relación con la toma de decisiones automatizadas[647].

Otra de las cuestiones sobre las que también emitió una valoración el referido organismo europeo radicaba en el acceso de las agencias de inteligencia de los EE. UU. a los datos transferidos desde la Unión Europea por motivos de vigilancia. Pese a haber alabado inicialmente los esfuerzos llevados a término por las autoridades gubernamentales y legislativas estadounidenses en aras de demostrar una mayor transparencia, seguía considerando que ello no era suficiente para entender muchos de los interrogantes que se habían abierto respecto del ordenamiento jurídico estadounidense. Entre otros, las actuaciones de recolección de información amparadas bajo la Sección 702 de la FISA, o la EO 12333 o, en su caso, el acceso masivo a datos personales bajo la habilitación del programa UPSTREAM, además de una ausencia total de garantías de protección como la correcta eficacia de la figura del Defensor del Pueblo[648].

Como conclusión de la primera revisión efectuada, pueden reproducirse las consideraciones de Cordero Álvarez sobre esta cuestión, pues afirma que ni la propuesta inicial ni, en definitiva, la Decisión por la que se establece el Escudo de privacidad ofrecían un nivel equivalente de protección al que existía en la UE para que las transferencias de datos a EE. UU. amparadas en este marco fueran lícitas[649].

En segunda instancia, procediendo con la enumeración de las distintas reacciones sucedidas con la aplicación del Acuerdo sobre el Escudo de Privacidad, cabe referirnos con suma importancia a la Resolución emitida por parte del Parlamento Europeo, en fecha 5 de julio de 2018[650], que siguiendo el modelo de los documentos que se han ido analizando, elogiaba los esfuerzos que se habían llevado a cabo durante la negociación del nuevo marco normativo, pero planteaba objeciones de calado. Por una parte, sobre las

---

[647] *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 255): EU – U.S. Privacy Shield – First annual Joint Review", aprobado por el Grupo de Trabajo, el 28 de noviembre de 2017, pp. 7-12. Consultado el 15.08.2020 desde: https://ec.europa.eu/newsroom/ just/ document.cfm?doc_id=48782.

[648] *Ibidem*, pp. 14-19.

[649] *Cfr*. CORDERO ÁLVAREZ, C. I., "La transferencia internacional de datos con terceros Estados en el nuevo Reglamento europeo: Especial referencia al caso estadounidense y la Cloud Act", en *Revista Española de Derecho Europeo*, nº 70 (2019), Madrid: Ed. Civitas, p. 42.

[650] *Vid*. Resolución del Parlamento Europeo nº 2018/2645(RSP), de 5 de julio de 2018, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. Consultado el 15.08.2020 desde: https://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_ES.html.

cuestiones comerciales e institucionales, manifestaba la necesidad de optar por una mayor implicación por parte del Departamento de Comercio en su papel de organismo supervisor, puesto que se habían detectado ciertas deficiencias en el funcionamiento de la figura del Defensor del Pueblo. A su vez, aprovechaba las revelaciones acaecidas en el asunto "Cambridge Analytica"[651] para reafirmar sus preocupaciones ante la ausencia de normas y garantías específicas sobre el Escudo de Privacidad[652].

Por otra parte, en relación con las cuestiones relativas a la aplicación de la ley y la salvaguarda de la seguridad nacional, advertía de varios defectos en el ámbito normativo, tales como la reautorización de la Sección 702 de la FISA, la vigencia de la EO 12333[653] y la aprobación de la *CLOUD Act*[654]. También ponía de manifiesto la ausencia de proactividad y cooperación de las autoridades gubernamentales de los Estados Unidos respecto del compromiso de dotar a la Comisión de la información suficiente que le permitiese valorar la idoneidad del marco legal existente en dicho territorio. Así como recordaba que en ningún momento se estaban aportando garantías suficientes respecto de la existencia de mecanismos efectivos que permitiesen que los

[651] El asunto "Cambrigde Analytica" hace alusión a las actividades fraudulentas realizadas por una empresa de servicios políticos del mismo nombre, que se valió de ciertas utilidades de la plataforma publicitaria de Facebook para ejercer influencia en las elecciones presidenciales de Estados Unidos en 2016. Para mayor información al respecto: *vid*. CADWALLADR C. y GRAHAM-HARRISON E., "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach", *The Guardian*. Consultado el 15.08.2020 desde: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election; KANG C. y FRANKEL S., "Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users", *New York Times*. Consultado el 15.08.2020 desde: https://www.nytimes.com /2018/04/04/technology/mark-zuckerberg-testify-congress.html; CADWALLADR C., "Google, Democracy and the Truth About Internet Search", *The Guardian*. Consultado el 15.08.2020 desde: https://www.theguardian.com/technology/2016/dec/04/google-democracy-truth-internet-search-facebook.

[652] *Ibidem*, apdos. 10-19.

[653] Cabe traer a colación las objeciones realizadas por parte de la Comisión Europea sobre la EO 12333, cuando señala que: "[r]eitera su preocupación por el Decreto 12333, que permite a la NSA compartir una gran cantidad de datos privados reunidos sin garantías, órdenes judiciales o autorizaciones del Congreso con otras dieciséis agencias, incluido el FBI, la Agencia Antidroga Norteamericana y el Departamento de Seguridad del Territorio Nacional; lamenta la falta de revisión judicial de las actividades de vigilancia llevadas a cabo sobre la base del Decreto 12333". *Ibidem*, apdo. 24.

[654] A efectos aclaratorios, conviene recordar la matización que realiza el Parlamento Europeo cuando señala que: "[…] El 23 de marzo de 2018, el Congreso de los EE. UU. promulgó la Ley de aclaración de la utilización de datos extranjeros (*Clarifying Overseas Use of Data Act*), que facilita el acceso policial al contenido de comunicaciones y otros datos relacionados, autorizando a las fuerzas del orden de los EE. UU. a obligar a presentar datos de comunicaciones incluso cuando están almacenados fuera de los Estados Unidos y permitiendo que algunos países extranjeros celebren acuerdos ejecutivos con los Estados Unidos para autorizar a los proveedores de servicios de estadounidenses responder a ciertas órdenes extranjeras para acceder a datos de comunicaciones". *Ibidem*, cdo. Q.

afectados sitos en la UE pudieran velar por la protección de sus derechos y libertades en relación con la protección de sus respectivos datos personales[655].

Como conclusiones, el Parlamento Europeo muestra unas declaraciones taxativas y rotundas sobre la situación acaecida, como destaca Cordero Álvarez, el citado organismo pidió a la Comisión que adoptase todas las medidas necesarias para garantizar que el Escudo de la privacidad cumplía plenamente con la normativa europea y jurisprudencia del TJUE en la materia —en particular, con el Reglamento—, con la CDFUE y el CEDH. Si bien, debían aplicarse de forma que no obstaculizasen innecesariamente el comercio o las relaciones internacionales, pero en ningún caso podían "compensarse" con intereses comerciales o políticos. Por todo ello, el Parlamento considera que, "a menos que los Estados Unidos cumplan plenamente el 1 de septiembre de 2018, la Comisión habrá dejado de actuar de conformidad con el artículo 45, apartado 5, del Reglamento general de protección de datos", solicitando expresamente a la Comisión que suspendiera el Escudo de la privacidad hasta que las autoridades estadounidenses cumpliesen con sus condiciones[656].

En tercera instancia y siguiendo el orden de las reacciones sucedidas, conviene detenerse en las manifestaciones efectuadas por parte de la Comisión en relación con la segunda revisión conjunta efectuada entre las autoridades norteamericanas y las comunitarias sobre la viabilidad del marco jurídico que hasta la fecha habilitaba las transferencias internacionales de datos personales a los EE. UU.[657] Concretamente, y

---

[655] *Ibidem*, apdos. 20-30.

[656] *Cfr*. CORDERO ÁLVAREZ, C. I., "La transferencia internacional de datos…", *op. cit.*, p. 43.

[657] La segunda reunión anual de revisión tuvo lugar en Bruselas los días 18 y 19 de octubre de 2018. La revisión fue inaugurada por la Comisaria de Justicia, Consumidores e Igualdad de Género Věra Jourová, el Secretario de Comercio de los Estados Unidos Wilbur Ross, el Presidente del Comisión Federal de Comercio Joseph Simons y el presidente de la Junta Europea de Protección de Datos Andrea Jelinek. Respecto del ámbito de la UE, acudieron representantes de la Comisión Europea y de la Dirección General de Justicia y Consumidores. La delegación de la UE también incluyó siete representantes designados por el Comité Europeo de Protección de Datos (el organismo independiente reunió a representantes de las autoridades nacionales de protección de datos del miembro de la UE Estados y Supervisor Europeo de Protección de Datos). Del lado estadounidense, representantes del Departamento de Comercio, el Departamento de Estado, la Comisión Federal de Comercio, el Departamento de Transporte, la Oficina del Director de Inteligencia Nacional, el Departamento de Justicia y miembros de la Junta de Supervisión de Privacidad y Libertades Civiles también participaron en la revisión, así como el Defensor del Pueblo en funciones y el Inspector General de la Comunidad de Inteligencia. Además, representantes de una organización que ofrece servicios independientes de resolución de disputas bajo el Escudo de privacidad y la Asociación Estadounidense de Arbitraje que proporcionó información durante las pertinentes reuniones de revisión. Finalmente, la revisión fue complementada con presentaciones de organizaciones sobre cómo

como hemos ido apreciando en las revisiones anteriores, las mismas se han venido dividiendo en dos partes principalmente. Una relativa a cuestiones comerciales, esto es, aquellas vinculadas al cumplimiento de las obligaciones que se preceptuaban en el contenido del propio Acuerdo sobre el Escudo de Privacidad. Y otra sobre los aspectos relacionados con la obtención y utilización de los datos personales de ciudadanos de la Unión por parte de las autoridades gubernamentales estadounidenses[658].

Respecto a la primera de ellas, la Comisión únicamente pone de manifiesto las mejoras que se han introducido por parte del Departamento de Comercio relativas a monitorizar proactivamente el cumplimiento de los principios incluidos en el Acuerdo por parte de las empresas adheridas al mismo, así como la articulación de herramientas orientadas a identificar falsas declaraciones de participación en el marco de protección. Incluso alguno de los casos que se habían comunicado a la FTC habían finalizado a través de un procedimiento sancionador. En consecuencia, se trataba encontrar un aumento de la efectividad de los procesos de certificación y supervisión existentes[659].

En relación con la segunda de las temáticas sobre las que se pronuncia la Comisión en la segunda revisión conjunta, podemos advertir que una de las cuestiones que mayor relevancia ostentaba residía en la Ley de Reautorización (*Reauthorization Act*) de 2017, que, desarrollada a principios de 2018, permitió que, entre otros cambios, se produjera la reautorización de la Sección 702 de la FISA por seis años más, extendiendo su vigencia hasta el 31 de diciembre de 2023, pese a que su fecha límite se había pactado hasta finales de 2017[660]. En cualquier caso, si bien ello no supuso la incorporación en la FISA de las protecciones que se habían acordado en la PPD-28 —de conformidad con las solicitudes expresadas por la Comisión—, no se produjeron limitaciones sobre las garantías que ya

---

las empresas cumplen con los requisitos del marco. *Vid*. COMISIÓN EUROPEA, "Informe al Parlamento Europeo y al Consejo sobre la segunda revisión anual del funcionamiento del Escudo de la privacidad UE - EE. UU. (SWD [2018] 497 final)", de fecha 19 de diciembre de 2018, pp. 3-4. Consultado el 15.08.2020 desde: https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_ 2018.pdf.

658 *Vid*. COMISIÓN EUROPEA, "Informe al Parlamento… (SWD [2018] 497 final)", cit., pp. 4-5.

659 *Ibidem*, p. 3.

660 *Vid*. COMISIÓN EUROPEA, "Documento de trabajo del personal de la Comisión que acompaña al Informe al Parlamento Europeo y al Consejo sobre la segunda revisión anual del funcionamiento del Escudo de la privacidad UE - EE. UU. (COM [2018] 860 final)", de fecha 19 de diciembre de 2018, pp. 26-28.Consultado el 15.08.2020 desde: https://ec.europa.eu/info/sites/info/files/staff_working_document_-_second_annual_review.pdf.

incorporaba la propia norma —refiriéndonos a la FISA—, así como las enmiendas introducidas tampoco reforzaron las potestades de las agencias de inteligencia respecto a sus capacidades de obtención y análisis de datos personales provenientes de ciudadanos no estadounidenses[661].

Adicionalmente, también se constataron avances en materia de transparencia y tutela de los derechos y libertades. Por un lado, siguiendo las recomendaciones de la Comisión, la Junta de Supervisión de Privacidad y Libertades Civiles (*Privacy and Civil Liberties and Oversight Board*) hizo público su informe en relación con la aplicación de la DPP-28, en el que se ponía de manifiesto que las agencias de inteligencia habían modificado ciertas prácticas que llevaban a cabo en función de los requisitos que establecía la norma[662]. Por otro lado, la Comisión concluyó que era preciso realizar un estrecho seguimiento de la evolución normativa estadounidense sobre esta temática, subrayando la necesidad de que el cargo del Defensor del Pueblo fuera desarrollado con carácter permanente —pues hasta la fecha había sido desarrollado en régimen de interinidad—[663], dándole de plazo hasta el 28 de febrero de 2018 al gobierno de los EE. UU. para efectuar los correspondientes cambios o acciones oportunas[664].

No obstante, cabe reproducir las manifestaciones efectuadas al respecto por parte del CEPD —en grandes líneas van en el mismo sentido que las advertencias expresadas por parte de la Comisión—, que prestan especial atención ante la necesidad de articular un mayor número de controles sustanciales a efectos de garantizar la correcta aplicación del Acuerdo sobre el Escudo de Privacidad y sus respectivos principios —como el de ulterior transferencia—[665]. Estos aspectos ya habían sido puestos de manifiesto por parte

---

[661] *Vid*. COMISIÓN EUROPEA, "Informe al Parlamento… (SWD [2018] 497 final)", cit., p. 4.

[662] *Ibidem.*

[663] *Vid*. COMISIÓN EUROPEA. GT29. "Documento de trabajo… (COM [2018] 860 final)", cit., pp. 28-29.

[664] A este respecto, cabe citar que el nombramiento final se produciría el 20 de junio de 2019, cuando el Senado de los Estados Unidos confirmó que el Subsecretario de Estado para el Crecimiento Económico, Energía y Medioambiente era designado como responsable de la oficina del Defensor del Pueblo.

[665] *Vid*. COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, "Escudo de la privacidad UE-EE. UU. – Segunda revisión conjunta anual", adoptado el 22 de enero de 2019, pp. 9-14. Consultado el 11.07.2020 desde: https://edpb.europa.eu/sites/edpb/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf.

del GT29 durante la primera revisión anual[666]. En este punto, el CEPD recuerda que aún quedaba pendiente resolver determinadas preocupaciones heredadas de esa primera revisión anual, relativas al acceso masivo e indiscriminado a los datos de ciudadanos europeos, así como a la posibilidad de que las autoridades gubernamentales de los EE. UU. publicaran informes de transparencia y seguimiento sobre las actividades de las agencias de inteligencia[667].

En cuarta instancia, conviene hacer alusión a la última revisión conjunta efectuada por parte de los organismos de la UE y los EE. UU. en relación con la viabilidad del Acuerdo sobre el Escudo de Privacidad antes de su correspondiente anulación[668]. Siguiendo con el mismo modelo que se ha observado respecto las anteriores revisiones, se diferencian las consideraciones en dos ámbitos sustantivos relativos a su aplicación y contenido.

Por un lado, en relación con las cuestiones comerciales orientadas a verificar el cumplimiento efectivo del referido Acuerdo por parte de las organizaciones adheridas al mismo, la revisión de la Comisión se basa en el análisis de ciertas cuestiones heredadas de la segunda revisión que se habían formulado el año anterior, centradas en: (i) la

---

666 *Vid*. COMISIÓN EUROPEA. GT29. "Documento de Trabajo (nº 255): EU – U.S. Privacy Shield…", cit., pp. 7-10.

667 *Vid*. COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, "Escudo de la privacidad UE-EE. UU…", cit., pp. 16-20.

668 La tercera reunión anual de revisión tuvo lugar en Washington, D.C. los días 12 y 13 de septiembre 2019. Siendo inaugurado por la Directora General de Justicia y Consumidores Tiina Astola, EE. UU., así como por el Secretario de Comercio Wilbur Ross, el Presidente de la Comisión Federal de Comercio Joseph Simons y el vicepresidente de la Junta Europea de Protección de Datos Ventsislav Karadjov. En representación de la UE, la reunión estuvo a cargo de representantes de la Dirección General de Justicia y Consumidores de la Comisión Europea, así como por ocho representantes designados por Comité Europeo de Protección de Datos que también participó en esta reunión. Del lado estadounidense, representantes del Departamento de Comercio, el Departamento de Estado, la Comisión Federal de Comercio, el Departamento de Transporte, la Oficina del Director de Inteligencia Nacional, el Departamento de Justicia y miembros del Junta de Supervisión de Privacidad y Libertades Civiles también participaron en la revisión, así como el recién nombrado Defensor del Pueblo y el Inspector General de la Comunidad de inteligencia. Además, representantes de dos organizaciones que ofrecían servicios independientes de resolución de disputas bajo el Escudo de Privacidad y la Asociación de Arbitraje, que administra el panel de arbitraje del Escudo de Privacidad. Finalmente, se complementaron las actuaciones con las presentaciones de organizaciones certificadas con la inclusión de aquellas actividades que las empresas llevan a cabo para cumplir con los principios contenidos en el marco de Acuerdo sobre el Escudo de Privacidad. *Vid*. COMISIÓN EUROPEA, "Informe al Parlamento Europeo y al Consejo sobre la tercera revisión anual del funcionamiento del Escudo de la privacidad UE - EE. UU. (SWD [2019] 390 final)", de fecha 23 de octubre de 2019, pp. 2-3. Consultado el 15.08.2020 desde: https://ec.europa.eu/info/sites/info/files/report_on_the_third_annual_review_of_the_eu_us_privacy_shield_2019.pdf.

asignación de plazos demasiado extensos para que las organizaciones pudiesen tomar acciones que les permitieran subsanar ciertos defectos que les impedían adherirse al proceso de recertificación del Acuerdo; (ii) la constatación de controles esporádicos escasos —con carácter mensual—, llevados a cabo por parte del Departamento de Comercio para revisar el cumplimiento del Acuerdo; (iii) necesidad de ampliar la búsqueda de afirmaciones falsas sobre aquellas empresas que nunca hubieran solicitado la adhesión al Escudo de Privacidad, pues señaló la Comisión que serían las que más perjuicios ocasionarían sobre los derechos y libertades de los afectados; (iv) ejecutar mecanismos de cooperación efectivos entre la FTC, la Comisión y las autoridades de protección de datos que permitiesen colaboraciones simultáneas durante la realización de investigaciones por incumplimiento de los principios recogidos en el Acuerdo, así como el desarrollo de recursos interpretativos sobre su correcta aplicación[669].

Por otro lado, respecto de las actuaciones de las autoridades administrativas norteamericanas con los datos personales obtenidos de ciudadanos de la Unión y su respectivo marco jurídico que las amparaba. La Comisión señaló que durante la última anualidad computada desde la segunda revisión no se habían producido desarrollos normativos vinculados a la obtención de información de inteligencia extranjera en virtud de la habilitación efectuada por la Sección 702 de la FISA, sino que incluso se habían realizado aclaraciones por parte de las agencias de inteligencia sobre el uso de "selectores"[670] en sus actividades de investigación, sujetos a mecanismos de independencia judicial y legislativa[671].

A mayor abundamiento, la Comisión también apuntó serias preocupaciones respecto de determinadas disposiciones normativas de protección que habían sido introducidas a partir de la *USA Freedom Act*, dado que, como su fecha de expiración era próxima —prevista para el 15 de diciembre de 2019—, existía la posibilidad de que las

[669] *Vid*. COMISIÓN EUROPEA, "Informe al Parlamento… (SWD [2019] 390 final)", cit., pp. 3-5.

[670] En cualquier caso, cabe recordar que los selectores no se entienden como palabras clave o nombres de personas, sino que se trata de cuentas de comunicación específicas como lo podría ser una dirección de correo electrónico o un número de teléfono. *Vid*. COMISIÓN EUROPEA, "Documento de trabajo del personal de la Comisión que acompaña al Informe al Parlamento Europeo y al Consejo sobre la segunda revisión anual del funcionamiento del Escudo de la privacidad UE - EE. UU. (COM [2019] 495 final)", de fecha 23 de octubre de 2019, pp. 20-22. Consultado el 15.08.2020 desde: https://ec.europa.eu/info/sites/info/files/staff_working_document_-_third_annual_review.pdf.

[671] *Vid*. COMISIÓN EUROPEA, "Informe al Parlamento… (SWD [2019] 390 final)", cit., p. 6.

mismas pudieran ser reautorizadas por parte del Congreso de los Estados Unidos, entre las que destacaría especialmente la Sección 501 de la FISA. Adicionalmente, se indicó por parte de la Comisión que, durante el desarrollo de las conversaciones sucedidas en el marco de la tercera revisión anual, se trasladó por parte del gobierno de los EE. UU. que la NSA había decidido suspender el programa de registros de llamadas habilitado bajo esta Sección por su limitado valor práctico, pero que en cualquier caso se reservaban la facultad de su reactivación si volvía a resultar relevante en un futuro[672].

No obstante, la Comisión apunta que, en caso de producirse la referida reautorización, deberían adoptarse las cautelas y salvaguardas que resultasen necesarias para evitar la recolección de datos de manera masiva e indiscriminada por parte de las agencias de inteligencia correspondientes. De lo contrario, se entraría en conflicto con las obligaciones y garantías preceptuadas en el Acuerdo sobre el Escudo de Privacidad. Al mismo tiempo, también se puso de manifiesto por parte de las autoridades norteamericanas que la DPP-28 seguía estando plenamente en vigor y desplegando sus efectos de protección, no siendo objeto de modificación alguna[673].

Por ende, no resulta óbice señalar las principales conclusiones alcanzadas por parte del CEPD durante la tercera revisión anual que se viene analizando, que, como sucedía en su pronunciamiento realizado sobre la segunda revisión anual, van en la misma línea que los aportados por parte de la propia Comisión Europea. Respecto de las cuestiones comerciales, señala las mismas preocupaciones que se habían ido reiterando desde la creación del Acuerdo sobre el Escudo de Privacidad, centradas en la ausencia de controles sustantivos que permitiesen articular un correcto funcionamiento del marco normativo que habilitase las transferencias, así como la necesidad de perfeccionar el proceso de recertificación de las empresas adheridas, así como abordar las cuestiones relativas a la gestión de los datos vinculada a los Departamentos de Recursos Humanos.[674]

En relación con los aspectos relativos a las capacidades de acceso de las autoridades administrativas norteamericanas sobre los datos personales de ciudadanos

---

672 *Vid*. COMISIÓN EUROPEA, "Documento de trabajo… (COM [2019] 495 final)", cit., pp. 19-24.

673 *Vid*. COMISIÓN EUROPEA, "Informe al Parlamento… (SWD [2019] 390 final)", cit., pp. 6-7.

674 *Vid*. COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, "Escudo de la privacidad UE-EE. UU. – Tercera revisión conjunta anual", adoptado el 12 de noviembre de 2019, pp. 10-16. Consultado el 11.07.2020 desde: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbprivacyshield3rda nnualreport.pdf _en.pdf.

europeos transferidos al otro lado del Atlántico, el CEPD celebraba el nombramiento del Defensor del Pueblo con carácter permanente —en respuesta a las innumerables peticiones realizadas por parte de las instituciones comunitarias—. Pero a pesar de estos acontecimientos, en línea con lo que ya había expresado tanto el propio organismo como el GT29, considera preciso dotar de mayores salvaguardas los programas de vigilancia llevados a cabo por parte de las agencias de inteligencia estadounidenses, mediante la revisión de las normas que habilitan esta tipología de actuaciones vinculadas a la seguridad nacional, tales como la Sección 702 de la FISA y la EO 12333[675].

[675] *Ibidem*, pp. 17-22.

5. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 16 de julio de 2020, asunto C-311/18) ("Schrems II")

Ahora que se ha analizado el contenido de la Decisión, así como las consecuencias que se han ido suscitando a lo largo de su escasa vigencia, debe prestarse especial atención a la sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 16 de julio de 2020, en el asunto C-311/18 (en adelante también, "Schrems II")[676]. Además de suponer la invalidación del Acuerdo sobre el Escudo de Privacidad, su emisión se ha convertido en un auténtico quebradero de cabeza, tanto desde el punto de vista operacional para el sector empresarial como para las propias instituciones comunitarias, dado que su contenido ha impactado en dos vertientes, jurídica y económica, teniendo la primera una consecuencia directa sobre la segunda por la situación de inseguridad generada.

No es cuestión baladí señalar que, pese a la dificultad de determinar con exactitud la importancia económica que los flujos de información entre los Estados Unidos de América y la Unión Europea suponen para los respectivos territorios, existen indicadores que permiten afirmar que esta última es el mayor socio digital de los Estados Unidos, pues el comercio entre ambos aumentó de quinientos noventa y cuatro mil millones de dólares a mil doscientos billones entre 2003 y 2017. Asimismo, los servicios vinculados a las nuevas tecnologías representaron aproximadamente ciento noventa mil millones de dólares de exportaciones estadounidenses a la Unión en 2017. Finalmente, se estimó que en 2016 la relación económica entre los referidos territorios generaba doscientos sesenta mil millones de dólares de comercio de servicios digitales al año[677].

5.1. Antecedentes de hecho

Como inicio del análisis de los antecedentes de hecho que convergen en la sentencia del TJUE relativa al caso Schrems II, conviene recordar para su correcta

[676] *Vid*. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 16 de julio de 2020, en el asunto C-311/18, que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la High Court (Tribunal Superior, Irlanda), mediante resolución de 4 de mayo de 2018, recibida en el Tribunal de Justicia el 9 de mayo de 2018, en el procedimiento entre el Comisario de Irlanda y Facebook Ireland Ltd, Maximillian Schrems, con intervención de: The United States of America, Electronic Privacy Information Centre, BSA Business Software Alliance Inc., Digitaleurope. Consultado el 15.08.2020 desde: https://edpb.europa.eu/ sites/edpb/files/files/file1/edpbprivacyshield3rdannualreport .pdf_en.pdf.

[677] *Vid*. U.S. CONGRESSIONAL RESEARCH SERVICE, "Digital Trade and U.S. Trade Policy", pp. 20-21.

comprensión que la misma no es más que una continuación de la acción judicial que el mismo demandante, el Sr. Maximillian Schrems, había emprendido años atrás en 2013, cuya finalización culminaría en 2015 con la invalidación del Acuerdo de Puerto Seguro, tal y como hemos tenido la oportunidad de abordar con anterioridad[678].

Sobre la base de lo anterior, conviene seguir relacionando ambas iniciativas, pues tienen por objeto principal atender las cuestiones prejudiciales planteadas por el Tribunal Supremo de Irlanda ante el TJUE en el marco de las actividades efectuadas por Facebook respecto de las transferencias internacionales realizadas con los datos personales de sus usuarios residentes en la Unión Europea hacia los Estados Unidos de América. Si bien también cabe afirmar que sus respectivos ámbitos de aplicación difieren entre sí, dado que el primero de los pronunciamientos se centra en abordar la validez de la Decisión de la Comisión, de fecha 26 de julio de 2000, en base a las limitaciones de facultades de las autoridades de control. El segundo, en cambio, analiza la validez de la Decisión de la Comisión, de fecha 12 de julio de 2016, partiendo de las obligaciones de las autoridades de control de velar por el cumplimiento del principio del nivel de protección adecuado del país destinatario de los datos personales objeto de tratamiento.

Ahora bien, una vez hecha esta anotación y siguiendo con la exposición de los antecedentes de hecho que motivaron este segundo pronunciamiento emitido por parte del TJUE. Cabe remontarnos al 1 de diciembre de 2015, cuando el Sr. Schrems presenta una versión modificada de la reclamación que había realizado con antelación al 25 de junio de 2013, como consecuencia de la desestimación de esta última sobre la base de las justificaciones aducidas por Facebook Irlanda. Dicha entidad manifestaba que las transferencias de datos personales de ciudadanos de la UE que efectuaba a los Estados Unidos se articulaban mediante la utilización de las cláusulas contractuales tipo aprobadas por parte de la Comisión[679].

La versión modificada de la reclamación remitida ante la autoridad de protección de datos de Irlanda solicitaba la suspensión de las transferencias internacionales de datos a los Estados Unidos por parte de Facebook Inc. En la misma, se argumentaba que las agencias de inteligencia norteamericanas recogían y trataban los datos de los ciudadanos de la Unión de manera masiva e indiscriminada en el marco de programas de vigilancia

[678] *Vid*. STJUE. Asunto C-311/18 (Schrems II), cit., apdos. 50-52.

[679] *Ibidem*, apdos. 52-54.

amparados por la legislación estadounidense. En consecuencia, ello resultaba totalmente incompatible con el mandado de protección efectuado por los artículos 7, 8 y 47 de la CDFUE[680].

Posteriormente, la autoridad de protección de datos de Irlanda, tras constatar mediante una investigación nacional la veracidad de las alegaciones efectuadas por el demandante Sr. Schrems —en la que intervino el gobierno de los EE. UU.—. Dio inicio a un procedimiento ante el Tribunal Supremo de Irlanda con base en la doctrina que había sido formulada un año antes en la STJUE por la que se declaraba la invalidez del Acuerdo de Puerto Seguro, solicitando la necesidad de plantear una petición de decisión prejudicial ante la Corte europea. La actuación finalmente se hizo efectiva el 4 de mayo de 2018[681] , culminando con su aceptación definitiva por parte de la Corte europea[682].

La cuestión prejudicial planteada giraba en torno a diferentes extremos vinculados a la validez de las CCT, para poder ser consideradas un mecanismo válido para articular las transferencias internacionales de datos personales a aquellos destinos que no ofreciesen garantías suficientes para ser considerados con un nivel de protección adecuado desde el prisma de la legislación europea en materia de protección de datos. Así como también se solicitaba la evaluación sobre si se producía una vulneración de los artículos 7 y 8 de la CDFUE, cuando se realizan movimientos de datos transfronterizos a los Estados Unidos, atendiendo a las particularidades de su sistema jurídico, en el que primaba, en todo caso, la salvaguarda a la seguridad nacional[683].

A este respecto, resulta oportuno traer a colación las palabras vertidas por Cordero Álvarez cuando señala que, en la cuestión prejudicial, se plantea qué relevancia tiene, en su caso, la Decisión sobre el Escudo de la privacidad en la valoración efectuada en cuanto a la adecuación de la protección ofrecida a los datos transferidos a EE. UU. conforme a la Decisión CCT. Y si constituye la figura del Defensor del Pueblo en el ámbito de este Acuerdo (anexo A del anexo III de la Decisión sobre el Escudo de la privacidad), en combinación con el régimen vigente en EE. UU., una garantía de que este país ofrece una vía de recurso compatible con el artículo 47 de la CDFUE a los interesados cuyos datos

[680] *Ibidem*, apdos. 55-57.

[681] *Ibidem*, apdos. 58-67.

[682] *Ibidem*, apdos. 71-76.

[683] *Ibidem*, apdo. 68.

personales son transferidos a EE. UU. (con arreglo a la Decisión CCT). En consecuencia, por todo ello, se plantea en definitiva si la Decisión CCT vulnera en este caso los artículos 7, 8 y 47 de la CDFUE, dada cuenta de la constatación del ínfimo nivel de protección del derecho a la protección de los datos personales existente en EE. UU., a pesar de que a nivel institucional se pretendiese efectuar una apariencia de legitimidad[684].

En este sentido, la cuestión suscitada se centraba en valorar si las CCT podían entenderse como una garantía suficiente que impidiese que el importador de los datos personales debiere revelar los mismos ante sus respectivas autoridades gubernamentales, en virtud de un requerimiento efectuado en aplicación de su legislación nacional. Sobre este punto, se incardinan esencialmente las conclusiones alcanzadas por el Abogado General, Sr. Henrik Saugmandsgaard Øe, presentadas el 19 de diciembre de 2019[685], con posterioridad a la audiencia pública sobre el caso que tuvo lugar durante el mes de julio de 2019. La misma contó con una amplia participación integrada por miembros del gobierno de los EE. UU., de la autoridad de protección de datos de Irlanda, de la Comisión Europea, autoridades de varios Estados miembros de la Unión, el propio Sr. Schrems, Facebook, Inc., grupos de interés y activistas en materia de protección de datos.

Dichas conclusiones versan esencialmente sobre dos temáticas. Por un lado, encontramos la relacionada con la validez de CCT propiamente, aspecto que atiende el Abogado General, recordando que las autoridades de control de los EE. MM. están obligadas a suspender o prohibir una transferencia internacional de datos personales cuando se considere que las CCT no van a resultar válidas en el tercer país al que se pretendan remitir los datos en cuestión, o siempre que el responsable o encargado del tratamiento establecido en la Unión no haya efectuado ninguna acción tendente a prevenir el incumplimiento. En cualquiera de los dos casos, se trata de un mandato efectuado por el artículo 58.2 del RGPD, que establece la necesidad de que las autoridades velen por la

684 *Cfr*. CORDERO ÁLVAREZ, C. I., "La transferencia internacional de datos…", *op. cit.*, pp. 44-45.

685 *Vid*. Conclusiones del Abogado General Sr. Henrik Saugmandsgaard Øe sobre el asunto C-311/18 promovido por la petición de decisión prejudicial presentada por la High Court (Tribunal Supremo de Irlanda) el 19 de diciembre de 2019. Consultado el 15.08.2020 desde: http://curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex= 0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=928552.

protección de los derechos y libertades de los afectados consagrados en la legislación europea que regula la materia[686].

Sin perjuicio de lo anterior, no debe olvidarse que las CCT amparadas bajo el acervo del artículo 42.2, letra c), del RGPD determinan la obligación del responsable, ya sea a través de sus propios medios o en colaboración con el destinatario de la transferencia, de verificar que el movimiento transfronterizo de datos personales se puede llevar a cabo lícitamente. Para ello, deberá tenerse en cuenta las particularidades que puedan converger sobre el ordenamiento jurídico del tercer país destinatario, pues en caso de que no se suceda la aplicación de garantías suficientes, deberá evitarse la transmisión de cualquier flujo de información, dado que, en cualquier momento, la autoridad de control competente podría proceder a su suspensión o anulación[687].

En consecuencia, la atención de cualquier requerimiento de las autoridades del tercer país destinatario de la transferencia formulado en atención de una obligación establecida por de la legislación nacional aplicable, que pueda contravenir el contenido referido en la cláusula 5 de las CCT —esto es, que la actuación en cuestión pueda considerarse que va "más allá de las restricciones necesarias en una sociedad democrática para la salvaguardia, en particular, de la seguridad del Estado, la defensa y la seguridad pública"[688]—, podrá considerarse que supone una vulneración de las CCT[689].

Por lo que puede concluirse a este respecto que para que las CCT se consideren válidas como mecanismo para garantizar las condiciones de protección adecuadas en el tercer país de destino al que se pretendan remitir los datos, será preciso que las mismas puedan desplegar todos los efectos y eficacia de sus disposiciones. El cumplimiento de dicha condición únicamente será posible si el importador trata los datos personales recabados conforme a las instrucciones que le facilite al respecto su exportador, así como de acuerdo con el contenido previsto en las CCT. Si estos condicionantes no se pudieran materializar, como se ha detallado, la transferencia internacional de datos tampoco podría llevarse a cabo.

---

686 *Ibidem*, apdo. 148.

687 *Ibidem*, apdo. 126.

688 *Vid*. STJUE. Asunto C-311/18 (Schrems II), cit., apdo. 141.

689 *Vid*. Apartado 131 de las conclusiones del Abogado General Sr. Henrik Saugmandsgaard Øe sobre el asunto C-311/18.

Por otro lado, la otra temática que aborda el Abogado General en sus conclusiones radica en la consideración de los Estados Unidos como un país que no ofrece un nivel de protección adecuado[690], poniendo en entredicho la validez de la Decisión que se viene analizando. Entre las diversas cuestiones que le llevan a asumir tal afirmación, podemos encontrar la ausencia de límites tangibles que impongan restricciones a las actuaciones realizadas por las agencias de inteligencia norteamericanas bajo el mandato de la Sección 702 de la FISA[691], así como la inexistencia de garantías específicas que pongan de manifiesto la efectividad e independencia de la figura del Defensor del Pueblo respecto al poder ejecutivo[692].

Por ende, debe recordarse la transcendencia de las conclusiones que son alcanzadas por parte del Abogado General cuando se plantea el estudio de un asunto dirimido por parte del TJUE. A pesar de que las opiniones que emite ostentan carácter meramente consultivo y se presentan con una debida antelación al pronunciamiento final, existen estudios que demuestran que cuando esta figura manifiesta la necesidad de declarar la nulidad de un acto en cuestión en su dictamen, la Corte Europea tiene un 67 % más de probabilidades de dirimir la problemática tomando como referencia las vicisitudes que previamente haya manifestado el referido órgano consultivo al respecto[693].

5.2. Contenido de la Sentencia "Schrems II"

Teniendo en cuenta todo lo que antecede, conviene entrar a analizar el contenido esencial vertido en la Sentencia "Schrems II", que, pese a no ser demasiado extensa en cuanto a su número de páginas, incluye consideraciones de gran calado por lo que a los efectos de este estudio interesa. En primer término, el Alto Tribunal concreta que los movimientos transnacionales de datos personales que se realicen con finalidades comerciales entre distintos responsables o encargados sitos en cualquier Estado miembro a terceros territorios seguirán considerándose como una transferencia internacional de los

690 *Ibidem*, apdo. 175.

691 *Ibidem*, apdos. 291, 292 y 297.

692 *Ibidem*, apdo. 337.

693 *Vid*. ARREBOLA, C., MAURICIO, A. J., JIMÉNEZ PORTILLA, H., "An Econometric Analysis of the Influence of the Advocate General on the Court of Justice of the European Union", en *Cambridge Journal of Comparative and International Law*, Vol. 5, nº 1 (2016), University of Cambridge.

mismos a la luz de lo establecido en el RGPD. No obstante, podrán existir excepciones justificadas que motiven que los datos objeto de tratamiento puedan ser conocidos por parte de las autoridades del país tercero de destino con el objetivo de atender finalidades vinculadas a la seguridad y defensa nacional[694].

En un segundo término, se aborda también el papel fundamental que adoptan las autoridades nacionales de los EE. MM. en aquellos supuestos en los que un tratamiento de datos personales conlleva aparejada una transferencia internacional de los mismos. Ello se realiza desde una doble perspectiva. Por un lado, encontramos las facultades que se les reconocen a estos organismos nacionales en relación con la aplicación de las CCT —siguiendo el mandato efectuado por el artículo 58.2, letras f) y j) del RGPD—, pues, ante la ausencia de una decisión de adecuación adoptada por parte de la Comisión, tienen la obligación de suspender o prohibir una transferencia internacional de datos a un país tercero que se fundamente en las referidas CCT. Lo anterior se podrá llevar a cabo siempre que constaten que las mismas no se cumplen o no pueden cumplirse atendiendo a todas las particularidades que se suceden en el movimiento de datos pretendido, a excepción de aquellos supuestos en los que el responsable o el encargado hubieran suspendido la transferencia o puesto fin a la misma por sí mismos[695].

Y, por otro lado, el literal de la sentencia recoge una serie de consideraciones relativas a las potestades de las susodichas autoridades nacionales frente a una decisión de adecuación adoptada por parte de la Comisión. Se recuerda que estas últimas no podrán suspender o prohibir una transferencia internacional de datos que encuentre amparo en una decisión de adecuación formalmente adoptada por la Comisión, siempre que esta no haya sido previamente declarada inválida por parte del TJUE. Todo ello, sin perjuicio de que cuando un interesado formule una reclamación ante la autoridad de control nacional competente y esta aprecie indicios fundados de incumplimiento de las exigencias establecidas por el RGPD, pueda interponer un recurso ante los tribunales nacionales para que éstos a su vez puedan plantear, si lo estiman oportuno, una cuestión prejudicial al Alto Tribunal comunitario para que determine sobre la validez de una decisión en cuestión[696].

---

694 *Vid*. STJUE. Asunto C-311/18 (Schrems II), cit., apdo. 89.

695 *Ibidem*, apdos. 115-121.

696 *Ibidem*, apdos. 156-162.

Prosiguiendo con el análisis que se viene efectuando respecto del pronunciamiento examinado. En un tercer término, se considera oportuno remarcar aquellas consideraciones de mayor calado que el TJUE reproduce respecto de las CCT. En consonancia con el criterio que había marcado con antelación el Abogado General en sus conclusiones, reitera la validez y vigencia de las mismas por no ser contrarias a los artículos 7, 8 y 47 de la CDFUE, dado que incorporan mecanismos efectivos que permiten garantizar que aquellas transferencias internacionales de datos personales que se efectúen a un país tercero que no respete el contenido de estas, puedan quedar automáticamente suspendidas o prohibidas[697].

En este sentido, el TJUE hace hincapié en la necesidad de diferenciar entre las CCT y las decisiones de adecuación. Estas últimas, a diferencia de las primeras, tienen como finalidad principal determinar el nivel de protección adecuado de un país tercero, una vez que se han evaluado diferentes circunstancias concurrentes como puede ser su legislación interna o los principios generales que definen su ordenamiento jurídico nacional, para que una vez terminada dicha evaluación, si la misma resultase favorable, la Comisión pudiese declarar la idoneidad de la adecuación de dicho territorio, generándose un efecto vinculante para las autoridades nacionales de los distintos EE. MM. de la Unión[698]. Por el contrario, en los supuestos en que deban de utilizarse las CCT, será el exportador establecido en el ámbito comunitario el responsable de comprobar si durante el movimiento transfronterizo se dan las garantías adecuadas[699]. De no ser así, estaría obligado a proporcionar aquellas adicionales que resultasen convenientes[700] o, en su defecto, evitar llevar a cabo el tratamiento de datos personales pretendido.

Por último, el TJUE concluye que el Acuerdo sobre el Escudo de Privacidad resulta incompatible con el mandato efectuado por el artículo 45.1 del RGPD interpretado

---

[697] *Ibidem*, apdos. 147-149.

[698] *Ibidem*, apdos. 128-130.

[699] A este respecto, cabe traer a colación el propio literal del texto de la STJUE, cuando afirma que: "[d]ado que, como se desprende del apartado 125 de la presente sentencia, es inherente al carácter contractual de las cláusulas tipo de protección de datos que estas no pueden vincular a las autoridades públicas de países terceros, pero que los artículos 44 y 46, apartados 1 y 2, letra c), del RGPD, interpretados a la luz de los artículos 7, 8 y 47 de la Carta, exigen que el nivel de protección de las personas físicas garantizado por dicho Reglamento no se vea comprometido, puede resultar necesario completar las garantías recogidas en esas cláusulas tipo de protección datos". *Ibidem*, apdo. 132.

[700] *Ibidem*, apdos. 147-149.

a la luz de los artículos 7, 8 y 47 del CDFUE. Entiende que la Comisión no tuvo en cuenta dichas consideraciones, pese que *a priori* había efectuado las comprobaciones necesarias que le permitieron determinar con exactitud que EE. UU. y, en consecuencia, la Decisión de Ejecución (UE) nº 2016/1250 reunían los condicionantes necesarios para declarar al país estadounidense con un nivel de protección adecuado. Máxime, si se aprecia que el propio contenido de la Decisión reconoce expresamente la primacía de las exigencias de las autoridades norteamericanas en relación con la salvaguarda de la seguridad nacional y el interés público frente a la protección del derecho a la protección de los datos personales. Esta circunstancia, con anterioridad, ya había provocado la caída del anterior Acuerdo de Puerto Seguro[701].

En consecuencia, el Alto Tribunal entiende que dichas injerencias únicamente serían válidas a la luz de la legislación europea en materia de protección de datos, si se hubieran regulado en consonancia con las garantías equivalentes y derechos exigibles que ofrece el ordenamiento comunitario a los sujetos afectados por la recogida y tratamiento de sus datos personales[702]. Pero, *a sensu contrario*, se constata que ni los programas de vigilancia empleados por los EE. UU. ofrecen una tutela judicial efectiva respecto del ejercicio de derechos por parte de los interesados[703], así como que tampoco el mecanismo del Defensor del Pueblo proporciona ninguna vía de recurso ante un órgano que ofrezca a las personas afectadas —ciudadanos no estadounidenses—, garantías sustancialmente equivalentes a las proporcionadas por el CDFUE[704].

5.3. Implicaciones de la Sentencia "Schrems II" para las transferencias internacionales de datos personales a los Estados Unidos de América

Ante la situación de incertidumbre generada por la declaración de invalidez del Acuerdo sobre el Escudo de Privacidad, fueron múltiples los pronunciamientos que se sucedieron, tanto por parte de las autoridades nacionales competentes como por los organismos comunitarios. El cometido principal de dichas actuaciones radicaba en intentar abordar la cuestión bajo la primacía del principio de seguridad jurídica, evitando que se volvieran a producir situaciones de desconcierto como las que se habían acontecido

[701] *Ibidem*, apdo. 164.

[702] *Ibidem*, apdos. 168-190.

[703] *Ibidem*, apdo. 192.

[704] *Ibidem*, apdo. 197.

escasos cinco años antes con la declaración de invalidez del anterior Acuerdo sobre Puerto Seguro que regulaba la materia. En las siguientes líneas únicamente se abordarán aquellas manifestaciones de mayor calado efectuadas por las principales instituciones con relevancia en el ámbito de la Unión, pues reproducir en detalle el contenido de cada una de las reacciones propiciadas excedería el alcance pretendido con la consecución del presente trabajo.

Una de las primeras instituciones de la Unión que tuvo a bien pronunciarse sobre el resultado de la Sentencia del TJUE fue la propia Comisión Europea protagonista de la Decisión objeto de invalidez, que mediante una declaración efectuada en fecha 16 de julio de 2020[705] manifiesta la necesidad de tomar como referencia las consideraciones efectuadas por el Alto Tribunal para mejorar las herramientas existentes respecto a la realización de transferencias internacionales de datos, así como también aprovecha la oportunidad para celebrar la confirmación de validez de las CCT. Al mismo tiempo, aprovecha para reafirmar su compromiso en seguir garantizando el cumplimiento de la legislación comunitaria y el respeto de los derechos fundamentales que la misma consagra, así como de seguir negociando con el Departamento de Comercio de los EE. UU. un nuevo marco mejorado de protección que pueda dar cabida a subsanar los defectos indicados por el propio TJUE.

Seguidamente a la Comisión, le sucedieron otros organismos de la Unión con competencias sobre la materia. Por un lado, encontramos que el Comité Europeo de Protección de Datos emitió una declaración en fecha 17 de julio de 2020[706] en que comenta varias cuestiones sobre la decisión del TJUE. En primera instancia recalca que, como ya había reflejado en sus anteriores informes sobre la segunda y tercera revisión del Acuerdo sobre el Escudo de Privacidad, existían dudas razonables que aconsejaban una revisión en profundidad sobre su viabilidad, tal y como se ha tenido la oportunidad de observar en los anteriores apartados del presente trabajo.

[705] *Vid*. Declaración efectuada por la Comisión Europea como consecuencia de la STJUE en el asunto C-311/18 (Schrems II), en fecha 16 de julio de 2020. Consultado el 15.08.2020 desde: https://ec.europa.eu/commission/presscorner/detail/en/statement_20_1366.

[706] Declaración efectuada por parte del Comité Europeo de Protección de Datos como consecuencia de la STJUE en el asunto C-311/18 (Schrems II), en fecha 17 de julio de 2020. Consultado el 15.08.2020 desde: https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en.

En segunda instancia, el CEPD acoge como propios los razonamientos vertidos por el TJUE en relación con ciertos aspectos vinculados a la validez y eficacia de las CCT. Subraya la responsabilidad que ostentan el exportador y el importador de los datos personales de garantizar un nivel de protección adecuado respecto de los datos personales que sean objeto de transferencia, así como la obligación de las autoridades de control nacionales de los Estados Miembros de suspender o prohibir aquellas transferencias a terceros países cuando las mismas no se realicen en condiciones que permitan asegurar el mantenimiento de un nivel de protección adecuado.

En tercera y última instancia, el Comité recuerda que existen otros mecanismos que permiten llevar a cabo movimientos transnacionales de datos personales con la observancia de las cautelas que propugna la legislación europea aplicable sobre la materia. Asimismo, reconoce como una de las alternativas, las excepciones a la regla general que se incluyen en el artículo 49 del RGPD. Pero que, en todo caso, únicamente podrán utilizarse en aquellos supuestos en que se haya valorado específicamente su utilización, así como que la recurrencia en su aplicación sea esporádica o puntual.

Por otro lado, podemos advertir la reacción efectuada al respecto por parte del Supervisor Europeo de Protección de Datos, que, en su declaración, también de fecha 17 de julio de 2020[707], acogía con aceptación la decisión alcanzada por parte del TJUE respecto la invalidez del Acuerdo sobre el Escudo de Privacidad. Dicho organismo lo entendió como una actuación necesaria para preservar un elevado nivel de protección respecto de los datos personales de los ciudadanos europeos cuando estos se transfieren a terceros países que no ostentan un nivel adecuado. Aprovecho a su vez para enfatizar que la Comisión, en los próximos acuerdos que se sucedan para abordar esta temática, deberá tener plena observancia sobre la interpretación que realiza el Alto Tribunal del contenido de RGPD que regula la materia.

Adicionalmente a lo anterior, el SEPD apunta que las grandes cuestiones que se analizan en la STJUE radican, por un lado, en la total ausencia de mecanismos que permitiesen una correcta tutela judicial respecto de los derechos de los interesados europeos de acudir a vías de recurso previstas en el ordenamiento jurídico norteamericano. Por otro lado, sobre la validez de las CCT, considera que para que las mismas sean consideradas como adecuadas, deberán de analizarse teniendo en cuenta las

[707] *Ibidem.*

circunstancias particulares del supuesto en que se pretendan articular. Más si recordamos que sus respectivos suscribientes serán los responsables de su correcta implementación práctica.

A modo de conclusión del presente apartado, resulta importante remarcar que con independencia de la totalidad de reacciones producidas por parte de las autoridades de control nacionales de los EE. MM., el Parlamento Europeo, a través de su correspondiente Comité[708], en fecha 3 de setiembre, inició una serie de reuniones internas en aras de revisar el futuro más próximo en lo relativo a los movimientos transatlánticos de datos personales a los Estados Unidos, centrando sus esfuerzos en tres grandes líneas de trabajo. Una primera relacionada con la preparación de una guía que abordase la problemática, una segunda centrada en la actualización de los clausulados de las CCT, así como una tercera y última orientada a trabajar juntamente con los EE. UU. para construir un marco robusto que habilitase nuevamente las transferencias internacionales de datos a dicho territorio con las suficientes garantías de protección.

Con posterioridad, dichas líneas de trabajo fueron profundizadas mediante una serie de actuaciones. En relación con la primera de ellas, el Comité Europeo de Protección de Datos publicó una serie de recomendaciones sobre aquellas medidas que podían ayudar a complementar los instrumentos existentes que permitían articular las transferencias internacionales de datos a terceros países u organizaciones internacionales y garantizar el cumplimiento del nivel de protección adecuado para los datos personales de ciudadanos de la Unión. El documento iba dirigido a aquellos responsables o encargados del tratamiento que actúan como exportadores de los datos, pues son los responsables de verificar, ya sea de manera individualizada o en colaboración con el importador de los datos del país destinatario, si la legislación o la práctica de ese tercer territorio da cumplimiento a las consideraciones establecidas en la normativa comunitaria que regula la materia[709].

---

[708] *Vid*. Declaración efectuada por parte del Parlamento Europeo como consecuencia de la STJUE en el asunto C-311/18 (Schrems II), en fecha 3 de septiembre de 2020. Consultado el 28.09.2020 desde: https://multimedia.europarl.europa.eu/en/committee-on-civil-liberties-justice-and-home-affairs_20200903-1345-COMMITTEE-LIBE_vd?auth_cloudf=c3e8a8d1-e536-ac08-b5a9-1a4fbc 1f3951.

[709] *Vid*. COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, "Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE, adoptadas el 10 de noviembre de 2020", p. 2. Consultado el

Asimismo, el CEPD proporcionaba una serie de pautas para los referidos exportadores que les permitiesen llevar a cabo una evaluación de los terceros países y establecer medidas complementarias para aquellos supuestos en que resultase preciso. Como primer paso, el referido organismo europeo determinaba la necesidad de tener identificadas las distintas transferencias que se producían, así como cerciorarse de que los datos tratados se limitaban a los estrictamente necesarios. Un segundo paso establecía la necesidad de verificar la idoneidad del instrumento por el que se había optado para legitimar cada una de las transferencias de datos. El tercer paso se centraba en evaluar si la legislación del tercer país podía poner en jaque la eficacia de las garantías adecuadas que se habían adoptado. Esta evaluación debía basarse en los distintos puntos que el CEPD ya había tenido la oportunidad de abordar, los cuales han sido examinados en el presente trabajo.

En consonancia con el orden de pautas que se venía enunciando, el cuarto paso se encontraba sujeto a que la evaluación anterior determinase la necesidad de aplicar medidas complementarias, a raíz de verificar que el país de destino de los datos personales no cumplía con el estándar de protección adecuado que exige la legislación comunitaria. El documento en cuestión incluye un listado de medidas complementarias, que por sí solas, o en combinación entre ellas, pueden ser eficaces en determinados terceros países para garantizar que la transferencia internacional de los datos se realiza con garantías adecuadas[710]. El CEPD también considera que si no existe ninguna medida que pueda resultar aplicable, el responsable o encargado del tratamiento deberá evitar, suspender o poner fin a la transferencia de los datos personales. Al mismo tiempo, también determina la necesidad de que las distintas cuestiones se documenten debidamente.

En última instancia, se reproducen los pasos quinto y sexto, respectivamente. El primero de ellos, consiste en adoptar cualquier procedimiento formal que pueda ser preciso para articular la medida complementaria que resulte de aplicación en función del instrumento escogido para legitimar la transferencia internacional de los datos. El segundo consiste en la obligatoriedad de ir supervisando con carácter regular si se ha producido alguna circunstancia que haya alterado o modificado el escenario que se había

21 de enero de 2021 desde: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_es.pdf.

[710] *Vid*. CEPD, "Recomendaciones 01/2020 sobre medidas…", cit., pp. 24-39.

contemplado inicialmente en el momento de escoger la medida complementaria. Si ello se hubiera producido, deberían valorarse nuevamente las condiciones que se aplican sobre el movimiento de datos transfronterizo en cuestión.

Como último aspecto a destacar, conviene advertir que, en fecha 21 de junio de 2021, el CEPD daba a conocer mediante nota de prensa[711], la versión final del documento que incluía las recomendaciones recibidas durante el período de consulta pública. Las principales modificaciones han sido incorporadas en el paso cuarto, que radican en la importancia de examinar las prácticas de las autoridades gubernamentales del tercer país de destino al que se pretendan transmitir los datos personales, con la intención de determinar si las mismas, así como el propio ordenamiento jurídico que resulte de aplicación, ofrecen suficientes garantías para la debida protección de los datos personales transferidos.

En el supuesto de que la evaluación de riesgos realizada no aporte un resultado favorable para llevar a cabo la transferencia internacional de datos personales que se pretenda articular. El CEPD recomienda: i) suspender la transferencia; ii) implementar aquellas medidas complementarias que puedan resultar de aplicación para mitigar el riesgo existente; iii) realizar la transferencia de los datos personales sin aplicar ningún tipo de medida complementaria, siempre que se considere que no existe justificación suficiente que motive la adopción de estas. En este último supuesto, resultará preciso demostrar y documentar dicha decisión mediante un informe detallado que acredite la aplicación de las suficientes garantías de protección en el tercer país de destino al que se pretendan remitir los datos personales. Este último de los puntos puede resultar un tanto paradigmático, pues parece revertir la carga de responsabilidad que debiera corresponderle a la Comisión Europea sobre los responsables y encargados del tratamiento. Siendo consciente dicho organismo de que, en el caso de los Estados Unidos, ni el mismo fue capaz de evitar que las agencias de inteligencia norteamericanas entrasen a conocer los datos personales de ciudadanos de la Unión.

Siguiendo con las líneas de trabajo que había anunciado la Comisión a tenor de la invalidez del Acuerdo sobre el Escudo de Privacidad, el 12 de noviembre de 2020 se

[711] *Vid*. Nota de prensa del CEPD sobre la adopción de distintas actuaciones en el marco de su sesión plenaria, de fecha 21 de junio. Consultado el 21 de junio de 2021 desde: https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en

publicó un proyecto de Decisión de Ejecución sobre las CCT para la transferencia de datos personales a terceros países de conformidad con el RGPD, así como otro proyecto de Decisión de Ejecución centrado en actualizar el contenido de las referidas CCT[712]. Ambos documentos combinan las cláusulas generales que originariamente se contenían con un nuevo enfoque modular para atender las distintas tipologías de movimientos transnacionales de datos personales que se producen. Su contenido fue sometido al escrutinio del CEDP y del SEPD, órganos que emitieron una opinión conjunta sobre ambos proyectos relativos a las CCT en fecha 14 de enero de 2021[713].

En términos generales, el documento acoge con satisfacción los esfuerzos llevados a cabo por parte de la Comisión para alinear el contenido de las CCT con los requerimientos que establece al respecto el RGPD, así como con las consideraciones vertidas sobre este instrumento por parte del TJUE en sus sucesivos pronunciamientos relacionados con los intercambios de datos con los Estados Unidos. En este sentido, la Opinión pone de manifiesto dos grandes problemáticas a las que se ha tenido que aportar una solución mediante las CCT. Por un lado, la necesidad de cubrir situaciones cada vez más complejas de movimientos de datos mediante un enfoque más flexible, como, por ejemplo, el número de partes que pueden unirse al contrato. Y, por otro lado, la obligatoriedad de prever salvaguardas específicas para aquellos supuestos en los que el ordenamiento jurídico del país de destino de los datos no aporte suficientes garantías, como, por ejemplo, en el momento de atender las peticiones de ejercicio de derechos efectuados por parte de los interesados.

Ante este contexto de cierta inseguridad jurídica, en fecha 4 de junio de 2021, la Comisión Europea hacía pública la Decisión de Ejecución que actualizaba las referidas CCT[714]. El referido organismo comunitario aprovecho la ocasión para prever diversas novedades respecto del contenido establecido en sus antecesoras. En primer lugar, la versión actualizada de las CCT introduce la posibilidad de que las mismas puedan aplicarse extraterritorialmente, esto es, en aquellos supuestos donde a pesar de que los

[712] Proyectos de Decisión de Ejecución sobre las CCT. Consultado el 21 de enero de 2021 desde: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-CommissionImplementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.

[713] *Vid*. CEPD. "Opinión conjunta emitida por el CEDP y el SEPD sobre la Decisión de Ejecución en relación con las CCT". Consultado el 21 de enero de 2021 desde: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22021-standard_es.

[714] *Vid*. Decisión de Ejecución (UE) 2021/914 de la Comisión, cit.

responsables están establecidos fuera de la Unión Europea, les resulta de aplicación el RGPD en virtud del punto de conexión establecido en su artículo 3.2 respecto a sus encargados o subencargados del tratamiento.

En segundo lugar, mediante su Cláusula 5 se permite que terceras partes puedan adherirse a la versión de las CCT que estuviere suscrita hasta la fecha, sin necesidad de instar su resolución para suscribir una versión actualizada. A su vez, los módulos dos y tres contienen todas las prerrogativas establecidas por el artículo 28 del RGPD. Lo anterior, se traduce en una mejora competitiva a nivel procesal y en términos de seguridad jurídica del propio documento, eliminando la posibilidad de disponer de versiones contradictorias respecto del contenido incluido en el contrato de encargado del tratamiento y el propio de las CCT. Todo y que éstas últimas, en cualquier caso, deberán de prevalecer ante una posible duda interpretativa.

En tercer lugar, se introducen nuevas obligaciones de información para los interesados, previéndose incluso la posibilidad de facilitar una copia a éstos de las CCT cuando así lo soliciten, con la respectiva salvaguarda de aquellas cuestiones de confidencialidad que no puedan divulgarse. Adicionalmente, a diferencia de la anterior versión de las CCT que únicamente disponía de un listado orientativo para los movimientos de datos entre responsable y encargado, en este nueva versión encontramos cuatro escenarios posibles con una descripción de medidas técnicas y organizativas particularizada para cada uno de ellos.

En cuarto lugar, siguiendo con las recomendaciones efectuadas por parte del CEPD y TJUE, la utilización de la versión actualizada de las CCT —por aplicación de sus cláusulas 14 y 15— supondrá la necesidad de realizar un análisis de impacto previo sobre los efectos que una transferencia internacional de datos pueda suponer sobre los derechos y libertades de los afectados. Lo anterior se contemplará en aquellos supuestos donde las mismas puedan no resultar suficientes para evitar la intromisión de las autoridades gubernamentales de un tercer país, o en su defecto, el proveedor no disponga de capacidad y medios suficientes que permitan garantizar la aplicabilidad de las medidas estipuladas en las propias CCT. El análisis en cuestión versará sobre la identificación de los factores de riesgos que pueda suponer la transferencia, prestando especial atención a la situación normativa existente en el país de destino al que se pretendan remitir los datos personales.

Adicionalmente, aparte de las novedades que se han expuesto en contraposición con el anterior régimen existente. Se ha optado por introducir un periodo de transición de 15 meses para su correspondiente aplicación, computados a partir de la fecha de vencimiento de las anteriores CCT que aún estuvieran en vigor. Por lo que, en cualquier caso, podrá suscribirse dicha versión anterior hasta el 27 de septiembre de 2021 como máximo, en virtud del periodo de gracia de tres meses que la Comisión ha considerado oportuno habilitar. Ello se podrá articular siempre que las actividades del tratamiento se sigan efectuando en idénticos términos a los que se venían realizando y que se garanticen las suficientes garantías adecuadas.

Por ende, cabe concluir la tercera y última de las líneas de trabajo abordadas por la Comisión, que se centraba en trabajar juntamente con los EE. UU. para construir un marco robusto que habilitase nuevamente las transferencias internacionales de datos a dicho territorio con las suficientes garantías de protección. A este respecto, las conversaciones se iniciaron en agosto de 2020, en aras de evaluar las potenciales actuaciones que debían de llevarse a término[715]. En fecha de 25 de marzo de 2021, las autoridades comunitarias y norteamericanas efectuaban una nota de prensa conjunta en las que manifestaban nuevamente la intensificación de dichas negociaciones, que habían quedado algo estancadas con las elecciones presidenciales de los Estados Unidos[716].

[715] Nota de prensa conjunta entre la Comisión Europea y el Departamento de Comercio de los EE. UU. sobre el inicio de las negociaciones. Consultado el 21 de enero de 2021 desde: https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en.

[716] Nota de prensa conjunta entre la Comisión Europea y el Departamento de Comercio de los EE. UU. relativa a la intensificación de las negociaciones. Consultado el 25 de marzo de 2021 desde: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443.

CAPÍTULO III – CASUÍSTICAS ESPECIALES DE TRANSFERENCIAS INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL

SUMARIO: 1. La Directiva 2016/681 de la Unión Europea sobre los datos del PNR (*Passenger Register Number*); 2. Transferencias internacionales de datos a los países asiáticos. Análisis de un nivel de adecuación.

Introducción

En este capítulo se ha creído oportuno abordar dos casuísticas especiales englobadas dentro del alcance de la institución jurídica de las transferencias internacionales de datos que se ha venido a examinar. En primer lugar, se ha optado por analizar una de las principales medidas adoptadas para la lucha contra las amenazas antiterroristas que tiene su fundamento en el intercambio masivo de datos personales de pasajeros entre las distintas compañías aéreas y las respectivas autoridades gubernamentales en el contexto de la Unión Europea, e incluso, en ocasiones, hacia los Estados Unidos de América.

Para ello, se analizará el contenido establecido en la Directiva relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave (en adelante, Directiva PNR). Cuya entrada en vigor se produciría el 24 de mayo de 2016 —en la misma fecha que lo hizo el Reglamento (UE) 2016/679—, colisionando directamente con los fundamentos intrínsecos de la cultura jurídica de protección de datos existente en la Unión Europea.

Y, en segundo lugar, se examinará otro de los principales escollos a los que se enfrenta la Unión Europea en el momento de habilitar el flujo de datos personales hacia terceros países que no ostentan un nivel de protección adecuado. En concreto, el análisis se delimitará a los principales países del continente asiático que disponen de una regulación sobre la materia —más o menos avanzada—. Su objetivo se centrará en demostrar que el marco jurídico existente en la actualidad en dichos territorios no da

cobertura suficiente a la protección de la privacidad y los datos de carácter personal. Y menos aún podría llegar a considerarse como un sistema de derechos y libertades más garantista —o incluso equiparable— al instaurado en el ámbito comunitario.

1. La Directiva 2016/681 de la Unión Europea sobre los datos del PNR (*Passenger Register Number*)

1.1. Introducción

Coincidiendo con la aprobación del RGPD, como se ha expuesto con anterioridad, el Parlamento Europeo y el Consejo dieron luz verde a un paquete de medidas orientado a la prevención del terrorismo y a la lucha contra el crimen organizado. Entre ellas, por lo que a efectos de este trabajo interesa, resulta preciso citar la Directiva relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave[717], cuya entrada en vigor se produciría el 24 de mayo de 2016, colisionando directamente con los fundamentos intrínsecos de la cultura jurídica de protección de datos existente en la Unión Europea.

Teniendo en cuenta lo anterior, resulta de interés en esta primera parte del capítulo realizar una enumeración de las principales consideraciones que se han vertido en la Directiva PNR, quedando fuera del alcance la realización de un análisis exhaustivo sobre las particularidades de su contenido. Así pues, de conformidad con lo establecido en su artículo 18, apartado primero, los Estados miembros debían adoptar, a más tardar el 25 de mayo de 2018, las disposiciones legales, reglamentarias y administrativas necesarias que permitiesen dar cumplimiento a lo dispuesto por la misma, mediante su incorporación a los respectivos ordenamientos jurídicos.

La norma que venimos comentando tiene como principal objetivo, como indica Pérez-Luño, garantizar la seguridad nacional, proteger la vida y la seguridad de los ciudadanos, mediante la prevención, detección, investigación y persecución de casos de terrorismo y delitos graves[718], así como a través de la creación de un marco jurídico para la protección de los datos PNR en lo que respecta a su tratamiento por las autoridades

[717] *Vid*. Directiva (UE) 2016/681 del Parlamento 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 delincuencia grave. Consultado el 12.08.2020 desde: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0681&from=EN

[718] *Vid*. Directiva (UE) 2016/681, *op. cit.*

competentes[719]. Siendo este último de los aspectos citados uno de los que mayor controversia suscita, pues se produce una habilitación para que las agencias de seguridad e inteligencia accedan de manera masiva a los datos relativos al PNR. Ello no es más que otra nueva iniciativa de las autoridades gubernamentales para ampliar su elenco de facultades, orientadas precisamente a obtener el máximo rendimiento en la recogida masiva de datos personales[720].

En este orden de cuestiones, y antes de seguir con el avance en el estudio de la Directiva PNR, cabe detenerse un momento para definir el contenido de las siglas PNR. Una vez traducidas al castellano, pueden entenderse como el Registro de Nombre de Pasajeros, que, según el artículo 3 de la referida norma comunitaria, radican en constituir una: "Relación de los requisitos de viaje impuestos a cada pasajero, que incluye toda la información necesaria para el tratamiento y control de las reservas por parte de las compañías aéreas que las realizan y participan en el sistema PNR, por cada viaje reservado por una persona o en su nombre, ya estén contenidas en sistemas de reservas, en sistemas de control de salidas utilizado para embarcar a los pasajeros de vuelo o en sistemas equivalentes que posean las mismas funcionalidades".

En palabras de Catalina Benavente, puede entenderse como el término comúnmente utilizado para designar la información relativa a reservas hechas en sistemas de reservas (en adelante, CRS), pues en el momento en que se efectúa una reserva, el sistema de reservas concede un número de esta o localizador. Este localizador permite al pasajero, a la empresa de transporte o a una agencia de viaje consultar, modificar o cancelar la reserva o elementos de la reserva, siempre que estén conectados al sistema de reservas en el que originalmente se creó la reserva[721].

1.2. Antecedentes

Una vez realizada esta breve conceptualización del término PNR, debe proseguirse citando que la recogida de esta tipología de datos no se trata de un ejercicio

[719] *Vid*. PÉREZ LUÑO, A. E., "La nueva normativa europea para la protección de los datos personales", en *Derechos y libertades*, nº 40 (2019), p. 233.

[720] *Vid*. CATALINA BENAVENTE, M. A., "La Directiva Europea (UE) 2016/681, de 27 de abril de 2016, relativa a la utilización de los datos por en la lucha contra el terrorismo y la delincuencia grave", en *Diario La Ley*, nº 8801 (2016), p. 5.

[721] *Ibidem*, p. 3.

recientemente moderno realizado por parte de las compañías aéreas. Se trata de una práctica que se ha venido efectuando durante las últimas décadas para finalidades vinculadas a intereses comerciales, así como también se ha utilizado por parte de los servicios de aduanas y policiales. Finalmente, dichas actuaciones se han convertido en una cuestión necesaria que ha precisado su legitimación jurídica a través de una norma de calado comunitario.

Como se ha tenido la oportunidad de advertir en el ámbito de la protección de los datos de carácter personal respecto de los programas de vigilancia masiva e indiscriminada llevados a cabo por las agencias de seguridad e inteligencia de los Estados Unidos de América, los atentados del 11 de septiembre de 2001 supusieron un antes y un después en la política legislativa exterior a nivel mundial. Especialmente en la estadounidense, suscitándose textos como los dispuestos en la *Patriot Act*, que habilitaban ciertas prácticas de obtención de información e intromisión en la esfera privada del individuo, cuya legalidad sería puesta en duda diversas ocasiones. El caso que aquí nos compete se convierte en otra muestra de ello, dado que las referidas autoridades gubernamentales podían acceder a los datos relativos a los pasajeros que operasen por rutas que tuvieran destino en el país norteamericano, o que incluso atravesasen su territorio.

En contraposición con lo anterior, la Unión Europea se había planteado en diversas ocasiones la necesidad de articular un escenario similar sobre el análisis de datos de pasajeros al existente en otros territorios[722], como era el caso que venimos apuntando de los EE. UU. En el contexto estadounidense, la *Aviation and Transport Security Act* de 2001[723], creada de manera inmediatamente posterior a los atentados del 11 de septiembre

[722] Como también sería el caso de Australia, Canadá o el Reino Unido, países con los que en la actualidad existe un acuerdo con la Unión Europea en materia de transmisión de datos PNR para la persecución de determinados delitos. *Vid*. CATALINA BENAVENTE, M. A., "La transmisión de los datos PNR en la lucha contra el terrorismo y otras formas de delincuencia grave", en COLOMER HERNÁNDEZ, I. (Dir.), OUBIÑA BARBOLLA, S. (Coord.), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Ed. Thomson Reuters-Aranzadi, 2015, pp. 301-356.

[723] Se trata de una legislación aprobada a finales de noviembre de ese mismo año 2001. *Vid*. *Aviation and Transportation Security Act (ATSA), 19 November 2001 (Public Law 107-71, 107th Congress, 49 USC Section 44909(c) (3) (2001))*; y en 2002, *the US passed legislation concerning border security (Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSV), 5 May 2002)*.

de ese mismo año[724], establecía, entre otras cuestiones, la obligación de realizar el registro de los datos de los pasajeros de las aerolíneas mediante el PNR.

Adicionalmente, también incorporó otro cambio importante basado en que los controles que hasta el momento se llevaban a cabo directamente por parte de las compañías aéreas pasaron a ser responsabilidad de un organismo público, la Administración de Seguridad en el Transporte. Dicha modificación habilitaba una vía para obtener información sobre los distintos pasajeros que viajaban, llegaban o pasaban sobre el territorio norteamericano, pues, entre los distintos datos que se obtenían, se encontraban desde los meramente identificativos hasta los más sensibles como la tipología de comida que era objeto de petición[725].

A colación del contexto expuesto, la Unión Europea creyó oportuna la aprobación de la Directiva 2004/82/CE[726], precisamente con la intención de paliar las deficiencias existentes en los controles fronterizos y poder luchar contra la inmigración ilegal a partir de la información facilitada con antelación por parte de las propias compañías aéreas sobre sus respectivos pasajeros. La norma en cuestión pivotaba sobre esta concepción de la "*advanced passenger information*" (en adelante, API), que, a diferencia del PNR[727], su contenido se utilizaba para el control del tráfico migratorio en los pasos fronterizos

---

[724] *Vid*. KAUNERT, C., LEONARD, S., y MCKENZIE, A., "The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the cases of PNR and SWIFT", en *European Security*, nº 21 (4) (2012), pp. 474-496.

[725] La legislación referida se encuadra en una espiral de sucesos legislativos acaecidos en Estados Unidos como una reacción de supervivencia como consecuencia de los ataques terroristas del citado 11 de septiembre de 2001. *Vid*. CAÑABATE PÉREZ, J., "La Directiva 2016/681 de la Unión Europea sobre los datos del PNR (Passenger Register Number): ¿se ha roto el frágil equilibrio entre garantía de la protección de datos personales y seguridad?", en *Working Papers*, Ed. ICPS, Universitat Autònoma de Barcelona, 2017, p. 4.

[726] *Vid*. Directiva 2004/82/CE del Consejo, de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas. Para un mayor detalle sobre la transposición de la norma al ordenamiento jurídico español. *Vid*., entre otros: RALLO LOMBARTE, A., "El terrorismo internacional y sus conflictos: Seguridad vs. Privacidad", en *Inteligencia y seguridad. Revista de análisis y prospectiva*, nº 3 (2007), pp. 113-131; CUBERO MARCOS, J. I. y ABERASTURI GORRIÑO, U., "Protección de los datos personales en las comunicaciones electrónicas: especial referencia a la Ley 25/2007 sobre conservación de datos", en *Revista Española de Protección de Datos*, nº 83, 2008, pp. 175-197. Más reciente: SERRA CRISTÓBAL, R., "Los derechos fundamentales en la encrucijada de la lucha contra el terrorismo yihadista. Lo que el constitucionalismo y el Derecho de la Unión Europea pueden ofrecer en común", en *XIV Congreso Asociación de Constitucionalistas de España*, 2016.

[727] Los datos del PNR se utilizan principalmente como un instrumento para la prevención y represión de ilícitos terroristas y formas graves de delitos transnacionales. *Cfr*. PÉREZ FRANCESCH, J. L., GIL MÁRQUEZ, T., GACITÚA ESPÓSITO, A., "Informe sobre el PNR...", *Working Paper*, *op. cit*., p. 4.

europeos, en aras de luchar contra la inmigración ilegal mediante la comunicación anticipada de los datos de los diferentes viajeros a las autoridades competentes de cada Estado miembro.

Asimismo, conviene precisar dos diferencias sustanciales existentes entre ambos conceptos. La primera de ellas radica en la fiabilidad de la fuente de origen de los datos recabados, dado que el PNR se conforma principalmente a partir de la información aportada por los distintos pasajeros a las compañías aéreas en el momento en que se produce la contratación del desplazamiento. Entre la información aportada, se incluye el detalle de los datos de pago de cada una de las personas transportadas, las posibles dietas que hayan podido escoger, así como cualquier otro dato adicional que se pueda considerar relevante. De esta manera, no resulta demasiado difícil la elaboración de perfiles mediante la utilización de estos parámetros.

En cambio, los datos API son recolectados directamente de documentos oficiales como puede ser un pasaporte, que incluye, entre otros, su número de referencia, así como los datos identificativos de su titular, esto es, su nombre, apellidos, nacionalidad y fecha de nacimiento. Por ende, la información dimanante de los datos API aporta una mayor seguridad jurídica y fiabilidad que el PNR, al tratarse de datos que no han sido debidamente cotejados[728].

La segunda de las diferencias indicadas se encuentra en la disponibilidad de la información, pues los datos de PNR se obtienen con mayor antelación que los API. Existen determinados acuerdos suscritos por la Unión Europea, que incluso llegan a considerar los API como parte integrante de los datos PNR para su efectivo intercambio.

---

[728] Como señala Catalina Benavente: "el Dictamen conjunto sobre la propuesta de Decisión marco del Consejo relativa al uso del registro de nombres de los pasajeros ("*Passenger Name Record*" —PNR—) a efectos de la aplicación de la ley, presentado por la Comisión el 6 de noviembre de 2007, adoptado el 5 de diciembre de 2007 por el Grupo de trabajo previsto en el art. 29 y el 18 de diciembre de 2007 por el Grupo de trabajo sobre Policía y Justicia, pág. 6, (a partir de ahora Dictamen conjunto): "[E]n cualquier caso, debe aclararse qué entendemos por necesidad operativa del uso de datos PNR y qué valor añadido tiene habida cuenta de la existencia de tres medidas —el SIS (Sistema de Información de Schengen), el VIS (Sistema de Información de los Visados) y el uso de datos API—. Hasta ahora no se han presentado pruebas de que en la lucha contra el terrorismo y la delincuencia organizada sean necesarios datos, con excepción de los datos API. Las autoridades responsables de la protección de datos de la UE no están, por lo tanto, en condiciones de concluir que sea necesario crear un régimen de PNR a escala de la UE". A continuación, señala que, antes de proceder a otras demandas, hubiera sido deseable un análisis exhaustivo de cómo están utilizando las autoridades competentes los datos API para los fines declarados en la Directiva. Finalmente, recuerda que los datos PNR, a diferencia de los datos API, no son datos validados y deben considerarse poco fiables. *Cfr*. CATALINA BENAVENTE, M. A., "La Directiva Europea…", *op. cit.*, pp. 13-14.

No obstante, como se tendrá ocasión de abordar en las próximas líneas, no debe obviarse que la situación descrita en relación con la obtención masiva de información conllevó que se generasen una serie de alertas desde el punto de vista de la protección de los datos de carácter personal, que motivaron que el Supervisor Europeo de Protección de Datos tuviera que pronunciarse al respecto.

En este sentido, cabe adicionar que el escaso volumen de datos personales que se regulaba bajo el contenido de la Directiva 2004/82/CE facilitó su tramitación. La norma estipulaba en su artículo 3 la imposición de la obligación a las empresas transportistas de comunicar, a más tardar al término del embarque —cuando así lo solicitasen las autoridades encargadas de los controles de personas en las fronteras exteriores—, la información relativa a las personas que iban a transportar a un paso fronterizo habilitado por el que tendrían acceso al territorio de un Estado miembro[729]. Se establecía así una obligación de transmisión de la información cuando existiese un requerimiento de la autoridad competente, que, a diferencia de lo que sucedía con el PNR, no implicaba una comunicación sistemática de la información relativa a cada vuelo planificado en el entorno de la Unión Europea. Siendo este último escenario más invasivo en relación con el respeto del derecho fundamental a la protección de los datos de carácter personal[730].

A partir de este momento, se inicia un largo proceso de discusión en el seno de las instituciones comunitarias para intentar conciliar la adopción de medidas para la persecución del terrorismo y determinados delitos graves con el respeto al derecho fundamental a la protección de los datos de carácter personal. Así pues, el 6 de noviembre de 2007, la Comisión presenta una propuesta de Decisión marco sobre la utilización de los datos PNR para fines represivos[731], que manifiesta como principal cometido: "Armonizar las disposiciones de los Estados miembros relativas a la obligación de las compañías aéreas que efectúen vuelos hacia o desde el territorio de un Estado miembro

[729] *Vid.* Artículo 3, apartado 1, de la Directiva 2004/82/CE.

[730] *Vid*. PÉREZ FRANCESCH, J. L., GIL MÁRQUEZ, T., GACITÚA ESPÓSITO, A., "Informe sobre el PNR…", *op. cit.*, pp. 3-24.

[731] *Vid*. Propuesta de decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros ("Passenger Name Record" —PNR—) con fines represivos (COM/2007/0654 final), de fecha 6 de noviembre de 2007. Consultado el 28.06.2020 desde: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52007PC0654&from=EN.

por lo menos de transmitir los datos PNR a las autoridades competentes con el fin de prevenir los atentados terroristas y la delincuencia organizada y luchar contra ellos"[732].

La propuesta de Decisión marco de 2007 encontró un escollo en su tramitación con la aprobación del Tratado de Lisboa, pues se hizo evidente la necesidad de articular su regulación mediante la instrumentalización de una Directiva. No sería entonces hasta principios de 2011 cuando se presentaría una propuesta de texto bajo la forma de Directiva[733], en virtud del mandato efectuado por parte del "Programa de Estocolmo: una Europa abierta y segura que sirva y proteja al ciudadano"[734], que intentaba extender el uso de los sistemas analíticos de datos de los pasajeros en aras de la prevención de delitos graves y vinculados a finalidades terroristas. No obstante, dicha propuesta no llegaría a materializar su objetivo pretendido, pues fue rechazada el 29 de abril de 2013 por parte del Parlamento Europeo, por no salvaguardar suficientemente el derecho a la protección de los datos de carácter personal[735].

No fue entonces hasta los atentados que tuvieron lugar en Paris en 2015 —y, posteriormente en Bruselas en marzo de 2016—[736] cuando se reactivaron los esfuerzos

---

[732] *Ibidem.*

[733] *Vid*. Propuesta de Directiva del Parlamento Europeo y del Consejo, relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves (COM/2011/0032 final).

[734] *Vid*. "Programa de Estocolmo: una Europa abierta y segura que sirva y proteja al ciudadano", DO C 115 de 4.5.2010, p. 1.

[735] A este respecto, Catalina Benavente apunta que: "[l]a votación sobre esta propuesta de Directiva tuvo lugar el 24 de abril en una Sesión en la que los eurodiputados, por una ajustada mayoría (30 votos a favor y 25 en contra), votaron en contra de que las autoridades dispusiesen de un registro de datos personales de los pasajeros de avión con origen o destino en la UE. Este rechazo supuso entonces un nuevo retraso en la aprobación de una herramienta que para muchos es fundamental en la lucha contra el terrorismo, y otras formas de delincuencia grave, mientras que, para otros, sigue sin estar demostrado la eficacia de una medida de esta naturaleza en la lucha contra el terrorismo, mientras que es evidente la injerencia que supone en los derechos fundamentales a la intimidad, a la protección de datos de carácter personal y a la no discriminación, recogidos en los arts. 7, 8 y 21 de la Carta de Derechos Fundamentales de la UE". *Cfr*. CATALINA BENAVENTE, M. A., "La Directiva Europea…", *op. cit*., p. 12.

[736] Como manifiesta Cañabate Pérez sobre esta cuestión: "[é]stos adeptos al grupo terrorista, en su mayoría con ciudadanía de algún Estado miembro, regresan a la Unión Europea suponiendo una gran amenaza, pues han recibido un fuerte adoctrinamiento que les hace radicalizarse en sus convicciones, a lo que se debe acompañar de un elevado entrenamiento en el manejo de armas y explosivos. Además, muchos de ellos han recibido instrucciones para cooptar nuevos partidarios y organizar cédulas terroristas que pueden acabar cometiendo atentados en la UE. En el año 2015, en el periodo previo a la aprobación de la Directiva del PRN, se estimaba que el número de ciudadanos procedentes de Francia, Reino Unido y Bélgica que habían viajado a Siria e Irak para sumarse al ISIS y habían regresado a territorio europeo superaba los 3.000. Estas circunstancias, sin duda muy alarmantes, condujeron a la UE a plantearse la necesidad de introducir una

por parte de las instituciones comunitarias para intentar articular los mecanismos necesarios que permitieran hacer frente a las amenazas terroristas que se estaban produciendo. Asimismo, durante un lapso temporal de casi dos años se realizó un esfuerzo regulatorio exhaustivo en relación con la regulación del PNR. Una prueba de ello la podemos encontrar en la resolución que fue aprobada el 11 de febrero de 2015 por parte del Parlamento Europeo, sobre las medidas a adoptar en la lucha contra el terrorismo, en aras de garantizar la seguridad y las libertades de los ciudadanos de la Unión[737].

Hasta la fecha, el Parlamento no había efectuado ninguna actuación adicional sobre las cuestiones relativas al PNR desde que la Comisión de Asuntos Civiles rechazó la propuesta de Directiva en 2013. No sería hasta el 2 de diciembre de 2015 cuando se alcanzaría un acuerdo provisional entre el Parlamento Europeo y el Consejo, con el respaldo de la Comisión de Asuntos Civiles por 38 votos a favor, 19 en contra y dos abstenciones. El texto definitivo de la Directiva PNR sería finalmente aprobado en abril de 2016, no estando su aplicación práctica exenta de complicaciones, pues no era más que otro escollo que ponía de manifiesto la dificultad sucedida durante su tramitación legislativa.

Vemos, pues, que la lucha frente al terrorismo se ha centrado esencialmente en los últimos años en torno a la creación del sistema PNR en el marco de la Unión Europea, a través de intentar homogeneizar los requerimientos en todos los Estados miembros. Ello es así incluso con la definición de los delitos relativos a actividades terroristas que se contienen en la Directiva PNR. Se trata de la misma conceptualización que la recogida en

nueva Directiva sobre el PNR para monitorear los flujos de pasajeros de aerolíneas con entrada o salida en la UE. *Cfr*. CAÑABATE PÉREZ, J., "La Directiva 2016/681…", *op. cit.*, p. 6. Adicionalmente. *Vid*. REINARES, F., "¿Cuál es la amenaza que el terrorismo yihadista supone actualmente para España?", en *Boletín Elcano*, nº 90 (2007), pp. 3-7.; JORDÁN, J., "Evolución organizativa de la militancia yihadista en España", en *Análisis del Real Instituto Elcano*, nº 12 (2014).

[737] La resolución anterior emitida por parte del Parlamento Europeo fue resultado, en cierta manera, de los acuerdos adoptados en la Sesión nº 3354 del Consejo de la Unión Europea, celebrada en diciembre de 2014, en la que los ministros concluyeron la necesidad urgente de adoptar la Directiva sobre los datos PNR, así como, en virtud del mandato del Consejo de Europa, instaron al susodicho Parlamento para que acelerara las negociaciones lo máximo posible.

la Decisión marco 2002/475/JAI del Consejo[738], concretamente respecto de los delitos catalogados como graves, incluidos en el Anexo II de la norma[739].

1.3. Contenido. Análisis de las UIP y su funcionamiento

La Directiva PNR gira sobre el eje fundamental de articular una serie de mecanismos orientados a garantizar la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de determinados delitos graves en el contexto de la Unión Europea, tal y como se contiene en su propia exposición de motivos. Para conseguir precisamente la consecución de los objetivos pretendidos, la norma opta por la creación de lo que ha venido a denominar como "Unidad de Información sobre los Pasajeros" (en adelante, UIP), que encontrándose ubicada en cada uno de los distintos Estados miembros —a excepción de Dinamarca—, se ha posicionado como la encargada de "gestionar" los respectivos datos PNR facilitados por parte de las respectivas compañías aéreas que operen sobre su espacio aéreo fronterizo[740].

No obstante, cabe destacar que las autoridades administrativas competentes nunca se han preocupado de implementar criterios para limitar la recogida de información, pues de cuanta más se dispusiera bajo su control y supervisión, mayor rendimiento se podía obtener de la misma. Un claro ejemplo de lo anterior lo vemos plasmado en la propia

---

[738] *Vid*. Decisión marco 2002/475/JAI del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo (2002/475/JAI).

[739] A continuación, se relaciona el contenido del Anexo II de la Directiva 2016/681, que incluye el listado de los delitos a que se refiere el artículo 3, apartado 9 de la misma, que incluye el tenor literal siguiente: 1. pertenencia a una organización delictiva, 2. trata de seres humanos, 3. explotación sexual de niños y pornografía infantil, 4. tráfico ilícito de estupefacientes y sustancias psicotrópicas, 5. tráfico ilícito de armas, municiones y explosivos, 6. corrupción, 7. fraude, incluido el que afecte a los intereses financieros de la Unión, 8. blanqueo del producto del delito y falsificación de moneda, con inclusión del euro, 9. delitos informáticos/ciberdelincuencia, 10. delitos contra el medio ambiente, incluido el tráfico ilícito de especies animales protegidas y de especies y variedades vegetales protegidas, 11. ayuda a la entrada y residencia ilegales, 12. homicidio voluntario, agresión con lesiones graves, 13. tráfico ilícito de órganos y tejidos humanos, 14. secuestro, detención ilegal y toma de rehenes, 15. robo organizado y a mano armada, 16. tráfico ilícito de bienes culturales, incluidas las antigüedades y las obras de arte, 17. falsificación y violación de derechos de propiedad intelectual o industrial de mercancías, 18. falsificación de documentos administrativos y tráfico de documentos administrativos falsos, 19. tráfico ilícito de sustancias hormonales y otros factores de crecimiento, 20. tráfico ilícito de materiales radiactivos o sustancias nucleares, 21. violación, 22. delitos incluidos en la jurisdicción de la Corte Penal Internacional, 23. secuestro de aeronaves y buques, 24. sabotaje, 25. tráfico de vehículos robados, 26. espionaje industrial.

[740] De conformidad con lo dispuesto en el artículo 3, apartado 1, de la Directiva 2016/681, la gestión de los datos PNR comprende su recogida, almacenamiento, procesamiento, intercambio y análisis oportuno. Es una cuestión importante, pues son las compañías aéreas las que suministran los datos de los pasajeros a las UIP, no siendo directamente estas últimas las que accedan directamente a las bases de datos de las distintas compañías aéreas, pudiendo recabar indiscriminadamente aquellos datos que considerasen relevantes.

evolución normativa de los distintos instrumentos comunitarios que se han ido sucediendo para regular la cuestión, dado que como indica Catalina Benavente, la propuesta de Decisión marco proponía la utilización de los datos PNR para la lucha contra el terrorismo y la delincuencia organizada; la propuesta de Directiva de 2011 para luchar contra delitos terroristas, delitos graves y delitos trasnacionales graves. En el Proyecto de Informe de febrero de 2015 se proponía limitar estos datos a la lucha contra los delitos trasnacionales graves, entre los que se incluían los delitos de terrorismo, siempre y cuando se diesen los requisitos previstos por la propia enmienda. En el Segundo Informe se concretaba la utilización de los datos PNR para los delitos terroristas y los delitos trasnacionales graves. Finalmente, la Directiva permite la utilización de los datos PNR para la lucha contra el terrorismo y para los delitos graves recogidos en el Anexo II[741] —que hemos reproducido—.

De esta manera, los riesgos que supone esta concentración de información y el uso que puede hacerse de la misma pone en verdadero jaque el derecho a la protección de los datos de carácter personal de los pasajeros como sujetos afectados, tal y como tuvo la ocasión de advertir el TJUE en su Dictamen 1/15, de 26 de julio de 2017, en relación con el proyecto de Acuerdo entre Canadá y la Unión Europea sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros, que se tendrá la oportunidad de examinar[742].

En idéntico sentido también se había postulado el SEPD, tanto inicialmente en 2011 cuando consideró que el contenido de la propuesta de Directiva PNR que se había formulado no daba cumplimiento a los requisitos de necesidad y proporcionalidad preceptuados por el artículo 8 de la CDFUE, el artículo 8 del CEDH y el artículo 16 del TFUE[743], como posteriormente en 2015, cuando señalaba expresamente sobre la nueva

[741] *Cfr*. CATALINA BENAVENTE, M. A., "La Directiva Europea…", *op. cit.*, pp. 5-6.

[742] *Vid*. Apartado 131 del Dictamen 1/15.

[743] *Vid*. SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, "Dictamen sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves, (2011/C 181/02)", de 25 de marzo de 2011, apdo. 10.

versión de la propuesta de Directiva PNR que los datos obtenidos únicamente podían utilizarse para los fines que se habían identificado explícitamente[744].

Sin perjuicio de lo anterior, podemos considerar entonces que los datos PNR se componen de información recogida y albergada por las propias compañías aéreas en aras de garantizar la correcta llevanza de su actividad de negocio, pero que no había sido verificada ni por la propia organización ni tampoco por ninguna autoridad competente. De hecho, una vez que los datos han sido debidamente recogidos, estos son remitidos a la UIP de cada Estado miembro a través del método *"push"* o de transmisión[745], que permite que las compañías aéreas remitan los datos PNR requeridos a la base de datos de la autoridad requirente[746]. Cabe destacar que en la Propuesta de Decisión marco de 2007 se había previsto en contraposición el método *"pull"* o de extracción[747], mediante el cual la autoridad requirente podía acceder al sistema de reservas de la compañía aérea y copiar los datos deseados en su propia base de datos[748].

Una vez culminado el proceso de transmisión descrito, las respectivas UIP disponían de un gran volumen de información que podían utilizar sin apenas restricciones o limitaciones[749]. De hecho, el texto de la Directiva PNR se limita a señalar únicamente al respecto que: "[c]ada Estado miembro establecerá o designará una autoridad competente para la prevención, detección, investigación o enjuiciamiento de los delitos de terrorismo y delitos graves, o una sucursal de esa autoridad, para actuar como su Unidad de Información sobre los Pasajeros (UIP)"[750].

---

[744] *Vid*. SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, "Second Opinion 5/2015 on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime", de 24 de septiembre de 2015, apdo. 24.

[745] *Vid*. Considerando 16 de la Directiva 2016/681.

[746] *Vid*. Artículo 3, apartado 7, de la Directiva 2016/681.

[747] *Vid*. Considerando 16 de la Directiva 2016/681.

[748] *Vid*. Artículo 2 de la Propuesta de Decisión marco de 2007.

[749] Esta cuestión fue una de las preocupaciones que el SEPD puso de manifiesto en su Dictamen de 2011, pues afirmaba que era preciso delimitar las amplias competencias de las que disponían las UIP, que se concretase su carácter y la composición de su personal integrante, así como que se implementaran una serie de garantías para evitar abusos, pues el autocontrol que se preveía debía complementarse con un control externo, de modo más estructurado. *Vid*. SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, "Dictamen sobre la propuesta de Directiva…", cit., apdos. 31-35.

[750] *Vid*. Artículo 4, apartado 1, de la Directiva 2016/681.

Las distintas competencias de las UIP a las que se viene aludiendo, se encuentran contendidas mínimamente en la Directiva PNR. Se puede citar, en primer lugar, la relativa a la realización de una evaluación general sobre todos los datos de los pasajeros que efectúan un vuelo de llegada o salida a alguno de los países integrantes de la Unión Europea, con la intención de que las autoridades competentes del Estado miembro en cuestión puedan proceder a su correspondiente análisis y examen. Una vez finalizado este, pueden dar traslado del caso a la Europol, en aquellos supuestos en los que el pasajero pueda estar relacionado con delitos graves o de terrorismo[751].

Respecto de este punto, cabe precisar que dichas evaluaciones se realizan a partir del tratamiento automatizado de grandes volúmenes de datos, sobre la base de una serie de modelos y criterios que han sido previamente determinados por parte de las autoridades competentes. Su tratamiento puede implicar incluso que lleguen a combinarse con otras bases de datos adyacentes[752]. Estos análisis pueden incluir hasta 19 categorías de datos diferentes, de conformidad con lo establecido en el Anexo I de las directrices de la Organización de la Aviación Civil Internacional (OACI) relativas a los datos del PNR[753], yendo desde datos meramente identificativos hasta observaciones subjetivas que puedan incluirse en los formularios de reserva y embarque de las diferentes aerolíneas[754]. Quedan excluidos, en todo caso, los criterios que se basen en el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud o la vida u orientación sexual de la persona[755].

En este mismo sentido, el TJUE apunta que aun cuando algunos de los datos del PNR, aisladamente considerados, no parezcan poder revelar información importante sobre la vida privada de las personas afectadas, no deja de ser cierto que, conjuntamente

---

[751] *Vid*. Artículo 6, apartado 2, letra a), de la Directiva 2016/681.

[752] Sobre este punto, cabe recordar las manifestaciones efectuadas por parte del SEPD al respecto, en que aparte de indicar que la propuesta de Directiva de PNR no da cumplimiento a las consideraciones establecidas en la Sentencia DRI, alienta al legislador comunitario para que defina aquellos supuestos específicos en los que las autoridades nacionales competentes van a poder acceder a los datos PNR y los correspondientes límites, con la intención de garantizar el respeto por el contenido de los artículos 7 y 8 de la CDFUE. *Vid*. SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, "Second Opinion 5/2015…", cit., apdos. 25-27.

[753] *Vid*. Apartado 156 del Dictamen 1/15.

[754] *Ibidem*, cdo. 121

[755] *Vid*. Artículo 6, apartado 4, de la Directiva 2016/681.

considerados, dichos datos pueden revelar, entre otros extremos, un itinerario de viaje completo, hábitos de viaje, relaciones existentes entre dos o varias personas, así como información sobre la situación económica de los pasajeros aéreos, sus hábitos alimentarios o su estado de salud, y podrían incluso proporcionar datos sensibles sobre dichos pasajeros[756]. Para mitigar este riesgo apuntado, el SEPD manifestaba la necesidad de que el sistema de recopilación de datos debía limitarse a criterios específicos como los datos pertenecientes a un período de tiempo particular, una zona geográfica concreta o un círculo de personas específicas que pudieran estar involucradas, de una forma u otra, en un delito grave o de terrorismo[757]. Prácticas que estarían en consonancia con el criterio marcado por parte del Alto Tribunal comunitario en la Sentencia *Digital Rights Ireland* (en adelante, Sentencia DRI)[758].

Esta primera evaluación general contemplada dentro del abanico competencial de las UIP puede entenderse como un ejercicio de vigilancia masiva e indiscriminada sobre la totalidad del flujo de datos perteneciente a los distintos pasajeros que circulan por el alcance territorial de la Unión Europea. Dicha concepción se introdujo por primera vez en la propuesta de Directiva de PNR de 2011, generando bastante rechazo por diversos actores[759]. Pese a ello, vemos como finalmente la redacción se mantuvo, aunque con la inclusión de alguna garantía adicional que, *a priori*, debería de permitir que su ejercicio respetase el contenido de otros derechos fundamentales —como el relativo a la protección de los datos personales[760]—. Por lo que en aquellos supuestos en los que se identificasen posibles personas de interés[761], la transmisión de los datos de PNR "solo se llevará a cabo

[756] *Vid*. Apartado 128 del Dictamen 1/15.

[757] *Vid*. SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, "Second Opinion 5/2015…", cit., apdo. 22.

[758] *Vid*. Apartado 59 de la Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 8 de abril de 2014, dictada en los asuntos acumulados C-293/12 y C-594/12.

[759] *Vid*. CATALINA BENAVENTE, M. A., "La Directiva Europea…", *op. cit.*, p. 7.

[760] Siguiendo con las consideraciones establecidas por el TJUE en la Sentencia DRI, en aras de intentar salvaguardar la protección de este derecho, el artículo 6, apartado 8, de la Directiva 2016/681, dispone que: "[E]l almacenamiento, el tratamiento y análisis de los datos PNR por parte de la UIP se realizará exclusivamente en uno o varios lugares seguros, dentro del territorio de los Estados miembros".

[761] Como Cañabate Pérez afirma: "La Directiva, que como vemos reconoce los «falsos positivos», ha creado una categoría jurídica similar a la «*person of interest*» del derecho estadounidense, es decir, alguien que no es sospechoso en una investigación previa, pero que su comportamiento encaja con un patrón predeterminado que lleva a las autoridades a recabar más información con el fin de prevenir o investigar posibles acciones delictivas. El hecho de que estimativamente unos trescientos millones de pasajeros en la

tras un análisis particular de cada caso y, en caso de tratamiento automatizado de los datos PNR, tras una revisión individualizada por medios no automatizados"[762].

Siguiendo con las competencias de las UIP enunciadas, procede destacar, en segundo lugar, que se les permitirá responder en cada caso particular a las peticiones efectuadas por parte de las autoridades competentes —siempre que se encuentren debidamente razonadas y dispongan de suficiente base—. Todo ello con la intención de que se suministren y traten los datos PNR en casos específicos a efectos de prevención, detección, investigación y enjuiciamiento de delitos graves y de terrorismo, facilitando así a las autoridades competentes o, en su caso, a Europol, los resultados de dicho tratamiento[763]. En tercer y último lugar, las UIP pueden analizar los datos PNR en cuestión, a los efectos de "actualizar o establecer nuevos criterios que deben utilizarse en las evaluaciones realizadas en virtud del apartado 3, letra b), a fin de identificar a toda persona que pueda estar implicada en un delito de terrorismo o delito grave"[764].

Una vez discernidas las supuestas "limitadas" competencias de las que disponen las UIP a tenor del texto de la propia Directiva 2016/681, conviene destacar el enfoque de recogida de información descentralizada por el que opta la norma. Como señala Brouwe[765], puede considerarse la mejor opción en aras de garantizar la protección de los datos personales, así como de minimizar los costes de configuración y funcionamiento. Pero, en cualquier caso, serán los Estados miembros los que deberán sufragar los costes del uso, la conservación y el intercambio de los datos PNR[766], así como desempeñar un rol activo en el intercambio de información a través de sus respectivas UIP, a los efectos

UE sean objeto de tratamiento por los sistemas que estamos analizando no les sitúa en absoluto dentro de esta categoría de «persona de interés». No obstante, les convierte en integrantes de un fichero policial durante cinco años, y en objeto de una investigación automatizada, pero investigación, a fin de cuentas". *Cfr*. CAÑABATE PÉREZ, J., "La Directiva 2016/681…", *op. cit.*, p. 12.

[762] *Vid*. Artículo 6, apartado 6, de la Directiva 2016/681.

[763] *Vid*. Artículo 6, apartado 2, letra b), de la Directiva 2016/681.

[764] *Vid*. Artículo 6, apartado 2, letra c), de la Directiva 2016/681.

[765] *Vid*. BROUWE, E., "The EU Passenger name record System and Human Rights: Transferring passenger data or passenger freedom", en *CEPS Working Document*, nº 320 (2009), p. 5.

[766] *Vid*. Considerando 14 de la Directiva 2016/681.

de facilitar dicho intercambio y garantizar la interoperabilidad —entre los distintos Estados miembros, y en su caso, la Europol[767]—.

Respecto del intercambio de información sobre los datos PNR entre los diferentes Estados miembros, resulta oportuno indicar que la Directiva 2016/681 se construye a partir de dos fundamentos básicos según se desprende del literal de su contenido. Por un lado, la facultad de las que disponen las UIP de solicitarse datos entre las mismas como parte integrante de la Unión Europea[768]. Por otro lado, la obligación que ostentan estos organismos de atender los requerimientos efectuados por parte de cualquier otra UIP perteneciente a un Estado miembro —sin dilación indebida—. En este sentido, la solicitud deberá estar suficientemente motivada, pudiéndose basar para ello en cualquier elemento de los datos o en una combinación de estos, según estime necesario la UIP solicitante en cada caso en particular[769].

Ahora que se han expuesto las condiciones en que debe de llevarse a cabo el intercambio de "información pertinente"[770], resulta oportuno abordar los condicionantes que establece la Directiva PNR en relación con el intercambio de datos que se produce entre las UIP y los distintos Estados miembros hasta la Europol[771]. Así pues, conviene reproducir el contenido del considerando 23 de la Directiva PNR, cuando afirma que:

---

[767] Como Cañabate-Pérez afirma: "La Directiva PNR establece que debe garantizarse el intercambio seguro de información sobre datos PNR entre los Estados miembros a través de cualquiera de los canales existentes de cooperación entre las autoridades competentes de los Estados miembros, así como en particular Europol, a través de la Aplicación Segura de la red de Intercambio de Información (SIENA) de Europol (CDO 24 Directiva PNR). En este sentido, la EDPS ya había recomendado en su Opinión que las agencias estatales encargadas de la gestión del PNR se alineen con el régimen aplicable por Europol para restringir las condiciones de acceso. Se debe señalar que Europol está sujeta a escrutinio judicial, después del Tratado de Lisboa de 2009, pues sus acciones están revisadas por el TJUE". *Cfr*. CAÑABATE-PÉREZ, J., "La Directiva 2016/681…", *op. cit.*, pp. 23-24.

[768] *Vid*. Artículo 9, apartado 1, de la Directiva 2016/681.

[769] *Vid*. Artículo 9, apartado 2, de la Directiva 2016/681.

[770] El intercambio de información pretendido deberá resultar pertinente, de conformidad con lo dispuesto el artículo 87 TFUE, apartado 2, letra a), en el ámbito de la prevención, detección e investigación de infracciones penales, dado que puede incluir datos personales, en cuanto permite "la recogida, almacenamiento, tratamiento, análisis e intercambio de información pertinente". *Vid*. Apartados 98 y 99 del Dictamen 1/15.

[771] Sobre este punto, no es cuestión baladí recordar la existencia del Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo, creándose la Agencia de la Unión Europea para la Cooperación Policial (Europol) con objeto de apoyar la cooperación entre las autoridades policiales de la Unión, sustituyendo la Europol creada bajo el acervo de la Decisión 2009/371/JAI.

"[L]os Estados miembros deben intercambiar y a través de Europol los datos PNR que reciban cuando ello se considere necesario para la prevención, detección, investigación o enjuiciamiento de delitos de terrorismo o delitos graves. Las UIP deben transmitir, cuando proceda y sin demora, los resultados del tratamiento de datos PNR a las de otros Estados miembros, para ulterior investigación. Las disposiciones de la presente Directiva se entienden sin perjuicio de otros instrumentos de la Unión relativos al intercambio de información entre la policía u otras autoridades policiales y las judiciales, incluida la Decisión 2009/371/JAI del Consejo[772] y la Decisión marco 2006/960/JAI[773]. Este intercambio de datos PNR entre las autoridades policiales y judiciales debe regirse por las normas de cooperación policial y judicial y no socavar el alto nivel de protección de la intimidad y de los datos personales exigido por la Carta, el Convenio nº 108 y el CEDH".

Adicionalmente a lo anterior, la Directiva PNR permite con carácter excepcional, que cuando sea necesario acceder a los datos PNR para responder a una amenaza concreta y real relacionada con delitos graves o de terrorismo, la UIP de un Estado miembro puedan a solicitar a la UIP de otro Estado miembro acceder a los datos PNR —de conformidad con el art. 8, apartado 5—, y facilitarlos a la UIP solicitante[774]. Pues como señala Catalina Benavente —tomando en consideración lo establecido por la Comisión de Transportes y Turismo para la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (LIBE, por sus siglas en inglés[775]—), la Directiva, sin embargo, adolece en este punto de una falta de precisión que debería ser subsanada por la regulación de los Estados miembros, pues hubiera sido necesario que se estableciese expresamente que las solicitudes de transmisión se limitasen estrictamente a los datos

[772] *Vid*. Decisión 2009/371/JAI del Consejo, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol) (DO L 121 de 15.5.2009), p. 37.

[773] *Vid*. Decisión marco 2006/960/JAI del Consejo, de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea (DO L 386 de 29.12.2006), p. 89.

[774] *Vid*. Artículo 9, apartado 4, de la Directiva 2016/681.

[775] *Vid*. Opinión de la Comisión de Transportes y Turismo para la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo, sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves (A7-0150/213), de fecha 14 de diciembre de 2011.

PNR necesarios en el caso específico para el cumplimiento de los fines perseguidos, así como que dichas solicitudes se efectuasen preferiblemente por escrito[776].

Como último aspecto a destacar sobre el contenido del intercambio de información sobre los datos PNR entre los diferentes Estados miembros, resulta oportuno analizar uno de los puntos clave del texto por lo que a los efectos de este trabajo interesa. Este no es otro que la previsión que se contiene detallada en la Directiva 2016/681 respecto de los movimientos de datos de PNR a terceros países fuera del ámbito de la Unión Europea[777], pues estos únicamente podrán llevarse a término por parte del Estado miembro en cuestión, siempre que se cumplan una serie de condicionantes recogidos en la Decisión marco 2008/977/JAI[778] —actualmente derogada, por lo que dicha remisión debe entenderse efectuada a la Directiva (UE) 2016/680—[779].

No resulta óbice destacar que la Directiva PNR, en consonancia con los pronunciamientos efectuadas por el TJUE[780], limita la capacidad de los Estados miembros de transmitir los datos de PNR a las autoridades competentes de terceros países, únicamente en aquellos supuestos en los que se dé cumplimiento a las condiciones previstas en la propia Directiva, así como exclusivamente después de asegurarse de que

[776] *Vid*. CATALINA BENAVENTE, M. A., "La Directiva Europea…", *op. cit.*, p. 10.

[777] *Vid*. Artículo 11 de la Directiva 2016/681.

[778] *Vid*. Decisión marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (DO L 350 de 30.12.2008), p. 60.

[779] *Vid*. Artículos 35 y ss. de 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.

[780] A este respecto, el TJUE manifiesta que el "derecho a la protección de los datos de carácter personal exige, en concreto, que, en caso de transferencia de tales datos desde la Unión a un país tercero, quede garantizada la continuidad del elevado nivel de protección de los derechos y libertades fundamentales conferido por el Derecho de la Unión. Aunque los medios encaminados a garantizar tal nivel de protección puedan ser diferentes de los aplicados en la Unión para garantizar el cumplimiento de las exigencias derivadas del Derecho de la Unión, tales medios deben ser eficaces en la práctica para asegurar una protección sustancialmente equivalente a la garantizada en la Unión (véase, por analogía, la sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartados 72 a 74)", de manera que "la transferencia de datos personales, como los datos del PNR, de la Unión a un país tercero únicamente puede verificarse legalmente si en ese país existen normas que garanticen un nivel de protección de los derechos y libertades fundamentales sustancialmente equivalente al garantizado en la Unión (véase, en ese sentido, la sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartados 68 y 74)". *Vid*. Apartados 134 y 93, respectivamente, del Dictamen 1/15.

la utilización de los datos PNR prevista por los receptores se ajusta a las condiciones y garantías que han posibilitado el intercambio de información. En caso contrario, se estarían violentando las previsiones efectuadas por el RGPD[781] en lo relativo a las transferencias internacionales de datos personales, las cuales se ha tenido la oportunidad de analizar en anteriores capítulos.

Asimismo, es preciso observar que, como bien recuerda el TJUE, "dado el importante papel que cumple la protección de los datos personales en relación con el derecho fundamental al respeto de la vida privada, así como el gran número de personas cuyos derechos fundamentales pueden ser vulnerados en caso de transferencia de datos personales a un tercer país que no garantice un nivel de protección adecuado, la facultad de apreciación de la Comisión sobre el carácter adecuado del nivel de protección garantizado por un tercer país queda reducida, por lo que se debe ejercer un control estricto de las exigencias derivadas del artículo 25 de la Directiva 95/46, entendido a la luz de la Carta (véase por analogía la sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 47 y 48)"[782].

En consecuencia, la utilización de los datos de PNR que efectúan las distintas UIP de los Estados miembros siguiendo con los protocolos y procedimientos que se han ido detallando permiten la discriminación de aquellos individuos que no son susceptibles de ser considerados "de interés" a los efectos de una investigación relacionada con delitos graves o vinculados al terrorismo. Se trata pues de una cuestión controvertida, generadora de una serie de preocupaciones que incluso la propia Directiva 2016/681 ya recoge en su Exposición de motivos, cuando afirma que, en consideración con el derecho a la protección de datos personales y el derecho a la no discriminación, no debe tomarse ninguna decisión que pudiera tener efectos jurídicos adversos para una persona o afectarle gravemente en razón únicamente del tratamiento automatizado de datos PNR[783].

Contenido. Análisis desde la perspectiva de protección de datos

Llegados a este punto, debe afirmarse que el respeto por el cumplimiento de la legislación aplicable en materia de protección de datos en el seno de la Unión Europea

[781] *Vid*. Artículo 44 y ss. del Reglamento General de Protección de Datos.

[782] *Vid*. STJUE. Asunto C-362/14 (Schrems I), cit., apdo. 78.

[783] *Vid*. Considerando 20 de la Directiva 2016/681.

siempre ha sido una preocupación, aspecto que la Directiva PNR constantemente se encarga de recordar[784]. Ello es así hasta el punto de que dicha cuestión se menciona en diversas ocasiones, siendo uno de los momentos en los que más evidentemente se refleja dicha consideración en su considerando 15. El mismo aboga expresamente por la salvaguarda de dos derechos fundamentales, en particular, el derecho a la intimidad y el ya referido relativo a la protección de datos de carácter personal, con base en las exigencias establecidas en la CDFUE, el Convenio 108 y el CEDH, las cuales han sido abordadas con anterioridad.

En este sentido, resulta evidente señalar como la sistemática de funcionamiento del PNR pone en jaque precisamente la salvaguarda del derecho a la protección de los datos de carácter personal, pues la recogida masiva e indiscriminada de información que se efectúa difícilmente encuentra encaje entre las exigencias regulatorias establecidas al respecto por parte de la legislación comunitaria. No se trata de ninguna novedad, sino que dicha problemática ya fue puesta de manifiesto en su momento por parte del SEPD en la primera revisión efectuada sobre la propuesta de Directiva PNR, cuando apuntaba que: "[E]l único objetivo que […] cumpliría los requisitos de transparencia y proporcionalidad, sería la utilización caso por caso de los datos PNR, tal como se establece en el artículo 4, apartado 2, letra c), aunque solo en los casos en que se establezca una amenaza grave y determinada a través de indicadores concretos"[785]. A lo que posteriormente, el GT29 se

[784] El mismo considerando 15 de la Directiva 2016/681 menciona que las listas PNR no deben basarse en el origen racial o étnico, religión o convicciones, opiniones políticas o de cualquier otro tipo, la pertenencia a un sindicato, la salud, vida u orientación sexual. A este respecto, el TJUE apuntaba que: "La comunicación de datos de carácter personal a un tercero, como una autoridad pública, constituye una injerencia en el derecho fundamental consagrado en el artículo 7 de la Carta, cualquiera que sea la utilización posterior de la información comunicada. Lo mismo puede decirse de la conservación de los datos de carácter personal y del acceso a esos datos con vistas a su utilización por parte de las autoridades públicas. A este respecto, carece de relevancia que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia (véanse, en este sentido, las sentencias de 20 de mayo de 2003, Österreichischer Rundfunk y otros, C-465/00, C-138/01 y C-139/01, EU:C:2003:294, apartados 74 y 75; de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 33 a 35, y de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 87)". *Vid*. Apartado 124 del Dictamen 1/15.

[785] *Vid*. SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, "Dictamen sobre la propuesta de Directiva…", cit., apdo. 17.

pronunciaría en el mismo sentido en 2015, a través de un comunicado remitido al presidente del LIBE[786].

Por ende, en las próximas líneas de redacción, se pretenderá profundizar en las principales problemáticas que la ejecución del sistema PNR supone para la salvaguarda de los derechos fundamentales vinculados a la intimidad y la protección de los datos de carácter personal. Se puede destacar, en primer lugar, la necesidad de esclarecer los criterios que se utilizan para determinar la identificación de los "sujetos de interés", pues la metodología que se lleva a cabo para realizar esta elaboración de perfiles mediante decisiones automatizadas[787] —ya sea a través de criterios preestablecidos o patrones de comportamiento—, tiene una afectación directa sobre la salvaguarda del último de los derechos aludidos.

Es por ello que, consciente sobre los peligros que se podían derivar, el SEPD se pronunció en la segunda revisión de la propuesta de Directiva PNR sobre las reglas que resultaban aplicables sobre los sistemas automatizados de tratamiento de datos personales[788]. Para ello, trajo a colación diversas consideraciones que con anterioridad el TJUE ya había tenido la oportunidad de reproducir en la Sentencia DRI[789], cuyo énfasis se centraba básicamente en la necesidad de establecer reglas específicas y adaptadas a las

---

[786] *Vid*. Comunicado efectuado por el GT29 al presidente del LIBE, en fecha 12 de junio de 2012. Consultado el 28.06.2020 desde: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120612_letter_to_libe_eu-pnr_en.pdf.

[787] *Vid*. A este respecto, resulta oportuno traer a colación el contenido preceptuado en el artículo 22 del RGPD cuando aborda las decisiones individuales automatizadas, incluida la elaboración de perfiles, estableciendo el siguiente literal: "1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. 2. El apartado 1 no se aplicará si la decisión: a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o c) se basa en el consentimiento explícito del interesado. 3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión. 4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado".

[788] *Vid*. SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, "Second Opinion 5/2015…", cit., apdos. 28-32.

[789] *Vid*. Apartado 66 de la Sentencia DRI.

distintas volumetrías de datos personales objeto de tratamiento, al posible carácter sensible de los mismos, así como a evitar que estos fueran accesibles por parte de terceros no autorizados, vulnerándose así la protección y seguridad que su utilización debe de conllevar asociada.

Como bien señala Cañabate-Pérez sobre este punto, la Directiva no precisa con claridad y transparencia estos criterios, haciendo una peligrosa concesión al ambiguo e indeterminado concepto de "automatizado", en el cual, como hemos señalado, radica la esencia del sistema. Y abundando en este aspecto, también hubiera sido deseable que la Directiva PNR apostase claramente por principios destacados por el RGPD como la *Privacy by Design* o la *Privacy by Default*[790].

En cualquier caso, es preciso apuntar que el TJUE, en su Dictamen 1/15 reproducido, también se hacía eco de los riesgos que suponen estos análisis automatizados efectuados sobre los datos del PNR para los derechos y libertades de los afectados, los cuales dependen fundamentalmente de dos factores esenciales, desde su punto de vista. Por un lado, los modelos y criterios preestablecidos. Por otro lado, las bases de datos en que se apoye esta tipología de tratamientos.

Así pues, el Alto Tribunal, en el marco del Acuerdo con Canadá, entiende respecto del primer factor que estos deberían de ser específicos y fiables, de modo que permitan alcanzar resultados que seleccionen individuos sobre los que podría recaer una "sospecha razonable" de participación en actividades terroristas o delitos graves de carácter transnacional y que, además, no ostenten carácter discriminatorio. Asimismo, en relación con el segundo factor —esto es, las bases de datos con las que se cotejan los datos PNR—, que las mismas deben ser fiables, estar actualizadas y limitarse a bases de datos utilizadas por Canadá en relación con la lucha antiterrorista y los delitos graves de carácter transnacional[791].

El TJUE sigue añadiendo al respecto que los referidos análisis automatizados siempre conllevan un cierto margen de error identificando "falsos positivos". En estos casos, cualquier resultado positivo que se detecte como consecuencia de la utilización de este sistema, deberá de revisarse al caso particular mediante medios no automatizados,

[790] *Cfr*. CAÑABATE-PÉREZ, J., "La Directiva 2016/681…", *op. cit.*, p. 16.

[791] *Vid*. Apartado 172 del Dictamen 1/15.

antes de adoptar cualquier tipo de medidas que pueda afectar colectivamente a los derechos y libertades de los pasajeros aéreos afectados[792].

Si a lo anterior le adicionamos también que no existe ningún control externo sobre la utilización del esquema expuesto del PNR por parte de las UIP, se hace todavía más evidente que estamos ante un escenario posiblemente flagrante de vulneración del contenido preceptuado por parte del artículo 8, apartado 2, del CEDH y el artículo 52, apartado 1, de la CDFUE. Reflexión que también había sido reivindicada por parte del TJUE en la Sentencia DRI[793] o en su Dictamen 1/15[794], así como también por parte del SEPD en la primera[795] y segunda[796] revisión sobre la propuesta de Directiva PNR. Incluso una parte sector doctrinal[797] había abogado por la creación de una autoridad judicial específica que tratase las cuestiones derivadas del mecanismo PNR en aras de garantizar un mayor respeto sobre los derechos fundamentales de los afectados, haciendo un ejercicio de analogía con el modelo norteamericano consagrado por el FISC[798], el cual se ha tenido la oportunidad de analizar.

Siguiendo con las problemáticas del mecanismo PNR que veníamos apuntando desde el prisma de la protección de datos de carácter personal. En segundo lugar, podemos abordar que la propia Directiva 2016/681 recoge la necesidad de arbitrar fórmulas para que el interesado pueda hacer valer el ejercicio efectivo de sus derechos de conformidad con lo establecido en la legislación comunitaria —y a su vez, en concordancia con la interna de los Estados miembros—. Se le reconocen una serie de mecanismos para solicitar y, en su caso, obtener, de forma gratuita, el acceso a sus datos personales, así

[792] *Ibidem*, apdo. 173.

[793] *Vid*. Apartado 60 a 62 de la Sentencia DRI.

[794] *Vid*. Apartado 232, apartado tercero, letra g), del Dictamen 1/15.

[795] *Vid*. SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, "Dictamen sobre la propuesta de Directiva…", cit., apdo. 18.

[796] *Vid*. SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, "Second Opinion 5/2015…", cit., apdos. 42-46.

[797] *Vid*. BROUWE, E., "The EU Passenger…", *op. cit.*

[798] *Vid*., entre otros: JAEGERA, P. T., BERTOTA, J. C., MCCLUREA, C. R., "The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act", en *Government Information Quarterly*, Vol. 20 (2003), Issue 3, pp. 295-314.

como su rectificación o supresión y la limitación de su tratamiento[799], incluyéndose, además, el derecho a presentar una reclamación[800].

En este sentido, el TJUE también tuvo la oportunidad de abordar la cuestión en su Dictamen 1/15, pues recordando la importancia del respeto de las vicisitudes establecidas por el artículo 8, apartado 2 de la CDFUE relativo a la salvaguarda del derecho fundamental a la vida privada[801], declara que, para garantizar el respeto de esos derechos[802], es importante que los pasajeros aéreos sean informados de la transferencia de sus datos y de la utilización de los mismos, siempre que tal comunicación no pueda perjudicar a las investigaciones llevadas a cabo por las autoridades[803]. En efecto, tal información resulta, de hecho, necesaria para que los pasajeros aéreos puedan ejercer su derecho a solicitar el acceso a los datos del PNR que les conciernan y, en su caso, su rectificación, así como a interponer, con arreglo al artículo 47, párrafo primero, de la Carta, un recurso efectivo ante un tribunal[804].

En tercer lugar, vinculado directamente con el punto anterior, conviene destacar la posible falta de observancia respecto del principio de proporcionalidad de la que adolece la propia Directiva PNR. Ello puede constatarse al interpretar su contenido a la luz de lo preceptuado por el artículo 52, apartado 1 de la CDFUE, el cual establece que únicamente podrán introducirse limitaciones a los derechos y libertades cuando estas resulten necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás[805].

---

[799] *Vid*. Considerando 40 de la Directiva 2016/681.

[800] *Ibidem*, cdo. 42.

[801] *Vid*. Apartado 219 del Dictamen 1/15.

[802] *Vid*. Sentencia del TJUE (Sala Tercera), de 7 de mayo de 2009, en el asunto C-553/07, que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 234 CE, por el Raad van State (Países Bajos), mediante resolución de 5 de diciembre de 2007, recibida en el Tribunal de Justicia el 12 de diciembre de 2007, en el procedimiento entre College van burgemeester en wethouders van Rotterdam y M.E.E. Rijkeboer, apartado 49. Consultado el 20.08.2020 desde: http://curia.europa.eu/juris/document/document.jsf;jsessionid=BA9F32826A720B236A571E7CA51636D1?text=&docid=74028&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=8511754.

[803] *Vid*. Apartado 224 del Dictamen 1/15.

[804] *Ibidem*, apdo. 220.

[805] *Ibidem*, apdo. 138.

Por lo que cabe añadir, en consonancia con la jurisprudencia emanada por parte del TJUE, que, para poder cumplir este requisito, la normativa controvertida que conlleve la injerencia sobre los derechos y libertades debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso[806].

En particular, afirma el Alto Tribunal en su Dictamen 1/15, que dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. Si a lo anterior le adicionamos que los datos en cuestión podrían encontrarse clasificados como categorías especiales de datos personales, así como que los mismos podrían ser sometidos a un tratamiento automatizado, la necesidad de disponer de las garantías reforzadas a las que alude el TJUE reviste de especial importancia[807].

Teniendo en cuenta lo anterior, y en concordancia con lo que también había tenido la oportunidad de señalar el SEPD en la segunda revisión de la propuesta de Directiva PNR, cabe cuestionar sustancialmente la validez de dicha sistemática para afrontar los nuevos retos vinculados a la comisión de delitos graves y los relativos al terrorismo. El Supervisor europeo mantiene que, según los elementos disponibles en el momento de sucesión del pronunciamiento, el borrador de la norma no había tenido en cuenta todas las exigencias preceptuadas al respecto por parte de la jurisprudencia comunitaria emanada del TJUE, pues sostenía la existencia de mecanismos alternativos con una tasa de efectividad superior a la alcanzada mediante la utilización de los esquemas PNR.

En cuarto y último lugar, conviene reproducir las vicisitudes que integra la Directiva PNR sobre los periodos de conservación de los datos, dado que se trata de una cuestión controvertida que ha ido generando interesantes debates al respecto. Pese a que

---

[806] Al respecto, Sentencias del TJUE, de 16 de diciembre de 2008, Satakunnan Markkinapörssi y Satamedia, en el asunto C-73/07, apdo. 56; de 8 de abril de 2014, Digital Rights Ireland y otros, en los asuntos acumulados C-293/12 y C-594/12, apdos. 51-55; de 6 de octubre de 2015, Schrems, en el asunto C-362/14, apdo. 92; y de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros, en los asuntos C-203/15 y C-698/15, apdos. 96, 103, 109 y 117. *Ibidem*, apdos. 140.

[807] *Ibidem*, apdo. 141.

el texto de la norma establece que dicho periodo deberá de ser necesario y proporcional a las finalidades de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves[808], su artículo 12 fija el plazo de conservación de los datos PNR desde su transmisión a la UIP del Estado miembro pertinente en cinco años. Una vez finalizados los primeros seis meses desde dicha transmisión, los datos personales obtenidos deberán ser despersonalizados mediante el enmascaramiento de aquellos que permitan identificar de manera directa al sujeto titular de los mismos[809].

Transcurrido el periodo mencionado, la Directiva PNR únicamente permite la divulgación de los datos PNR completos cuando se dé cumplimiento a las finalidades previstas por la propia norma, así como cuando así se haya aprobado por parte de una autoridad judicial o, en su defecto, por parte de alguna otra autoridad nacional competente. Todo ello, a los efectos de verificar si se cumplen los condicionantes necesarios para efectuar la divulgación conforme al derecho nacional, con sujeción a la información y revisión *a posteriori* del responsable de la protección de datos de la UIP[810]. Como Catalina Benavente manifiesta: "Esta excepción que, en nuestra opinión, tiene todo su sentido, debería no obstante precisarse un poco más, para evitar que con la transmisión de datos PNR a las autoridades competentes de los Estados miembros, no se controle la conservación real de los datos PNR"[811].

Los Estados miembros se asegurarán de que los datos PNR sean suprimidos de modo permanente al finalizar el período a que se refiere el artículo 12. Esta obligación se entenderá sin perjuicio de aquellos casos en que se hayan transferido determinados datos PNR a una autoridad competente y se estén utilizando en el marco de un asunto en particular, a los efectos de prevenir, detectar, investigar o enjuiciar los actos de terrorismo

[808] *Vid*. Considerando 40 de la Directiva 2016/681.

[809] A continuación se reproduce el literal del artículo 12, apartado 2, de la Directiva PNR, cuando se refiere a aquellos datos que permitan identificar directamente a su titular: "a) nombre(s) y apellido(s), incluidos los de otros pasajeros que figuran en el PNR y número de personas que figuran en el PNR que viajan juntas; b) dirección y datos de contacto; c) todos los datos sobre el pago, incluida la dirección de facturación, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el PNR, o a cualquier otra persona; d) información sobre viajeros asiduos; e) observaciones generales, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el PNR, y f) toda la API recopilada".

[810] *Vid*. Artículo 12, apartado 3, de la Directiva 2016/681.

[811] *Vid*. CATALINA BENAVENTE, M. A., "La Directiva Europea…", *op. cit.*, p. 10.

o delitos graves, en cuyo caso la conservación de los datos por la autoridad competente se regirá por la legislación nacional aplicable[812].

De esta manera, los resultados del tratamiento serán conservados por la UIP únicamente durante el tiempo necesario para informar de un resultado positivo a las autoridades competentes y a las UIP de otros Estados miembros. Cuando el resultado de un tratamiento automatizado, tras un examen individual por medios no automatizados, arroje un resultado negativo, este se podrá almacenar para evitar falsos resultados positivos mientras los datos de base no se hayan eliminado. En cualquier caso, como bien señala Pérez-Luño, este artículo aparece como una cláusula que corrobora el interés de la Unión Europea por garantizar el derecho al olvido estableciendo un plazo máximo para la conservación de los datos[813].

Sobre este aspecto, el TJUE también ha tenido ocasión de pronunciarse, abogando por limitar la conservación de los datos del PNR tras la partida de los pasajeros aéreos a los de aquellos que pudieran presentar indicios objetivos y suficientes que fueran susceptibles de entrañar un riesgo en materia de lucha contra el terrorismo y los delitos graves de carácter transnacional. Aspecto que entraría en colisión directa con el contenido propio de la Directiva PNR[814].

En suma, podemos advertir también que la transposición en España de dicha Directiva PNR se ha culminado con la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, en los que, como el propio Preámbulo indica, se compone de tres capítulos, treinta y cuatro artículos, seis disposiciones adicionales y cuatro disposiciones finales. Su ámbito de aplicación se centra en regular, en primera instancia, la transferencia de los datos PNR por parte de las compañías aéreas y otras entidades obligadas. En segunda instancia, la recogida, el tratamiento y la protección de esos datos, su transmisión a las autoridades competentes y el intercambio de dichos datos con otros Estados miembros, Europol y

[812] *Vid*. Artículo 12, apartado 4, de la Directiva 2016/681.

[813] *Vid*. PÉREZ-LUÑO ROBLEDO, E., "La nueva normativa…", *Derechos y libertades, op. cit.,* p. 233.

[814] *Vid*. Apartado 232.3, letra d), del Dictamen 1/15.

terceros Estados; para, por último, designar la Unidad de Información sobre Pasajeros española y establecer un régimen sancionador.

Teniendo en cuenta lo anterior, se puede concluir afirmando que la Directiva PNR debería estar dotada de criterios de Disposición derogatoria más precisos que ayudasen a dotar de seguridad jurídica el marco normativo comunitario y nacional relativo a esta materia. En consonancia con las consideraciones vertidas por el propio TJUE[815], la utilización de los datos PNR por las respectivas UIP de los Estados miembros —tanto durante la estancia de los pasajeros en un determinado país como tras su salida de este—, así como toda comunicación de dichos datos a otras autoridades, debe someterse al cumplimiento de una serie de requisitos materiales y procedimentales basados en criterios objetivos.

Al mismo tiempo, también deberá supeditarse esa utilización y comunicación —salvo supuestos de urgencia debidamente justificados—, a un control previo efectuado, bien por un órgano judicial, bien por una entidad administrativa independiente, cuya decisión por la que se autoriza la utilización se adopte a raíz de una solicitud motivada de esas autoridades, presentada, en particular, en el marco de procedimientos de prevención, de descubrimiento o de acciones penales.

En este sentido, resulta oportuno traer a colación las reflexiones realizadas por Cañabate-Pérez, cuando señala que: "Se debe concluir que el sistema PNR no cumple plenamente con las exigencias de la Carta y del RGPD, y así lo ha apuntado el EDPS en sus opiniones, y el TJUE en resoluciones como la sentencia DRI o en el Dictamen 1/15"[816]. Adicionalmente sigue apuntado que: "[…] Se ha producido un desequilibrio a favor de la seguridad que implica la asunción de la doctrina americana involucionista de derechos y libertades civiles asentada tras los atentados del 11 de septiembre de 2001"[817].

[815] *Vid*. Apartado 232.3, letra c), del Dictamen 1/15.

[816] *Cfr*. CAÑABATE-PÉREZ, J., "La Directiva 2016/681…", *op. cit.*, p. 27.

[817] *Ibidem,* pp. 3-4.

2. Transferencias internacionales de datos a los países asiáticos. Análisis de un nivel de adecuación

2.1. Introducción

A modo de introducción del presente apartado, resulta conveniente apuntar que las iniciativas legislativas comunitarias que se han ido sucediendo en materia de protección de datos de carácter personal en los últimos años han ido suponiendo cada vez más un notable impulso para consagrar la regulación de este derecho en una serie de territorios situados fuera del ámbito de la Unión Europea. Esta aseveración resulta ampliamente contrastada al analizar algunos datos existentes sobre la cuestión, pues de un total de 39 legislaciones existentes en 2012 en el panorama internacional[818] —año en el que daba inicio la redacción del RGPD—, en tan solo cinco años se pasó a 66 en 2017[819], las cuales tomaban como punto de referencia tanto las Directrices elaboradas por la OCDE, como el propio Convenio 108 y la Directiva 95/46/CE para su desarrollo.

Dicha tesitura viene marcada por el creciente interés de los países no comunitarios de obtener la categorización como "adecuada" de su respectiva legislación nacional que desarrolle la materia objeto de estudio, pues dicha clasificación equivale considerar que el territorio que resulte avalado por la Comisión gozará del estándar comunitario de protección sobre los derechos y libertados de los afectados. Por ende, ello supone que los datos personales podrán circular libremente desde la Unión Europea y/o los países integrantes del EEE a ese tercer país, sin precisar ninguna salvaguarda adicional —en palabras del propio GT29[820]—.

Como se ha podido ir observando en los anteriores capítulos de este trabajo, y en consonancia con las consideraciones vertidas por Greenleaf, el cambio de paradigma

---

[818] *Vid*. GREENLEAF, G., "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108", en *International Data Privacy Laws*, 2012, pp. 68–92. Consultado el 15.09.2020 desde: https://papers.ssrn.com/sol3/papers.cfm?abstract_id= 2992537.

[819] *Vid*. GREENLEAF, G., "'European' data privacy standards implemented in laws outside Europe", en *UNSW Law Research Paper*, nº 149 (2017), pp. 1-3. Consultado el 15.09.2020 desde: http://www.ssrn.com/link/UNSW-LEG.html.

[820] *Vid*. COMISIÓN EUROPEA. GT29. "Transferencias de datos personales a terceros países: Aplicación de los artículos 25 y 26 de la directiva de protección de datos de la UE" (WP 12, DG XV D / 5025/98, adoptado el 24 Julio de 1998); "Primera orientación sobre transferencias de datos personales a Terceros países: posibles formas de avanzar en la evaluación de la adecuación" (WP 4, DG XV D / 5020/97-EN final, adoptado el 26 de junio de 1997).

descrito viene motivado en cierta medida por el mandato contenido inicialmente en los artículos 25 y 26 de la Directiva 95/46/CE —cuyo contenido se verá ampliado y reforzado posteriormente en los artículos 44 a 50 del RGPD—. Dichos artículos establecen la posibilidad de que la Comisión Europea, mediante un acto de ejecución, pueda valorar la idoneidad de declarar que un tercer país u organización internacional goce de un nivel de protección adecuado, siempre que se reúnan una serie de condicionantes, tanto por lo que se refiere a los "derechos exigibles" como a las "acciones legales efectivas".

En este orden de acontecimientos, se puede observar cómo en los últimos años ciertos países del continente asiático han ido mostrando paulatinamente su interés en obtener tal distinción, tal y como ha sucedido en el último de los casos avalados con una decisión de adecuación, esto es, Japón, que hace escasamente un año ha obtenido su habilitación como país de nivel de protección adecuado. A ello se le suma que Corea del Sur está en trámites de su obtención en los próximos meses —después de sendas negociaciones efectuadas desde el pasado año 2015—. Con todo ello, podemos advertir que no se trata pues de un hecho puntual y meramente anecdótico, sino que el creciente interés de ciertos países asiáticos en conseguir la "categorización" a la que venimos haciendo alusión se ha convertido en una realidad contrastada.

En cierta manera, lo anterior ha llegado a propiciar que, en el contexto de emergencia sanitaria producido por la pandemia del virus COVID-19, se hayan llegado a poner en contraposición los modelos de protección de privacidad y protección de datos asiático y europeo, pues la lucha sanitaria que se ha llevado a cabo no ha hecho más que poner al límite los sistemas de protección de derechos europeos frente a la necesidad de poner fin al avance de la enfermedad. Dicha situación ha sido interpretada por parte del filósofo y pensador alemán, de origen surcoreano, Binyung-Chul Han, quien a través del concepto de "vigilancia digital y biopolítica" que él mismo ha acuñado[821], manifiesta que el modelo de control sistemático y autocrático existente en China jugará un factor determinante que permitirá que la balanza del poder mundial se decante ligeramente hacia Asia.

[821] *Vid.* HAN, B., "El virus es un espejo, muestra en qué sociedad vivimos", en *El Tiempo*, 16 de mayo de 2020. Consultado el 09.07.2020 desde: https://www.eltiempo.com/mundo/asia/byung-chul-han-habla-del-efecto-del-coronavirus-en-las-personas-y-sociedades-496296.

En cualquier caso, la paradoja está en que hasta el inicio de la pandemia Europa acusaba a Estados asiáticos democráticos, como Japón, Corea del Sur, Taiwán o Singapur, de tener una mentalidad autoritaria, así como de ser unas sociedades con muy poca conciencia crítica ante la vigilancia electrónica; mientras que China y el convulso Hong Kong se entendían como sometidos a una "dictadura digital", y se podría añadir que real. Sin embargo, la digitalización, a través del *Big Data*, de la Inteligencia Artificial, el análisis de macrodatos, etc., permite salvar vidas. La falta del espíritu reivindicativo de las sociedades asiáticas se suple con un ahora admirado civismo[822]. Este es el gran dilema al que se enfrentan los europeos y los estadounidenses.

Un claro ejemplo de lo anterior lo vemos a través de lo que desde las instancias europeas se han empeñado en manifestar reiteradamente ante la mencionada contraposición de intereses en juego, señalando que el despliegue del derecho a la protección de los datos personales no puede impedir que prevalezca un bien jurídico superior como el derecho a la vida. Pero recuerdan que se debe respetar al máximo su contenido y eficacia: "[*w*]*hile it is crucial to make clear that data protection can in no way be an obstacle to save human lives, it is equally crucial to reaffirm that the exercise of human rights, and notably the rights to privacy and to data protection are still applicable. Data protection principles always allow for balancing the interests at stake. Convention 108 sets forth high standards for the protection of personal data which are compatible and reconcilable with other fundamental rights and relevant public interests*. *The principles enshrined in several international and national instruments cannot be suspended but only restricted in a lawful manner, and so for defined limited duration*"[823].

Teniendo en cuenta lo anterior, el objetivo del presente apartado del capítulo se centrará básicamente en analizar someramente el régimen jurídico vigente en materia de protección de datos de carácter personal de los principales países del continente asiático que disponen de una legislación al respecto, o que, en su defecto, han iniciado trámites

---

[822] *Vid*. HAN, B., "Por qué a Asia le va mejor que a Europa en la pandemia: el secreto está en el civismo", en *El País*, 25 de octubre de 2020. Consultado el 29.10.2020 desde: https://elpais.com/ideas/2020-10-24/por-que-a-asia-le-va-mejor-que-a-europa-en-la-pandemia-el-secreto-esta-en-el-ivismo.html?ssm=TW_CC.

[823] Comunicado conjunto emitido por parte de Alessandra Pierucci, Presidenta del Comité de la Convención 108 y Jean-Philippe Walter, Comisionado de Protección de Datos del Consejo de Europa respecto de derecho a la protección de datos en el contexto de la pandemia del COVID-19, de fecha 30 de mayo de 2020. Consultado el 15.05.2020 desde: https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter.

suficientes para su eventual desarrollo. Debe tenerse en cuenta que partimos de concepciones antagónicas, pues resulta oportuno indicar que la construcción cultural de la privacidad parte de una premisa distinta que, en el contexto comunitario, dado que la ley nacional se preceptúa como el principio por antonomasia, quedando las particularidades internacionales en un segundo plano. Adicionalmente, la situación democrática de cada país en cuestión también tiene una influencia directa en la construcción jurídica a la que se viene haciendo alusión.

La hipótesis de la que se parte radica en demostrar que el marco jurídico existente hoy en día en Asia no da cobertura suficiente a la protección de la privacidad y los datos de carácter personal, y menos aún puede llegar a considerarse como un sistema de derechos y libertades más garantista —o incluso equiparable— al instaurado en el ámbito comunitario. Para constatar lo advertido, se iniciará el análisis de los distintos países a partir de sus respectivos textos constitucionales para constatar si los mismos recogen manifestación alguna sobre la materia.

2.2. Principales países con regulación en materia de protección de datos

2.2.1. China

La República Popular China no cuenta con un sistema político y jurídico homologable por el orden jurídico internacional a un régimen democrático en el que se respeten los derechos y las libertades fundamentales de los ciudadanos[824]. La vulneración de derechos humanos es una constante en el país asiático, especialmente en aquellos ámbitos relacionados con la vigilancia digital y la privacidad. El sistema de crédito social instaurado en algunas grandes ciudades es una muestra del control digital masivo que ejerce el gobierno chino sobre sus ciudadanos[825]. Este contexto provoca una

[824] *Vid*. WANG, J., "China: Legal Reform in an Emerging Socialist Market Economy", en BLACK, E. A., y F. BELL. G., *Law and Legal Institutions of Asia: Traditions, Adaptions and Innovations*, Cambridge: Ed. Cambridge University Press, 2011, pp. 24 y ss.

[825] Sobre el sistema de crédito social, *vid*.: CHEN, Y. y CHEUNG, A., "The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System", en *The Journal of Comparative Law*, vol. 12, nº 2 (2017), pp. 356-378. Consultado el 15.09.2020 desde: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2992537; CREEMERS, R., "What Could China's 'Social Credit System' Mean for its Citizens?", en *Foreign Policy*, 15 de agosto de 2016. Consultado el 15.09.2020 desde: https://foreignpolicy.com/2016/08/15/what-could-chinas-social-credit-system-mean-for-its-citizens/; CREEMERS, R., "Big data, meet Big Brother China invents the digital totalitarian state. The worrying implications of its social-credit Project", en *The Economist*, 17 de septiembre de 2016. Consultado el 15.09.2020 desde: https://www.economist.com/briefing/2016/12/17/china-invents-the-

incompatibilidad con los principios y requerimientos de los estándares internacionales y regionales de privacidad de la OECD (las *Privacy Guidelines*) y la APEC (el *Privacy Framework*[826]) y de la UE (el RGPD). Tales circunstancias no han sido óbice para que la gran potencia asiática haya aprobado en la última década normativa referente a la protección de datos de personales.[827]

El régimen jurídico adoptado en esta materia reviste una especial complejidad ya que no existe una norma general como ocurre en Europa. El país oriental ha articulado un sistema que cuenta con un enfoque más parecido, salvando las enormes distancias en garantía de derechos y libertades, al fragmentado propio de los Estados Unidos. Se produce, por tanto, una dispersión normativa sectorial en ámbitos como el bancario, el asegurador, los servicios postales, el de telecomunicaciones o el sanitario que nos ocupa, pues ni su propia Constitución recoge acción alguna dirigida a la protección de la privacidad y los datos de carácter personal, a pesar de que los artículos 33 a 40 del texto reconocen toda una serie de derechos para sus respectivos ciudadanos[828].

Las primeras iniciativas legislativas se produjeron en diciembre de 2012, cuando el Comité Permanente de la Asamblea Popular Nacional (en adelante, APN)[829] promulgó la Decisión sobre el fortalecimiento de la protección de la información en las redes. Este instrumento jurídico estableció una serie de principios generales aplicables a los distintos operadores de servicios en la red. El objetivo era que se adoptasen medidas para garantizar la protección de los datos personales de los ciudadanos chinos. En base a estas directrices,

digital-totalitarian-state; ALDAMA, Z., "Privacidad y datos. El sistema de crédito social chino salta de la teoría a la práctica", en *El País*, 23 de julio de 2018. Consultado el 15.09.2020 desde: https://retina.elpais.com/retina/2018/03/27/tendencias/1522145305_569868.html.

826 *Vid*. APEC Privacy Framework (2015). Consultado el 15.09.2020 desde https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015). Sobre la aprobación de este acuerdo, *vid*., WATER, N., "The APEC Asia-Pacific Privacy Initiative: A New Route to Effective Data Protection or a Trojan Horse for Self-Regulation?", en *UNSW Law Research Paper*, nº 59 (2008), pp. 1-15. Consultado el 15.09.2020 desde: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1402445. Para más discusión sobre este estándar, *vid*., GREENLEAF, G., "Five Years of the APEC Privacy Framework: Failure or Promise?", en *Computer Law & Security Report*, nº 25 (2009), pp. 28-43. Consultado el 15.09.2020 desde: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2022907.

827 *Vid*. GREENLEAF, G., "Ch. 7. China-From Warring States to Convergence?", en *Asian Data Privacy. Trade and Human Rights Perspectives*, Oxford: Ed. University Press, 2014, pp. 191-226.

828 *Vid*. GREENLEAF, G., "The Right to Privacy in Asian Constitutions", en *Oxford Handbook of Constitutional Law in Asia*, Oxford: Ed. Oxford University Press, 2020.

829 Comité Permanente de la Asamblea Popular Nacional. Consultado el 15.05.2020 desde http://www.npc.gov.cn/englishnpc/c4166/column.shtml.

varios departamentos del Consejo de Estado de la República Popular de China adoptaron normas administrativas sobre los tratamientos de datos en su ámbito competencial.

Las mencionadas iniciativas legislativas se vieron culminadas por la aprobación de la Ley de Ciberseguridad[830] por parte del APN, que entró en vigor el 1 de junio de 2017. Esta norma estableció el marco regulatorio de China para la seguridad cibernética y la protección de los datos personales[831]. La ley regula aspectos tales como: a) las obligaciones existentes en la protección de los datos personales, b) las obligaciones generales para la protección de la red por parte de sus operadores, c) la protección para infraestructuras críticas, d) las medidas para la localización de datos, e) la evaluación de seguridad para las transferencias transfronterizas[832], f) así como una serie de revisiones de seguridad de los productos y servicios de red. La norma prevé un régimen sancionatorio para aquellos sujetos que incumplan con sus obligaciones.

Por último, cabe indicar que existen acciones específicas relacionadas con la protección de la privacidad en el ámbito penal y de la responsabilidad civil extracontractual. Para el primero de los ámbitos, se encuentra regulada la acción en el artículo 253, letra a), del Código Penal de la República de China. Para el segundo de los ámbitos, debemos de dirigirnos al *Tort Liability Law*, en sus artículos 2 y 36, respectivamente[833]. Sin embargo, las normativas a las que se ha hecho alusión se encuentran repletas de conceptos jurídicos indeterminados, y en ningún caso pueden homologarse a la legislación de protección de datos existente en Europa, o en última instancia, en Estados Unidos.

---

[830] China. "Cybersecurity Law of the People's Republic of China, November 6, 2016". Acceda la versión no oficial en inglés. Consultado el 05.05.2020 desde: https://www.chinafile.com/ngo/laws-regulations/cybersecurity-law-of-peoples-republic-of-china.

[831] *Vid*. GREENLEAF, G., "China's Personal Information Standard: The Long March to a Privacy Law", en *Privacy Law & Business International Report*, nº 150 (2017), pp. 1-8. Consultado el 15.09.2020 desde: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3128593. *Vid*. GREENLEAF, G., y LIVINGSTON, S., "China's Cibersecurity Law – also a data privacy law?", en *Privacy Law & Business International Report*, nº 144 (2016), pp. 1-7. Consultado el 15.12.2020 desde: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2958658.

[832] *Vid*. GREENLEAF, G. y LIVINGSTON, S., "PRC's New Data Export Rules: «Adequacy with Chinese Characteristics? »", en *Privacy Laws & Business International Report*, nº 147 (2017), pp. 1-8. Consultado el 15.09.2020 desde: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3026914.

[833] *Vid*. GREENLEAF, G., "The Right to Privacy…", en *Oxford Handbook of…*, *op. cit*.

2.2.2. Hong Kong

La Región Administrativa Especial de Hong Kong, por sus características políticas, jurídicas e históricas, procedentes de su antiguo estatus colonial, cuenta con un sistema jurídico muy diferenciado del resto de China[834]. Al respecto, cabe señalar que el texto que sirve *de facto* como constitucional —desmarcándose del resto de sus compatriotas asiáticos—[835], acoge como propia la aplicación del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, que preceptúa el respeto de la vida privada frente a injerencias arbitrarias o ilegales, previendo incluso una serie de acciones de protección al respecto[836].

Detalle que favoreció el hecho de que cuando todavía era un enclave bajo soberanía británica fuera el primer territorio asiático en disponer de una norma general sobre protección de datos: la *Personal Data (Privacy) Ordinance*[837], de 1 de agosto de 1996. La norma se aplica a todas aquellas organizaciones que realicen cualquier tipo de tratamiento de datos de carácter personal, abarcando tanto el sector público como el privado. La *Ordinance* creó también un organismo de control independiente, la *Office of the Privacy Commissioner for Personal Data*, encargado de velar por su cumplimiento, así como, de emitir recomendaciones y directrices para ayudar a las organizaciones a cumplir con sus obligaciones[838].

---

834 *Vid*. BENNY, Y. Y. T., "Hong Kong: Maintaining a Common Law Legal System in a Non-Western Culture", en BLACK A. y BELL G., *Law and Legal Institutions of Asia: Traditions, Adaptions and Innovations,* Cambridge: Ed. Cambridge University Press, 2011, pp. 62 y ss.

835 *Vid*. Hong Kong. "The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China". Consultado el 05.05.2020 desde: https://www.basiclaw.gov.hk/en/basiclawtext/images/ basiclaw_full_text_en.pdf.

836 *Vid*. Artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966. Consultado el 01.06.2020 desde: https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx.

837 La Ordenanza entró en vigor el 20 de diciembre de 1996, siendo posteriormente modificada en 2012 y 2013 para introducir cuestiones relativas a actividades de prospección comercial y asistencia jurídica respectivamente. "*Ordinance to protect the privacy of individuals in relation to personal data, and to provide for matters incidental thereto or connected therewith*", de 6 de agosto de 1996 (L.N. 343 of 1996). Consultado el 24.05.2020 desde: https://www.elegislation.gov.hk/hk/cap486. Sobre la evolución de la normativa de protección de datos, *Vid*. CHEUNG, A., "An Evaluation of Personal Data Protection in Hong Kong Special Administrative Region (1995-2012)", en *International Privacy Law*, 3 (1) (2013), pp. 29-41; BERTHOLD, M. y WACKS, R., *Hong Kong Data Privacy Law: Territorial Regulation in a Borderless Word*, Ed. Thomson, Sweet & Maxwell Asia, 2002.

838 A modo de ejemplo, *vid*., CHIANG, A., "Reviewing the Personal Data (Privacy) Ordinance through Standstill and Crisis. (Speech delivered by Mr. Allan Chiang, Privacy Commissioner for Personal Data at

La norma dispone de seis principios de protección de datos que están recogidos en su Apéndice I, los cuales, como se verá a continuación, cuentan con un gran alineamiento con los principios y enfoque del RGPD. Estas directrices recogidas por el apéndice son los siguientes: i) únicamente se recogerán los datos si existe una finalidad legítima y deberá informarse a los interesados sobre los usos a los que se van a destinar; ii) las organizaciones deben velar para que los datos sean precisos, estén actualizados y no se conserven más de lo necesario; iii) los datos personales no se utilizarán para un nuevo propósito, si con antelación no media el consentimiento del interesado; iv) se deberán establecer una serie de medidas que permitan gestionar los riesgos de seguridad asociados con el tratamiento de datos personales; v) las organizaciones deberán elaborar políticas de privacidad que permitan a los usuarios entender qué se va a realizar con sus datos personales; y vi) se advierte de la necesidad de articular procedimientos que permitan atender en plazo y forma el ejercicio de los derechos de acceso de los afectados.

Dicha legislación ha sido objeto de paulatinas enmiendas, una de las más sustanciales se produjo en 2012, a tenor de las recomendaciones de modificación efectuadas por parte de la autoridad de control en materia de protección de datos de Hong Kong. A pesar de incluirse modificaciones sustanciales para el fortalecimiento de la fuerza ejecutiva de la *Ordinance*, no se realizaron todos los cambios solicitados por el Comisionado. Además, resulta oportuno advertir, pese a que la referida autoridad de control realiza esfuerzos en mantener un nivel de transparencia adecuado respecto de sus actuaciones, se puede realizar un amplio margen de mejora sobre este aspecto.

2.2.3. Corea del Sur

Corea del Sur[839] está considerada como una de las grandes potencias tecnológicas asiáticas, tanto por el gran número de empresas tecnológicas existentes como por los altos hábitos de consumo de servicios de internet que se producen por parte de sus habitantes.

ONC Conference on Law Reform «Does Law Reform need Reforming in Hong Kong?» (on 17 September 2011 at Rayson Huang Theatre, The University of Hong Kong)". Consultado el 15.09.2020 desde: https://www.pcpd.org.hk/english/files/infocentre/speech_20110917.pdf.

[839] Sobre el sistema jurídico en Corea del sur, *vid*., YOUNGJOON, K., "Korea: Bridging the Gap between Korean Substance and Western Form", en BLACK A. y BELL G., *Law and Legal Institutions of Asia: Traditions, Adaptions and Innovations*, Cambridge: Ed. Cambridge University Press, 2011; YOON, D., "Korea", en TAN, P. (Ed.), *Asian Legal Systems: Law, Society and Pluralism in East Asia*, Ed. Butterwoths, 1997.

Según el informe *Digital 2020*[840] de la agencia *We are Social*, se estimaba que en enero de 2020 el país contaba con 49,21 millones de usuarios en internet, suponiendo un índice de penetración de internet del 96 % del total de la población.

La existencia de este contexto tecnológico tan extendido en la sociedad surcoreana hace que no resulte sorprendente que la preocupación por la protección de los datos de carácter personal haya cobrado especial importancia en los últimos años. Así pues, la Constitución de la República de Corea del Sur establece explícitamente la protección general de la privacidad, así como de la intimidad y el secreto de las comunicaciones[841]. Pero no es hasta 2011 cuando se aprueba el primer marco normativo general, a pesar de contar con normas sectoriales que abordaban dicha materia y una jurisprudencia consolidada por parte del Tribunal Constitucional de Corea del Sur.

En esta fecha se produjo la aprobación de la Ley de Protección de la Información Personal ("PIPA", bajo sus siglas en inglés), que sentaría las bases jurídicas para regular las cuestiones relacionadas con esta materia[842]. La norma creó la Comisión de Protección de la Información Personal[843], que es la encargada de configurar las líneas generales en su aplicación, así como de cumplir funciones de órgano interpretativo y supervisor sobre esta materia.

En términos comparativos, se pueden sostener similitudes entre la legislación surcoreana en materia de protección de datos personales y la europea, pues su sistemática y composición es muy parecida. La legislación del país asiático incorpora específicamente las directrices sobre privacidad emitidas por parte de la OCDE[844]. No obstante, alberga algunas diferencias sustantivas, tales como la ausencia de un entorno

---

[840] Para más información sobre los datos del estudio titulado "Digital 2020", elaborado por la agencia We are Social. Consultado el 30.05.2020 desde: https://datareportal.com/reports/digital-2020-south-korea.

[841] *Vid*. Corea del Sur. Artículos 16 a 18 de la Constitución de la República de Corea del Sur de 1987. Consultado el 01.06.2020 desde: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=1&lang=ENG.

[842] *Vid*. GREENLEAF, G. y PARK, W. "Korea's New Act: Asia's Toughest Data Privacy Law", en *Privacy Laws & Business International Report*, nº 117 (2012), pp. 1-6. Consultado el 15.09.2020 desde: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2120983.

[843] *Vid*. Página web de la Comisión de Protección de la Información Personal. Consultado el 31.05.2020 desde: http://www.pipc.go.kr/cmt/main/english.do.

[844] Directrices sobre privacidad emitidas por parte de la Organización para la Cooperación y el Desarrollo Económicos (OCDE). Consultado el 31.05.2020 desde: https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

regulatorio claramente definido que garantice una transparencia por lo que se refiere al uso de la información personal por parte de los responsables del tratamiento, así como la opción principal por el consentimiento como base jurídica que habilita la mayoría de los tratamientos de datos personales. Ambos aspectos la alejarían de los principios del RGPD, en especial con relación a los esfuerzos normativos y de los órganos regulatorios de la UE por ampliar las bases de legitimación y postergar el consentimiento por el cuestionamiento de su carácter libre en relaciones asimétricas, así como en las transferencias internacionales de datos.

Con el objetivo de paliar estas divergencias, que dificultaban la consideración de Corea del Sur como un "país con un nivel adecuado de protección" para la UE[845], desde 2015 se inició un dialogo entre ambos territorios que culminó con la suscripción de un Acuerdo de Libre Comercio. Se convirtió en el primero que fue negociado con un país asiático, dentro de la estrategia de política comercial iniciada desde 2007 por parte de la Comisión Europea[846]. La Comisión Europea presentaría en marzo de 2019 su primera evaluación tras cinco años de aplicación, demostrando que se habían alcanzado los resultados previstos en relación con la liberalización del comercio de mercancías, servicios e inversiones. Se estimó que el acuerdo había generado un crecimiento del producto interior bruto de la Unión de 4.400 millones de euros[847].

Esta tesitura favorecería aún más las intenciones que tenían las autoridades de los citados territorios de adoptar un acuerdo en materia de protección de datos que permitiese el intercambio de información personal bajo un mismo nivel de garantía y control. En consecuencia, desde 2017 se venían intercambiando impresiones sobre la necesidad de dotar a Corea del Sur de una decisión de adecuación[848]. Una iniciativa sustancial que permitiría alcanzar el objetivo pretendido se produjo mediante las reformas iniciadas en 2019 y culminadas en agosto de 2020 en relación con la modificación de la Ley de Protección de la Información Personal. Esta modificación legislativa vino a reforzar las

---

845 *Vid*. Nota de prensa relativa a la decisión de adecuación de Corea del Sur. Consultado el 31.05.2020 desde: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_17_4739.

846 *Vid*. Acuerdo de Libre Comercio suscrito entre la Unión Europea y Corea del Sur. Consultado el 15.09.2020 desde https://ec.europa.eu/trade/policy/countries-and-regions/countries/south-korea/.

847 *Ibidem.*

848 *Vid*. Estrategias de la Unión Europea en materia de transferencias internacionales de datos a Corea del Sur. Consultado el 15.09.2020 desde: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN.

facultades de control y supervisión de la autoridad de control que velaba por su cumplimiento, esto es, la Comisión de Protección de la Información Personal. La norma en cuestión también centró sus esfuerzos en proporcionar garantías sólidas para velar por los principios de trasparencia, limitación de la finalidad y ulterior transferencia.

Vemos como se propiciaba un escenario plausible para que la Comisión Europea entendiera conveniente adoptar una decisión de adecuación sobre Corea del Sur, aspecto que se materializaría a lo largo del 2021[849]. Específicamente, a fecha 16 de junio de 2021, la Comisión Europea hacía público el Proyecto de Decisión de Ejecución con Corea del Sud[850], después de realizar una evaluación pormenorizada de su legislación en materia de protección de datos de carácter personal. Con antelación a su aprobación, el documento se deberá de trasladar al Comité Europeo de Protección de Datos para que emita su correspondiente dictamen al respecto.

Una vez más, se pone de manifiesto como los intereses comerciales y económicos suponen una merma en la garantía de los derechos y libertades de los ciudadanos de la Unión Europea en materia de protección de datos de carácter personal. De conformidad con lo que había tenido la oportunidad de manifestar el TJUE, a través de la sentencia que invalidaba el Acuerdo sobre el Escudo de Privacidad existente entre la UE y los Estados Unidos —que ha sido objeto de estudio en el anterior capítulo—. Máxime, si tenemos en cuenta que una de las principales motivaciones que esgrime la Comisión para seguir avanzando en la consideración de Corea del Sur como un país de un nivel de protección equivalente, radica en que la relación comercial existente con este país se valora en 90 billones de dólares[851].

---

[849] *Vid*. Consecución de la Decisión de adecuación de Corea del Sur por parte de la Comisión Europea. Consultado el 02.04.2021 desde: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN.

[850] *Vid*. Proyecto de Decisión de Ejecución, de conformidad con el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, sobre la protección adecuada de los datos personales por parte de la República de Corea en virtud del Ley de Protección de la Información Personal. Consultado el 20.06.2021 desde: https://ec.europa.eu/info/sites/default/files/draft_decision_on_the_adequate_level_of_protection_of_the_republic_of_korea_with_annexes.pdf.

[851] *Vid*. Nota de prensa efectuada por la Comisión Europea sobre el Proyecto de Decisión de Ejecución con Corea del Sur, en fecha 16 de junio de 2021. Consultado el 20.06.2021 desde: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964

2.2.4. Indonesia

La República de Indonesia ha experimentado en los últimos años grandes cambios tecnológicos del mismo modo que el resto de los países asiáticos de su entorno, circunstancia que ha motivado una gran preocupación por las cuestiones relacionadas con la protección de los datos personales. El régimen jurídico de este derecho parte del reconocimiento en la Constitución de la República de Indonesia de 1945 del derecho a la protección de la seguridad e intimidad personal.[852] Hasta la aprobación en 2008 de la Ley nº 11 sobre Información y Transacciones Electrónicas (en adelante, Ley de Información Electrónica), reformada en el año 2016[853], la protección de datos en Indonesia había experimentado una regulación parcial y sectorizada.[854] La norma cuenta con un desarrollo reglamentario a través del Reglamento del Gobierno nº 71 de 2019 relativo a la implementación de Sistema Electrónico de Transacciones. Esta legislación tiene similitudes con la legislación europea en cuanto a las bases de legitimación, primando el consentimiento por encima de otras[855], a la vez que reconoce algunos derechos a los afectados.

El Reglamento también incorpora una serie de obligaciones para los denominados Proveedores de Sistemas Electrónicos (ESP, por sus siglas en inglés). Los ESP deben disponer de políticas de protección de datos que informen a los afectados sobre los usos y finalidades para las cuales se van a utilizar los datos recabados, que deberíanarticularse con carácter previo a la recogida de estos. Se impone, igualmente, la obligación de disponer de medidas de seguridad que permitan mejorar la protección de la información. La cuestión relativa a la seguridad de la información se ha convertido cada vez más en una constante preocupación para los ciudadanos indonesios, pues resulta habitual que

[852] *Vid*. Indonesia. Artículo 28(G) de la Constitución de la República de Indonesia de 1945. Consultado el 01.06.2020 desde: http://www.humanrights.asia/countries/indonesia/laws/uud1945.

[853] *Vid*. Indonesia. Ley nº 19 de 2016, que modifica la Ley de Información Electrónica. Consultado el 01.06.2020 desde: https://peraturan.bpk.go.id/Home/Details/37582/uu-no-19-tahun-2016. Esta norma se desarrolla reglamentariamente a través del Reglamento del Gobierno nº 71 de 2019 relativo a la implementación de Sistema Electrónico de Transacciones.

[854] Como ejemplo de legislaciones sectoriales específicas, podemos citar, entre otras, las existentes en el ámbito de las telecomunicaciones, bancario, asegurador y servicios de proveedores relacionados con la salud.

[855] Indonesia. Estructuración del consentimiento electrónico en el Reglamento nº 20 de 2016, relativo a la protección de los datos personales en los Sistemas Electrónicos de Transacciones. Consultado el 01.06.2020 desde: https://ppidkemkominfo.files.wordpress.com/2016/12/pm-kominfo-no-20-tahun-2016.pdf.

cada cierto tiempo se produzcan brechas de seguridad que llevan aparejadas revelaciones significativas de datos de carácter personal.[856]

En el contexto descrito, y pese a no existir una autoridad de control específica en materia de protección de datos, el Ministerio de Comunicaciones e Informática supervisa el cumplimiento de la legislación aplicable sobre la materia, por lo que está autorizado a realizar cualquier tipo de requerimiento que le permita garantizar el cumplimiento de esta. Con el objetivo de lograr el alineamiento con la UE, la Cámara de Representantes de Indonesia presentó el pasado mes de enero un proyecto de Ley de Protección de Datos Personales en la que lleva trabajando desde 2015, paralizado en numerosas ocasiones, que supondría la primera legislación existente en este país asiático que aborda de manera específica la materia objeto de análisis[857].

El proyecto en cuestión incluye algunas novedades importantes, pues su alcance se establece tanto para ciudadanos indonesios como extranjeros, así como resulta aplicable para el sector público y privado. Se ha aprovechado la oportunidad también para incluir aspectos similares a los preceptuados por la legislación europea sobre la materia, tales como la obligación de notificación cuando se produzca una brecha de seguridad, un derecho de indemnización en favor de los afectados cuando se produzca una infracción que ponga en jaque sus derechos y libertades y una regulación expresa para las transferencias internaciones de datos personales fuera de Indonesia. Al mismo tiempo, se propone la creación de una autoridad de supervisión independiente que ocupe el vacío normativo existente al respecto en el ordenamiento jurídico de este país asiático.

---

[856] El último ejemplo lo podemos encontrar en la violación sucedida a principios del pasado mes de mayo de 2020 en la empresa Tokopedia, una empresa indonesia especializada en actividades de comercio electrónico que vio comprometidos los datos personales de más de 15 millones de usuarios, encontrándose, entre otros, la información relativa a correos electrónicos, contraseñas y nombres de usuario, cuyo valor de venta en la Internet profunda ascendió a unos 5.000 dólares, aproximadamente. Para más información sobre la brecha de datos de carácter personal sucedida en la empresa indonesia especializada en comercio electrónico Tokopedia, *vid*: ELOKSARI, E. A. "Tokopedia data breach exposes vulnerability of personal data", en The Jakarta Post, 5 de mayo de 2020. Consultado el 01.06.2020 desde: https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personal-data.html.

[857] *Vid*. DAMIANA, J. "Indonesia to step up data protection with new bill amid booming digital economy", en *Reuters*, 28 de enero de 2020. Consultado el 01.06.2020 desde: https://www.reuters.com/article/us-indonesia-data/indonesia-to-step-up-data-protection-with-new-bill-amid-booming-digital-economy-idUSKBN1ZR1NL.

2.2.5. Singapur

La ciudad Estado de Singapur es uno de los países más avanzados en tecnologías de la información del mundo, circunstancia que ha posibilitado una aproximación basada en un uso intenso de los datos de sus ciudadanos a gran escala[858]. Este territorio situado en el sudeste asiático ha recibido severas críticas por la utilización de medidas tecnológicas para el control y vigilancia de sus habitantes[859] ya que suponen una vulneración e injerencia desproporcionada en sus derechos y libertades. En consecuencia, nos brinda un caso de estudio privilegiado para analizar los frágiles equilibrios que existen entre seguridad y privacidad que se erigen en esta nueva era de cambios tecnológicos.

La Constitución de la República de Singapur contiene varios preceptos orientados a la protección de las libertades individuales de los ciudadanos, pero ninguno de ellos regula de manera expresa las cuestiones relativas a la protección de la privacidad y los datos de carácter personal. La mención más importante que se contiene en dicha norma la podemos hallar en su artículo 9.1, cuyo literal reconoce que ninguna persona se verá privada de su vida o de su libertad personal, salvo que ello resulte oportuno por imperativo legal.

Así pues, cabe indicar que la principal norma que regula la recopilación, el uso y divulgación de datos personales en Singapur es la *Personal Data Protection Act* (en adelante, PDPAS), aprobada por el parlamento de esta ciudad Estado el 15 de octubre

[858] *Vid*. GREENLEAF, G. "Singapore—Uncertain Scope, Strong Powers", en *Asian Data Privacy Laws*, Oxford, 2017, pp. 25 y 26.

[859] A pesar de la existencia de una tendencia autoritaria en Singapur, el control en Internet cuenta con una aprobación de alta a moderada por parte de sus ciudadanos. *Cfr*. SHEN, F. ("Cris"), TSUI, L. "Public Opinion toward Internet Freedom in Asia: A Survey of Internet Users from 11 Jurisdictions", en *Research Publication, nº* 8 (2016), The Berkman Center for Internet and Society at Harvard University. Consultado el 01.06.2020 desde: http://ssrn.com/abstract=2773802.

2012[860] y sancionada por el presidente el 20 de noviembre de 2012[861]. La norma está inspirada en las regulaciones de la Unión Europea, Reino Unido, Canadá, Honk Kong, Australia y Nueva Zelanda, así como en las *OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data*[862] y el *APEC Privacy Framework*[863]. El informe de la organización no gubernamental International Privacy, *The Right of Privacy in Singapore,* a pesar de las críticas a este Estado del sudeste asiático por no haber ratificado el Pacto Internacional de Derechos Civiles y Políticos, entiende que la PDPAS es un avance en la defensa del derecho a la protección de datos y la privacidad[864].

Con carácter previo a su promulgación, el pequeño Estado asiático no contaba con una reglamentación general de la protección de datos personales. Por el contrario, existía una normativa sectorial y, en su caso, la propia autorregulación de las organizaciones. Cabe señalar que estas normas específicas han continuado operando junto con la PDPAS. Desde mediados de 2016, la autoridad de protección de datos de Singapur ha ido publicando paulatinamente sus resoluciones en cumplimiento de la legislación aplicable. La mayor parte de las sanciones provienen por la sucesión de brechas de seguridad, así

[860] La PDPA previó que su vigencia se iniciase de forma progresiva en tres fases. La primera de estas relacionada con las disposiciones generales entró en vigor el 2 de enero de 2013. Estas disposiciones se relacionan con el alcance y la interpretación de la PDPA; el establecimiento de la Comisión de Protección de Datos Personales, la autoridad que administra y hace cumplir la PDPA; el establecimiento del Comité Asesor de Protección de Datos; el establecimiento de los Registros de No Llamar (DNC) y otras disposiciones generales del PDPA. La segunda fase guarda relación con la regulación del mencionado Registro DNC, su entrada en vigor fue el 2 de enero de 2014. La tercera y última fase corresponde al desarrollo del régimen jurídico de la protección de datos personales (Disposiciones de protección de datos), específicamente las Partes III a IV de la PDPA, que entró en vigor el 2 de julio de 2014.

[861] Sobre la protección de datos y privacidad en Singapur, véase CHESTERMAN, S. (Ed.), *Data Protection Law in Singapore. Privacy and Sovereignity in a Interconnected World*, Singapur: Ed. Academy Publishing, 2014; GREENLEAF, G., "Regulations with Data Export Limitations Bring Singapore's Data Privacy Law into Force", en *Privacy Laws & Business International Report*, nº 130 (2014), pp. 1-4. Consultado el 15.09.2020 desde: https://ssrn.com/abstract=2516735.

[862] *Vid*. OCDE. *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data*. Consultado el 01.06.2020 desde: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[863] El Marco de privacidad de APEC es un conjunto de principios y pautas de implementación que se crearon para establecer protecciones de privacidad efectivas que eviten las barreras a los flujos de información y aseguren el crecimiento comercial y económico continuo en la región de Cooperación Económica Asia Pacífico (APEC), la cual comprende a 27 países. Véase "APEC Privacy Framework". Consultado el 01.06.2020 desde: https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).

[864] *Vid*. PRIVACY INTERNATIONAL, "Universal Periodic Review Stakeholder Report: 24th Session, Singapore The Right to Privacy in Singapore". Consultado el 01.06.2020 desde: https://privacyinternational.org/sites/default/files/2017-12/Singapore_UPR_PI_submission_FINAL.pdf.

como por realizar comunicaciones de datos a terceros no autorizados. Se ha empezado a percibir que el criterio de la autoridad de control, en ciertas ocasiones, actúa en beneficio de las empresas[865].

2.2.6. Taiwán

Siguiendo con la tónica que hemos ido viendo hasta la fecha en la mayoría de los países asiáticos analizados, la Constitución de la República de Taiwán tampoco reconoce ninguna cláusula concreta orientada a la protección de la privacidad y los datos de carácter personal, aunque sí que cita la necesidad de proteger el secreto de la correspondencia (o el secreto de las comunicaciones) a través de su artículo 12. Dicha cláusula se ve respaldada por una decisión de 1992 efectuada por parte del Tribunal Constitucional de Taiwán sobre las obligaciones de las entidades bancarias de mantener la confidencialidad de sus respectivos registros crediticios[866].

La principal norma que regula la protección de datos en Taiwán[867] es la *Personal Data Protection Act* (en adelante, PDPAT)[868]. Esta norma fue adoptada en 1996 pero cuenta con significativas reformas en 2010[869] y, especialmente, en 2015 para alinearse con la normativa europea de protección de datos. Las *Enforcement Rules of the Personal Data Protection Act* establecen las normas de desarrollo para la interpretación e implementación de la PDPAT.

La norma recoge unos principios básicos que se deben aplicar en el tratamiento de datos personales, los cuales guardan una estrecha identidad con los que establece el artículo 5 del RGPD. Estos serían la trasparencia, licitud (existencia de una base de

---

865 *Vid*. CHIA, K. y CELESTE, A., "Data Privacy Enforcement Trends". Consultado el 05.05.2020 desde: http://www.bakermckenzie.com/en/insight/publications/2017/01/data---privacy---enforcement---newsletter/.

866 *Vid*. PENG, S., "Privacy and the Construction of Legal Meaning in Taiwan", en *International Lawyer*, nº 37, p. 1037, 2003. Consultado el 01.06.2020 desde: https://ssrn.com/abstract=957800.

867 *Vid*. LO, C., "Taiwan-External Influences Mixed with Traditional Elements to Form Its Unique Legal System", en BLACK A. y BELL G., *Law and Legal Institutions of Asia: Traditions, Adaptions and Innovations*, Cambridge: Ed. Cambridge University Press, 2011, p. 94.

868 *Vid*. GREENLEAF, G. y HUI-LING, C., "Data privacy enforcement in Taiwan, Macau and China", en *Privacy Laws & Business International Report*, nº 117, 11-13, pp. 1-6.

869 Sobre esta reforma, *vid*. GREENLEAF, G., "Taiwan revises its Data Protection Act", en *Privacy Laws & Business International Report*, nº 108 (2010) y 109 (2011), pp. 1-9.

legitimación para el tratamiento), con alusión al tratamiento de datos sensibles, limitación de la finalidad, minimización de los datos, proporcionalidad, retención limitada.

Este marco regulatorio cuenta con una autoridad, el *National Development Council* (en adelante, NDC), que es la encargada de interpretar a la PDPAT. En julio de 2018 el NDC creó la *Personal Data Protection Office* con la misión de ser un órgano de control en el cumplimiento de esta materia. Entre las funciones de esta agencia se halla el lograr una "decisión de adecuación" al RGPD por parte de la Comisión Europea. La obtención de este "sello de conformidad" con la normativa europea es fundamental para lograr mecanismos más flexibles y ágiles de transferencias internacionales entre la UE y el país asiático. El impacto económico positivo de la agilización de los flujos transfronterizos de datos personales es muy elevado. En consecuencia, se observa un marco normativo que, a la espera de las instituciones europeas, podría considerarse homologable al RGPD.

2.2.7. Japón

El último caso que se analiza es el de Japón[870]. Al igual que en los supuestos anteriores se hace una breve referencia al régimen jurídico de la protección de datos del país asiático. El derecho a la privacidad en Japón procede de una interpretación jurisprudencial del artículo 13 (Capítulo Tercero, Derecho y Deberes del Pueblo) de su Constitución, en virtud de la cual este derivaría del "derecho a perseguir la felicidad"[871]. La privacidad protegería a este último derecho de aquellas injerencias no consentidas.

Sobre la base de lo expuesto, la Corte Suprema japonesa dictaminó, por un lado, en 1969, que el artículo que se acaba de referenciar establece que la libertad de los ciudadanos en la vida privada queda protegida contra el ejercicio de la autoridad pública, pudiendo entenderse que todo individuo tiene la libertad de proteger su propia

[870] *Vid*. CHIBA, M., "Japan", en TAN, P. (Ed.), *Asian Legal Systems: Law, Society and Pluralism in East Asia*, Butterwoths, 1997; ANDERSON, K. y RYAN, T., en BLACK A. y BELL G., *Law and Legal Institutions of Asia: Traditions, Adaptions and Innovations*, Cambridge: Ed. Cambridge University Press, 2011.

[871] Japón. Artículo 13 de la Constitución japonesa: "*All of the people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental affairs*".

información personal para que no sea divulgada a un tercero o se haga pública sin legitimación[872].

Y por otro lado en 2008, que "la libertad de los ciudadanos en su vida privada estará protegida contra el ejercicio de la autoridad pública y puede considerarse que, como una de las libertades de las personas en su vida privada, cada particular es libre de proteger su propia información personal de modo que no sea comunicada a terceros ni hecha pública sin un motivo justificado"[873].

El artículo 709 del Código Civil japonés, en el capítulo 5 dedicado a los denominados "*Torts*", establece que: "*A person who has intentionally or negligently infringed any right of others, or legally protected interest of others, shall be liable to compensate any damages resulting in consequence*".

Adicionalmente, los tribunales japoneses han descrito el derecho de privacidad en Japón como:

- El derecho a que los asuntos privados no sean hechos públicos sin que exista una debida causa.
- El derecho al control de la información privada.

La primera regulación específica sobre protección de datos se produjo con la adopción de la *Act on the Protection of Personal Information* (APPI, por sus siglas en inglés) en 2003[874]. La APPI fue una de las primeras regulaciones de protección de datos en Asia. Recibió una revisión sustancial en septiembre de 2015 después de que una serie de violaciones de datos críticos se produjesen en Japón. Los mencionados ataques dejaron al descubierto las carencias de la norma aprobada a principios del presente siglo.

A pesar de estas problemáticas, la Comisión Europea homologó la normativa de privacidad japonesa al RGPD a través de la Decisión de Ejecución (UE) 2019/419 de la

---

872 *Vid*. *1965 (A) No. 1187, Judgement of the Grand Bench of the Supreme Court of December 24, 1969*, Keishu Vol. 23, nº 12, p. 1625.

873 Vid. *Judgement of the Grand Bench of the Supreme Court, March 6, 2008*, Minshu, Vol. 62, nº 3, p. 665.

874 *Vid*. LAWSON, C., "Japan's New Privacy Act in Context", en *University of New South Wales Law Journal*, 29 (2) (2006), pp. 88-113. Consultado el 01.06.2020 desde: http://www.austlii.edu.au/au/journals/UNSWLJ/2006/17.pdf; ADAMS, A., MURATA, K. y ORITO, Y., "The Devolpment of Japanese Data Protection", en *Policy and Internet*, nº 2 (2) (2010), pp. 95-126.

Comisión, de 23 de enero de 2019[875]. En efecto, esta decisión considera que Japón cuenta con un nivel de protección adecuado de los datos personales en virtud de su Ley sobre la protección de la información personal (APPI), siendo la primera que se realiza a partir de la fecha donde resultaba de aplicación efectiva el RGPD —esto es, *a posteriori* del 25 de mayo de 2018—. Este hecho aparece constatado en sus considerandos iniciales, en que se realiza la motivación a partir del artículo 45 del RGPD, así como se tienen en cuenta a su vez las directrices emitidas al respecto por el Comité Europeo de Protección de Datos.

La decisión en cuestión está compuesta de 190 considerandos, cuatro artículos y dos anexos, refiriéndose estos dos últimos a las reglas complementarias adoptadas por parte de la Comisión de Protección de Información Personal (en adelante, PPC), así como la carta remitida por parte del Gobierno japonés a la Comisión Europea que incluye la respuesta de la petición de información sobre la visión general del marco jurídico relativo al acceso a la información por parte de las autoridades públicas japonesas. Como el propio documento indica, el contenido de este se centra en lo que respecta a las bases jurídicas disponibles, las condiciones aplicables (limitaciones) y las salvaguardas, incluidas la supervisión independiente y las posibilidades de reparación individual.

Volviendo nuevamente al contenido de los considerandos, la Comisión efectúa una explicación sucinta del marco jurídico japonés aplicable en materia de protección de datos de carácter personal. En los mismos se analiza el ámbito de aplicación material y personal, que incluye las definiciones de los conceptos más relevantes, las exclusiones aplicables, las salvaguardas, los derechos y obligaciones aplicables —que incluyen la mayoría de los principios rectores consagrados en el RGPD— tanto a los sujetos obligados como respecto de los afectados por la recogida de sus datos personales. Adicionalmente, también se menciona las cuestiones relativas a la supervisión y control de la aplicación de la normativa por una autoridad de protección de datos independiente, cuya función recae sobre la CPP —órgano al que nos hemos referido en el párrafo anterior—.

[875] *Vid*. Decisión de Ejecución (UE) 2019/419 de la Comisión, de 23 de enero de 2019, con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales por parte de Japón en virtud de la Ley sobre la protección de la información personal. (DOUE, L 76/1, de 19 de marzo de 2019, pp. 1-58. Consultado en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019D0419&from=ES.

Finalmente, los considerandos a los que se viene haciendo alusión constatan la conclusión a la que llega la Comisión Europea declarando a Japón como un país con un nivel de protección adecuado. Uno de los puntos importantes, y que en principio debería cumplirse, radica en la supervisión continua a la que se compromete la institución comunitaria respecto de la verificación de la proporción del nivel adecuado de protección. Para reforzar este punto, el considerando 180 manifiesta el tenor literal siguiente: "[...] La Comisión, tras la adopción de la presente Decisión, debe comprobar periódicamente si las constataciones relativas a la adecuación del nivel de protección garantizado por Japón siguen estando justificadas desde el punto de vista factual y legal"[876].

Adicionalmente, cabe indicar que el 10 de marzo de 2020, coincidiendo con la pandemia, se aprobó un proyecto de ley para reformar parcialmente la Ley de Protección de Información Personal (en adelante, APPI). Las enmiendas propuestas están destinadas a responder a las crecientes necesidades de equilibrar la protección y la utilización de la información personal, así como mitigar los riesgos que se producen al realizar las transferencias transfronterizas de datos personales. La norma se compromete también a fortalecer los derechos de los interesados, imponer nuevas obligaciones a las empresas que recopilan y gestionan datos personales, instaurar la obligación de notificar ciertas brechas de seguridad sobre datos personales a la Comisión de Protección de Información Persona, ampliar las facultades de la referida autoridad de control sobre empresas *offshore*, introducir el concepto de seudonimización y aumentar el monto de las sanciones por incumplimiento de la APPI.

2.3. Consideraciones

Cuando se habla de Asia, debe pensarse que estamos abordado un sistema político, económico y social diferente al que se puede encontrar en el ámbito de la Unión Europea. Incluso entre las distintas regiones que conforman el continente asiático, se pueden advertir divergencias significativas que, sobre todo, se hacen palpables en cada uno de sus respectivos contextos políticos. En la Unión Europea encontramos democracias consolidadas, dotadas de sistemas electorales que velan por garantizar un relevo de los partidos políticos gobernantes y de las instituciones judiciales —con sus correspondientes

[876] Al respecto, la Comisión Europea indicó, en su comunicación 374 final (Comisión Europea, 2019), que en 2020 proporcionará información sobre la revisión de las decisiones de adecuación que fueron adoptadas conforme a la directiva 95/46/CE.

imperfecciones—. En contraposición, en Asia podríamos llegar a afirmar que estas "realidades" europeas no se corresponden con la situación existente en los países asiáticos. Si bien alguno de ellos dispone de un sistema democrático parecido al europeo, la mayoría se encuentran en proceso de consolidación de lo que se vendría a denominar como un "estado de derecho".

La situación descrita dificulta la consolidación del derecho a la protección de datos como fundamental. Las Directrices elaboradas por la OCDE, como el propio Convenio 108 y la Directiva 95/46/CE, sentaron las bases de la evolución de este derecho en los territorios asiáticos, a pesar de que no disponen de acuerdos vinculantes similares a los aludidos, así como tampoco de tribunales que velen por el cumplimiento de un derecho fundamental a la protección de los datos de carácter personal. Si bien es cierto que, en general, las Constituciones de la mayoría de los países asiáticos que han podido avanzar más en la consecución de ese "estado de derecho" al que se hacía mención reconocen un derecho fundamental a la protección de los datos de carácter personal, ya sea manifestado de manera expresa o indirectamente, según el caso, como establece Davis, la importación del sistema de derechos humanos en Asia no se ha realizado verticalmente, sino horizontalmente, comparando las normas internacionales de derechos humanos con sus respectivos sistemas jurídicos mediante interpretaciones y debates[877].

Los únicos acuerdos internacionales que existen en Asia sobre la materia se reducen a las escasas palabras que se contienen en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos. Pero, en cualquier caso, no pueden compararse en exceso con el régimen que se establece al respecto en la Unión Europea, pues se trata de sistemas antagónicamente diferentes. Lo anterior se hace más evidente si tenemos en cuenta las prácticas que han ido extendiéndose entre los países asiáticos en relación con la vigilancia sistemática de sus ciudadanos. Una buena muestra de ello puede observarse a través del seguimiento de las distintas iniciativas tecnológicas que se han sucedido para controlar el avance de la pandemia originada por el virus del COVID-19.

Lo anterior, a su vez, ha propiciado que una vez más se haya puesto en duda la viabilidad del sistema garantista de derechos y libertades comunitario, en pro de un marco regulatorio más laxo que "supuestamente" hubiera permitido luchar de manera más eficaz

[877] *Vid*. DAVIS M.C., "The Political Economy and Culture of Human Rights in East Asia", (2011) 1(1), en *Jindal Journal of International Affairs*, pp. 48–72.

contra el avance de la pandemia, tal y como se había efectuado en los países del entorno asiático[878]. Como reacción a este planteamiento, se publicaron algunos estudios que abogaban por todo lo contrario, como el realizado por Bradford *et. al.* del Centre for Law, Medicine and Life Sciences de la Universidad de Cambridge. En el mismo se sostiene que: "*The GDPR's expansive scope is not a hindrance but rather an advantage in conditions of uncertainty such as a pandemic. The GDPR framework offers a comprehensive, functional blueprint for digital system design that is compatible with fundamental rights*"[879].

Si se realiza un análisis de las aplicaciones de seguimiento de contactos surgidas para hacer frente al virus del COVID 19 en los países asiáticos, nos permite alcanzar diversas conclusiones[880]. En primer lugar, no sorprende que los sistemas digitales de seguimiento de contactos instaurados en la República Popular China no sean adecuados a la legislación europea. La pandemia no ha hecho más que incrementar el control y la vigilancia de los usuarios chinos con información de carácter sanitario y con una mayor trazabilidad de sus movimientos. La no utilización de protocolos seguros, la ausencia de transparencia y la desviación de las finalidades no son más que abusos a los derechos humanos que no legitiman ni justifican, ni siquiera con un pragmatismo exacerbado, la grave injerencia en la privacidad y la protección de datos. Por tanto, en el caso de la aplicación china denominada "*Alipay Health Code*", se cumpliría plenamente la hipótesis de que no cumple con los requerimientos del RGPD.

El caso de Hong Kong, región especial de China, es muy particular por los condicionantes jurídicos, políticos e históricos que envuelven este enclave territorial. A pesar de contar con una de las primeras normativas de protección de datos de la región,

---

878 *Vid*. MOON, G., "How South Korea Flattened its Coronavirus Curve", en *NBC News*, 24/3/2020. Consultado el 31.05.2020 desde: https://www.nbcnews.com/news/world/how-south-korea-flattened-its-coronavirus-curve-n1167376.

879 *Vid*. BRADFORD, L., ABOY, M. y LIDDELL, K, "COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR and Data Protection Regimes", en *Journal of Law and the Biosciences, University of Cambridge Faculty of Law Research Paper*, nº 23/2020 (2020), p. 3. Consultado el 15.10.2020 desde: https://ssrn.com/abstract=3617578.

880 *Vid*. BOCK, K. *et. al*., "Data Protection Impact Assessment for the Corona App", en *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF)*, vol. 1.6 46 e. V. (29 de abril de 2020). Consultado el 15.10.2020 desde https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3588172.

su aplicación "*StayHomeSafe*"[881] no resultaba conforme al RGPD ya que se basa en la localización a través del geoperimetraje del afectado. Este aplicativo, como se ha dicho, es altamente intrusivo y no cuenta con las salvaguardas exigidas por la normativa europea. En este sentido, cabría plantearse si se está produciendo un retroceso en los elevados estándares de privacidad y protección de datos de los que Hong Kong había disfrutado. El contexto actual apunta a un intento del gobierno chino de recortar los derechos y libertades, esta involución estaría en la línea de los acontecimientos.

El caso de la aplicación "Corona 100" de Corea del Sur presenta las mismas problemáticas[882], incluso superiores, como se ha visto, que "*StayHomeSafe*" de Hong Kong. Esta democracia asiática, que está siendo objeto de escrutinio en cuanto a privacidad y protección de datos por la UE, ha adoptado una solución que tensiona los derechos y libertades de sus ciudadanos y que no es conforme a los principios del RGPD. Ambos supuestos, el de Hong Kong y Corea del Sur, conducen a un concepto muy amplio de interés público, el cual entendería que el derecho a la vida es preferente a la privacidad. Aunque podríamos considerar que se trata de un falso debate, ya que se puede lograr una alta eficiencia en la gestión sanitaria cumpliendo con elevados estándares de privacidad, se trata de cuestiones complementarias, no excluyentes entre sí.

A estos dos países hay que sumar Taiwán, que igualmente ha aplicado mecanismos de trazabilidad con la ausencia de anonimización, elementos a los que hay que añadir la obligatoriedad que estarían en contra del RGPD[883]. Este país de especial estatus internacional, a pesar de contar con una normativa avanzada haría un uso desproporcionado de los datos personales de los usuarios de su aplicación "*SafeEntry*" no conforme con la legislación europea. La aplicación "*PeduliLindungi*" de Indonesia cuenta

---

[881] Para más información sobre el aplicativo, véase el siguiente enlace (en inglés). Consultado el 24.05.2020 desde https://www.coronavirus.gov.hk/eng/stay-home-safe.html.

[882] *Vid*. MAX, K. S., "South Korea is watching quarantined citizens with a smartphone app", en *MIT Technology Review*, 06/03/2020. Consultado el 01.05.2020 desde: https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/.

[883] *Vid*. MONTJOYE, A. *et. al*., "Evaluating COVID-19 contact tracing apps? Here are 8 privacy questions we think you should ask", Ed. Computational Privacy Group, 2 de abril de 2020. Consultado el 11.10.2020 desde: https://cpg.doc.ic.ac.uk/blog/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask/.

con mayores impedimentos[884], si cabe, que los anteriores aplicativos, pues el país no cuenta con un contexto normativo de protección de datos homologable al de la UE[885] que pueda compensar las medidas invasivas y desproporcionadas como ocurre en Hong Kong o Corea del Sur.

En consecuencia, en los casos de China, Hong Kong, Taiwán, Corea del Sur e Indonesia se cumpliría la hipótesis de contar con aplicaciones de seguimiento de contacto COVID-19 no conforme con el RGPD. En el extremo contrario, es decir, que cuentan con aplicaciones que son adecuadas con la normativa de protección de datos de la UE, hallaríamos Singapur y Japón. El primero de estos países ha recibido tradicionalmente críticas de exceso de control y vigilancia digital; no obstante, su aplicación, "*TraceTogether*", cumpliría los requerimientos técnicos sustanciales que exigen las recomendaciones de las instituciones europeas. La misma afirmación es aplicable a la COVID-19 Contact App —la aplicación japonesa—, a un contexto homologado plenamente por las autoridades comunitarias se suma la utilización de la plataforma desarrollada por Apple y Google, API, que ha recibido la validación por parte de la UE y de EEUU[886].

Así pues, puede afirmarse que la disminución de la privacidad y de la protección de datos personales no es lo que otorga una mayor eficiencia en la lucha contra la pandemia, sino un sistema sanitario lo suficientemente robusto para gestionar la información y efectuar las acciones que sean necesarias con la información que ofrecen las aplicaciones alineadas con el RGPD. Si atendemos a la finalidad principal de las

---

[884] *Vid*. FACHRIANSYAH, R. y SYAKRIAH, A., "COVID-19: Indonesia develops surveillance app to bolster contact, tracing, tracking", en *The Jakarta Post*, 30 de marzo de 2020. Consultado el 01.06.2020 desde: https://www.thejakartapost.com/news/2020/03/30/covid-19-indonesia-develops-surveillance-app-to-bolster-contact-tracing-tracking.html.

[885] A modo de ejemplo de las vulneraciones a la privacidad que ha ocasionado la pandemia, se puede mencionar que los dos primeros pacientes confirmados de la enfermedad en Indonesia fueron revelados a través de redes sociales, concretamente mediante la publicación de sus iniciales en grupos de WhatsApp, para posteriormente ser increpados, tanto por parte de los medios de comunicación como en las redes sociales. *Vid*. FACHRIANSYAH, R. y SYAKRIAH, A., "COVID-19 patients become victims of Indonesia's lack of privacy protection", en *The Jakarta Post*, 4 de marzo de 2020. Consultado el 01.05.2020 desde: https://www.thejakartapost.com/news/2020/03/04/covid-19-patients-become-victims-of-indonesias-lack-of-privacy-protection.html.

[886] *Vid*. CEPD. "Guidelines of the European Data Protection Board 04/2020 on the Use of Location Data and Contact Tracing contact tracing tools in the Context of the COVID-19 Outbreak", sec. 2.2., 21 de abril de 2020. Consultado el 05.05.2020 desde: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

aplicaciones, que es el seguimiento de contactos COVID-19 para prevenir la expansión de la pandemia, los exigentes requerimientos establecidos por la normativa europea no son ningún obstáculo o impedimento para que se cumpla con la misma. Por tanto, es una falacia que el estado de vigilancia digital con deriva totalitaria asiático sea la clave del éxito, tal como señalaba Binyung-Chul Han. Por el contrario, es la existencia sinérgica de sistemas de recopilación de la información preventivos y eficientes, que actúen de manera proporcional y con todas las garantías, con estrategias sanitarias públicas adecuadas a la situación de pandemia.

Por lo tanto, se puede concluir que la brecha en garantía de derechos y libertades entre la UE y el gigante asiático se agranda aún más tras esta crisis global sanitaria y que, salvo en casos excepcionales como el de Japón —y próximamente Corea del Sur—, la legislación de protección de datos existentes en los países asiáticos no daría cumplimiento a las consideraciones establecidas por el RGPD, aspecto que imposibilitaría la obtención por parte de estos países asiáticos del nivel de protección adecuado avalado por parte de la Comisión Europea. Esta falta de homologación con la legislación europea, del mismo modo que ocurre con otros países asiáticos, tiene un impacto muy negativo en las transacciones comerciales con la UE altamente ligadas a la "economía del dato", tal y como se ha podido ir observando en distintos apartados del presente estudio.

CONCLUSIONES

En consonancia con los distintos objetivos e hipótesis planteadas en el presente trabajo de investigación, en este apartado se expondrán las conclusiones alcanzadas:

PRIMERA. – Como se ha podido constatar a lo largo del presente trabajo, una de las principales conclusiones que pueden extraerse radica en la manifiesta hipocresía adoptada por parte de la Unión Europea en lo relativo a la materia que aquí nos ocupa. Dicha aseveración viene motivada esencialmente por la negligencia incurrida por parte de la Comisión Europea en su labor de velar por la garantía y respeto de los derechos y libertades de los afectados en aquellos supuestos donde sus datos personales se transfieren a terceros territorios situados fuera del entorno comunitario. En particular, ello se evidencia en el contexto del intercambio de datos personales con los Estados Unidos, donde se constata de manera efectiva la prevalencia de los intereses económicos y políticos en detrimento de la correcta salvaguarda y tutela del derecho fundamental a la protección de los datos de carácter personal de los ciudadanos de la Unión.

El razonamiento que se viene exponiendo no puede considerarse trivial y sin fundamento. Como se ha tenido ocasión de observar en el contenido de este trabajo, el GT29 lo venía indicando reiteradamente —en las sucesivas revisiones de los acuerdos que habilitan el flujo transnacional de datos personales entre ambos territorios—, el propio TJUE lo acogió como propio y posteriormente como colofón, se vería refrendado por parte del Parlamento Europeo en dos ocasiones de manera taxativa. La primera en su Resolución de fecha, 5 de julio de 2018, donde responsabilizaba a la Comisión de no haber logrado el equilibrio entre la protección del derecho fundamental a la protección de los datos personales y el desarrollo de los intereses comerciales o políticos, por lo que solicitaba la suspensión del acuerdo que habilitaba las transferencias internacionales de datos personales a los Estados Unidos hasta que se dieran las condiciones necesarias que permitiesen el intercambio de los mismos con las garantías adecuadas.

La segunda mediante la Resolución de fecha, 20 de mayo de 2021, cuando manifiesta por un lado, que "lamenta que la Comisión haya hecho caso omiso de los llamamientos del Parlamento a suspender el Escudo de la privacidad hasta que las autoridades estadounidenses se atengan a sus disposiciones, y en los que subrayaba el riesgo de que el Tribunal de Justicia invalide el Escudo de la privacidad; recuerda que el

Grupo de Trabajo del Artículo 29 y el CEPD plantearon en repetidas ocasiones problemas relacionados con el funcionamiento del Escudo de la privacidad" [887]. Y, por otro lado, también lamenta "que la Comisión anteponga las relaciones con los EE. UU. a los intereses de la ciudadanía de la Unión y que, de este modo, la Comisión haya dejado en manos de ciudadanos particulares la tarea de defender el Derecho de la Unión"[888].

Por ende, el TJUE en el marco de su Sentencia "Schrems II" [889], se pronuncia nuevamente en el mismo sentido que se viene señalando. El referido organismo judicial concluyó que el Acuerdo sobre el Escudo de Privacidad resultaba incompatible con el mandato efectuado por el artículo 45.1 del RGPD interpretado a la luz de los artículos 7, 8 y 47 del CDFUE. Entendió que la Comisión no tuvo en cuenta dichas consideraciones, pese que "a priori" había efectuado las comprobaciones necesarias que le permitieron determinar con exactitud que EE. UU. y, en consecuencia, la Decisión de Ejecución (UE) nº 2016/1250 reunían los condicionantes necesarios para declarar al país estadounidense con un nivel de protección adecuado. Cuestión que resulta cuanto menos paradigmática, si se tiene en cuenta que el propio contenido de la Decisión reconoce expresamente la primacía de las exigencias de las autoridades norteamericanas en relación con la salvaguarda de la seguridad nacional y el interés público frente al amparo del derecho a la protección de los datos personales. Circunstancia que, con anterioridad, ya había provocado la caída del anterior Acuerdo de Puerto Seguro.

Así pues, resulta del todo evidenciado que la relación entre los Estados Unidos de América y la Unión Europea en materia de protección de datos ha estado siempre supeditada al beneficio económico que el intercambio de estos supone para ambos territorios —a pesar, de partir "teóricamente" de concepciones jurídicas de protección diametralmente opuestas—. Se calcula que el comercio total entre ambos socios comerciales aumentó de 594.000 millones a 1.2 billones de dólares de 2003 a 2017[890]. Por este mismo motivo, las respectivas autoridades de dichos territorios han mostrado históricamente su más profundo interés en negociar acuerdos que habilitasen el intercambio de datos personales sin apenas restricciones. A sabiendas, en todo momento,

[887] Apartado 19 de la Resolución del Parlamento Europeo, de 20 de mayo de 2021, cit.

[888] Apartado 20 de la Resolución del Parlamento Europeo, de 20 de mayo de 2021, cit.

[889] *Vid*. STJUE. Asunto C-311/18 (Schrems II), cit., apdo. 164

[890] *Vid*. PATEL, O. y LEA, N., *EU-U.S. Privacy Shield…, op. cit.*, p. 11.

de la existencia de un manifiesto menoscabo en relación con la tutela del derecho fundamental a la protección de los datos personales de los ciudadanos comunitarios.

SEGUNDA. – Puede concluirse que resulta un tanto paradigmático que, en el ámbito de las transferencias internacionales de datos de carácter personal, desde la perspectiva comunitaria se tilde a los poderes públicos norteamericanos de excesivamente proteccionistas en lo relativo a la salvaguarda de la seguridad nacional y se manifieste que sus prácticas de vigilancia sistemática ponen en jaque los derechos fundamentales de los afectados, excediendo en demasía los limites previstos para esta tipología de actuaciones. Cuando desde la Unión Europea, se están realizando prácticas similares orientadas a la protección de este bien jurídico frente a la sucesión de posibles amenazas externas de carácter terrorista. Lo que supone en la práctica, una vulneración flagrante del contenido propio del derecho fundamental a la protección de datos de carácter personal.

Dicho razonamiento tiene su fundamento —sin mencionar ciertas prácticas de inteligencia que también se han indicado a lo largo del trabajo— en la Directiva relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave. Su aprobación coincidió con la del RGPD, dentro del paquete de medidas orientado a la prevención del terrorismo y a la lucha contra el crimen organizado validado por el Parlamento Europeo y el Consejo. La entrada en vigor de la Norma vendría a colisionar directamente con los fundamentos intrínsecos de la cultura jurídica de protección de datos existente en la Unión Europea, a pesar de abogar en diversos puntos de su contenido por el respeto de este derecho fundamental, con base en las exigencias establecidas en la CDFUE, el Convenio 108 y el CEDH.

Su sistemática de funcionamiento sustentada en la utilización del PNR pone en jaque precisamente la salvaguarda del derecho a la protección de los datos de carácter personal, pues la recogida masiva e indiscriminada de información que se efectúa difícilmente encuentra encaje entre las exigencias regulatorias establecidas al respecto por parte de la legislación comunitaria. Como se ha podido observar, no se trata de ninguna novedad, sino que dicha problemática ya fue puesta de manifiesto en su momento por parte del SEPD en la primera revisión efectuada sobre la propuesta de Directiva

PNR[891]. A lo que posteriormente, el GT29 se pronunciaría en el mismo sentido en 2015, a través de un comunicado remitido al presidente del LIBE[892].

En este sentido, la Directiva PNR contiene distintos puntos de inflexión que vienen a producir la colisión que se ha venido describiendo. Desde la ambigüedad en la que se incluye el concepto de "automatizado" respecto los tratamientos de los datos PNR, pasando por la inexistencia de controles externos sobre la utilización del esquema expuesto del PNR por parte de las UIP, hasta la ausencia de garantías suficientes que den cobertura eficaz sobre la salvaguarda y tutela de las garantías de los afectados respecto al tratamiento de sus datos de carácter personal. Donde se incluye tanto la ausencia de información relativa al ejercicio de derechos, como la falta de previsión de períodos máximos de conservación respecto la información recabada.

Teniendo en cuenta estas consideraciones, se puede concluir afirmando que la Directiva PNR debería estar dotada de criterios de transparencia y claridad más precisos que ayudasen a dotar de seguridad jurídica el marco normativo comunitario y nacional relativo a esta materia. En consonancia con las manifestaciones realizadas por el propio TJUE[893], la utilización de los datos PNR por las respectivas UIP de los Estados miembros —tanto durante la estancia de los pasajeros en un determinado país como tras su salida de este—, así como toda comunicación de dichos datos a otras autoridades, debe someterse al cumplimiento de una serie de requisitos materiales y procedimentales basados en criterios objetivos.

Por ende, puede manifestarse que el sistema PNR expuesto no da cumplimiento a las prerrogativas normativas establecidas por la CDFUE, el CEDH y el propio RGPD —de conformidad con lo expuesto por parte de distintos organismos comunitarios con competencias sobre la materia—, produciéndose un claro desequilibrio de intereses en favor de la salvaguarda de la seguridad nacional. Dicha coyuntura implica la asunción de la doctrina norteamericana involucionista que vela por la protección de este bien jurídico por encima de cualesquiera otros derechos, aunque éstos últimos puedan ostentar el rango de fundamental.

---

[891] *Vid*. SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, "Dictamen sobre la propuesta de Directiva…", cit., apdo. 17.

[892] *Vid*. Comunicado efectuado por el GT29 al presidente del LIBE, cit.

[893] *Vid*. Apartado 232.3, letra c), del Dictamen 1/15.

TERCERA. – En el contexto comunitario, no será hasta finales del siglo XX que se vendrán a iniciar toda una serie de actuaciones legislativas tendentes a regular el derecho fundamental a la protección de datos de carácter personal. El continente europeo se encontraba en una situación particular motivada por la necesidad de seguir apostando por el proceso de construcción de la Unión Europea, así como con el reto de conjugar la pluralidad de ordenamientos jurídicos nacionales con las normas de carácter supranacional que se iban promulgando. Esta tesitura propiciará que la evolución de este derecho sea constante, a tenor de los debates doctrinales y pronunciamientos jurisprudenciales que se iban produciendo.

Tras los antecedentes sentados por la Declaración Universal de los Derechos Humanos de 1948 y el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales —a lo que se podría adicionar también las Directrices de la OCDE—. El principal hito normativo viene marcado por el Convenio 108 adoptado por el Consejo de Europa, constituyéndose como el primer instrumento jurídico internacional en materia de protección de datos con carácter vinculante. Dicho texto sentaba las bases de lo que posteriormente vendrá a convertirse en un derecho fundamental, a pesar de que no aparecía expresamente así establecido en su contenido. Su proceso de consagración será gradual hasta culminar definitivamente con su previsión en la CDFUE.

Pese a ser un gran avance en relación con el respeto al derecho a la vida privada y familiar, el Convenio 108 adolecía de dos cuestiones que dificultaban su aplicación efectiva. Por un lado, su contenido no era susceptible de aplicación directa sobre los ordenamientos jurídicos nacionales de los Estados parte, tal y como tendrían ocasión de ratificar con posterioridad a su adopción el TC y el TS respectivamente en el caso español. Y, por otro lado, se omitió la introducción de una regulación que habilitara los movimientos transfronterizos de datos personales entre los distintos Estados firmantes del Convenio respecto a terceros Estados u organizaciones internacionales no integrantes del mismo. Dicha deficiencia sería posteriormente subsanada en el año 2001 mediante la elaboración de un Protocolo Adicional.

Así pues, con soporte en la jurisprudencia alemana y la corriente doctrinal dimanante de Estados Unidos, se empieza a reconocer que la vertiente propia relacionada con el derecho a la autodeterminación informativa puede ser susceptible de consolidarse con rango de constitucionalidad. Este carácter será posteriormente refrendando por ciertas disposiciones incorporadas sucesivamente en el Acuerdo de Schengen, el Tratado de

Maastricht y la Directiva 95/46/CE, para verse finalmente consagrado en la CDFUE. Su artículo 8 recoge expresamente el derecho a la protección de datos de carácter personal, diferenciándose de lo que había sucedido con anterioridad con el CEDH. Este último texto normativo únicamente había incluido alguna previsión en relación con el respeto de la vida privada, a *sensu contrario* la CDFUE introduce una nueva perspectiva abordando de manera diferenciada el respeto a la vida privada y familiar respecto del derecho a la protección de datos de carácter personal.

Con base en este planteamiento, la Directiva 95/46/CE vendría a consolidarse como el marco de referencia en materia de protección de datos personales, en consonancia con los principios que se habían establecido por parte del Convenio 108 del Consejo de Europa. Lo anterior supuso el reconocimiento de un haz de facultades para que los interesados pudieran optar por la defensa de sus respectivos derechos y libertades fundamentales. No obstante, también propició la generación de situaciones controvertidas en relación con su efectiva aplicación práctica, motivadas por la divergencia de posiciones interpretativas que se fueron adoptando por parte de los órganos jurisdiccionales y las autoridades competentes sobre la materia, así como por el amplio margen de discrecionalidad que aplicaron los Estados Miembros en el ejercicio de transposición a sus respectivas legislaciones nacionales.

Lo anterior motivó la necesidad de buscar soluciones que resolvieran las incongruencias incurridas. De hecho, incluso en el propio Preámbulo de la LOPDGDD se pone de manifiesto la situación de inseguridad jurídica que se produjo, cuando preceptúa el tenor literal siguiente: "[l]a transposición de la directiva por los Estados miembros se ha plasmado en un mosaico normativo con perfiles irregulares en el conjunto de la Unión Europea lo que, en último extremo, ha conducido a que existan diferencias apreciables en la protección de los derechos de los ciudadanos".

El Tratado de Lisboa surge como una de las soluciones *prima facie* desde el prisma de la protección de los datos de carácter personal, que juntamente con el Reglamento General de Protección de Datos se erigirán como los mecanismos por antonomasia de regulación de este derecho en el contexto de la Unión Europea. El Tratado trae consigo la introducción del artículo 16 en el TFUE que establece que la CDFUE pasa a ser plenamente aplicable sobre aquellos Estados miembros que habían ratificado el acuerdo. En suma, se le reconoce el mismo valor jurídico para todos los Estados que el TUE y el TFUE, en virtud de lo preceptuado por el artículo 6 del TUE.

Por su parte, siguiendo el mismo razonamiento, el RGPD no centra su objeto de protección en el derecho a la intimidad como lo hacía la Directiva 95/46/CE, sino que lo hace sobre el derecho a la protección de los datos de carácter personal, en base a lo establecido por el artículo 8.1 de la CDFUE y el artículo 16.1 del TFUE, por considerarlo un derecho autónomo y de carácter fundamental. No obstante, pese a sus magníficas intenciones, la mayoría de los objetivos que pretendía no se han visto definitivamente alcanzados en la práctica —y al menos, a corto plazo, tampoco lo harán—. Su Considerando número 10 constituye toda una declaración de intenciones cuando establece que, a través de este nuevo instrumento, se garantizará un "nivel uniforme y elevado de protección de las personas", eliminando las fronteras que dificultan el libre movimiento de datos en el ámbito de la Unión Europea.

Por lo que a modo de conclusión, se considera oportuno reproducir nuevamente la literalidad de las palabras de Sancho López —con las que no se puede estar más de acuerdo—, cuando manifiesta que: "[...] es ingenuo pensar que la finalidad última del Reglamento es acabar con la desprotección de los ciudadanos europeos, nada más lejos de la realidad pues lo que realmente quiere evitarse es que se continúen produciendo obstáculos para el mercado interior de la UE, lo que dificulta el ejercicio de actividades económicas a escala comunitaria y está provocando un falseamiento de la competencia"[894].

CUARTA. – Como resultado de lo analizado, puede concluirse que la institución jurídica relativa a las transferencias internacionales de datos personales, pese a su reciente introducción en el acervo normativo comunitario, ha sido manifiestamente insuficiente y de difícil interpretación, siempre vinculada a la ambigüedad por su imposibilidad de aplicación práctica. En este sentido, sería el TJUE quien tuvo a bien formular una primera conceptualización al respecto ante la ausencia de un pronunciamiento expreso efectuado por parte de los distintos instrumentos legislativos. Su regulación en la Directiva 95/46/CE se reducía básicamente a dos artículos que incluían una prohibición general de realizar esta tipología de tratamientos de datos personales, así como una serie de excepciones que levantaban dicha prohibición.

[894] *Cfr*. SANCHO LÓPEZ, M., "Consideraciones procesales del ejercicio del derecho al olvido: examen de jurisprudencia reciente y del nuevo marco legal", en Revista Aranzadi de Derecho y Nuevas Tecnologías, nº 41 (2016), pp. 1-17.

Tomando en consideración el legado normativo del Convenio 108, los movimientos transnacionales únicamente estaban previstos si se constataba el "nivel de protección adecuado" del país destinatario de los datos personales. Pese a que las circunstancias que debían darse eran varias para declarar dicha condición, resultaba bastante habitual que los motivos económicos y los intereses comerciales jugasen un papel preponderante en la consecución de la decisión, como se ha tenido ocasión de comprobar. Al mismo tiempo, solían preverse en la misma mecanismos de supervisión para verificar periódicamente su validez, independientemente de la tarea de control que tuvieran asignadas las respectivas autoridades competentes de los distintos EE. MM. y la propia Comisión. No obstante, pese a estos esfuerzos, puede afirmarse que ninguna de las alternativas existentes ha solventado los incumplimientos que se materializan en el momento de la sucesión de flujos de datos personales fuera del contexto comunitario a terceros destinos, que pese a mantener una apariencia de cumplimiento, no aplican las suficientes garantías.

El RGPD pretendía poner fin a la multitud de dificultades que se suscitaban en el ámbito de las transferencias internacionales de datos personales mediante la aportación de un régimen jurídico específico para esta tipología de tratamientos. Esta nueva sistemática partía de la tradición histórica que se había previsto en la Directiva 95/46/CE, pero con un nuevo enfoque basado en el equilibrio entre los intereses comerciales y la protección de este derecho fundamental. Pero como si de una quimera se tratase, por el momento no ha conseguido el objetivo pretendido en lo relativo a la casuística que aquí nos concierne, sino que, en términos generales, ha venido a realizar únicamente ciertas apreciaciones sobre el régimen de excepciones previsto en la Directiva 95/46/CE. A título ejemplificativo, el fracaso estrepitoso obtenido con la anulación del Acuerdo de intercambio de datos personales entre la Unión Europea y los Estados Unidos en el marco de la STJUE sobre el asunto "Schrems II" supone una muestra de lo expuesto.

En el contexto español, la alusión conceptual sobre las transferencias internacionales encuentra su encaje normativo en la Instrucción 1/2000 de la AEPD, haciendo mención nuevamente a un concepto erróneo a raíz de una inobservancia incurrida durante la transposición respecto de lo establecido en el texto de la Directiva 95/46/CE. No será hasta la entrada en vigor del RLOPD que se formulará un nuevo concepto expreso de la institución que dispondrá de un enfoque más cercano a lo establecido por el derecho comunitario. Al mismo tiempo, la escasez de regulación a la

que hacíamos alusión en el ámbito comunitario en lo relativo a las transferencias internacionales de datos personales se traslada también al ordenamiento español.

Tanto la LORTAD como la LOPD no aprovecharon los márgenes de desarrollo y mejora que la Directiva —como instrumento de derecho comunitario— facultaba a los distintos países de la Unión Europea para introducir mejoras que redundasen en propiciar una mayor seguridad jurídica. El régimen jurídico se ventiló en dos artículos básicamente en cada uno de los textos normativos aludidos, siguiendo la estructura del principio general de prohibición y la previsión de excepciones que evitaban la suspensión de las transferencias introducida por la propia Directiva 95/46/CE. Dichas excepciones serían posteriormente interpretadas y acotadas por parte del GT29, en aras de evitar abusos y fraudes de ley que se estaban produciendo durante su vigencia por parte de distintos EE.MM.

Adicionalmente, debe de hacerse expresa mención a la LOPDGDD, que tal y como preceptúa la propia Disposición derogatoria única que en la misma se contiene, trae consigo la derogación de la Ley Orgánica 15/1999. A este respecto, puede afirmarse que su aprobación no supone ninguna novedad, pues parece ser que se ha optado por la costumbre de que las normas que se encargan de transponer la normativa comunitaria a nuestro maltrecho ordenamiento jurídico no aportan cuestiones de calado. Sino que, lejos de incluir mejoras respecto de lo previsto por el legislador europeo, en determinados aspectos la LOPDGDD supone incluso una merma de garantías. Su redactado se limita a reproducir la literalidad contenida en el RGPD, introduciendo algunas particularidades que no afectan significativamente las cuestiones vinculadas a las transferencias internacionales de datos.

Por último, la situación descrita constata una vez más que el proceso de armonización y homogeneización normativo que pretende la Unión está más lejos de consolidarse de lo que se manifiesta. No se trata únicamente de optar por cuestiones formales como modificar el instrumento de derecho comunitario —pasando de una Directiva a un Reglamento—, sino que los esfuerzos que deben de realizarse van más allá, cambiando costumbres y pensamientos hacía un objetivo común de mercado interior y de armonización completa. Máxime, si tenemos en cuenta que existen dos factores que juegan en contra. Por un lado, el principio de soberanía nacional y el peso de los presupuestos nacionales —que es superior al de la propia Unión Europea—, configurándose como elementos clave. Y, por otro lado, las distintas preferencias y

costumbres existentes en los diferentes EE. MM., que incluso, en determinados casos, se preceptúan como diametralmente opuestas.

QUINTA. – Puede afirmarse que el histórico de acontecimientos que se ha venido exponiendo a lo largo de este trabajo, no hace más que constatar una realidad evidente que redunda en la impracticabilidad de realizar transferencias internacionales de datos personales a los Estados Unidos de América con la aplicación de unas garantías adecuadas ante el contexto normativo descrito. Dicha situación viene motivada principalmente por la imposibilidad de intentar encuadrar un régimen de amparo en lo relativo a la protección de los datos personales similar al europeo en el contexto del ordenamiento jurídico norteamericano. Debe entenderse que las situaciones jurídicas de ambos territorios se preceptúan como realmente antagónicas, pues su punto conexión más cercano lo encontraremos principalmente en determinados puntos de su histórico desarrollo normativo, pero en ningún caso, en la sistemática utilizada para su protección.

Para hacer viable el intercambio de datos personales que se pretende —tal y como el propio Parlamento Europeo señala[895]—, el poder legislativo de los Estados Unidos debería llevar a cabo una profunda reforma de múltiples normas que debería pasar, entre otras por la modificación de la Sección 702 de la FISA, la EO 12333 y la PPD-28 en lo relativo a las prácticas de vigilancia masiva y sistemática, otorgando el mismo nivel de protección para los ciudadanos de la Unión y los propios de los EE. UU. Para ello resultaría preciso articular mecanismos de protección específicos y eficaces, que permitiesen la debida tutela judicial de los derechos y libertades de los ciudadanos que no ostenten la nacionalidad estadounidense. No siendo suficiente con los marcos reguladores que se han sucedido hasta el momento, ni tampoco con las eventuales legislaciones que se están empezando a adoptar por parte de los distintos Estados norteamericanos en materia de protección de la intimidad y los datos personales de los consumidores.

Para entender lo anterior, cabe recordar que los Estados Unidos de América parten de un sistema que no reconoce la protección de la privacidad mediante una legislación específica, sino que ello se efectúa a través de diversas normativas federales de carácter

[895] Apartado 23 de la Resolución del Parlamento Europeo, nº 2020/2789 (RSP), de 20 de mayo de 2021, sobre la sentencia del Tribunal de Justicia de 16 de julio de 2020, Data Protection Commissioner / Facebook Ireland Limited y Maximillian Schrems («Schrems II»), C-311/18. Consultado el 5 de mayo de 2021 desde: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_ES.html

sectorial que mediante su completitud con las autorregulaciones privadas de determinados sectores propician un marco normativo singular —repleto de excepciones y lagunas que dificultan su interpretación—. Este escenario descrito difiere del preceptuado en el ámbito europeo, tendente a vehicular toda la regulación sobre una materia a través de un mismo cuerpo legal, huyendo de las características propias de los sistemas basados en una dispersión normativa. Lo anterior se constata con la regulación introducida inicialmente por la Directiva 95/46/CE y, posteriormente, con el RGPD.

Las diferentes visiones entre los Estados Unidos de América y la Unión Europea, aparte de hacerse evidentes en la configuración de los distintos regímenes jurídicos de protección sobre los datos de carácter personal, también se pone de manifiesto en el contexto de las acciones de vigilancia masiva llevadas a cabo por parte de las agencias de inteligencia de los Estados Unidos. Lo anterior se hizo evidente durante la negociación del primer acuerdo de intercambio de datos entre ambos territorios, articulado a través de la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000. Con posterioridad, a lo largo de su dilatada vigencia —teniendo en cuenta, los numerosos incumplimientos que se hallaban previstos en su contenido—, el GT29 vendría a poner de manifiesto reiteradamente las diferentes carencias de las que adolecía. Las mismas se sustentaban esencialmente en las particularidades propias de la legislación interna de los Estados Unidos existente sobre la materia, basada en la prevalencia de la seguridad nacional frente a la protección de cualesquiera otros bienes jurídicos, como se ha mencionado.

Si a la tesitura anterior, le adicionamos que las autoridades norteamericanas competentes no velaban por la aplicación de la propia Decisión, así como que su contenido incluía una serie de excepciones —donde se situaba en primer lugar, la relativa al cumplimiento de las exigencias de seguridad nacional, interés público y cumplimiento de la ley— y garantías que funcionaban bajo un principio de discrecionalidad interpretado por parte de éstas. Se produce así, un escenario de manifiesta incertidumbre que acabará provocando que la Comisión Europea se tenga que pronunciar en 2013, para intentar apaciguar la situación de inseguridad que se había venido generando, proponiendo una serie de recomendaciones y propuestas de trabajo para reestablecer la confianza estratégica que unía a ambos territorios y seguir permitiendo el intercambio transatlántico de datos personales.

Dichos esfuerzos no obtendrán ninguna recompensa —ni en el ámbito político, ni en el legislativo—, puesto que las revelaciones efectuadas por E. Snowden supondrán un

punto de inflexión, que aunado con las actuaciones llevadas a cabo por M. Schrems, sustentarán que, en fecha, 6 de octubre de 2015, el TJUE determine la invalidez de la Decisión y declare la imposibilidad de efectuar transferencias internacionales a los Estados Unidos de América. El Alto Tribunal comunitario también aprovechó dicho pronunciamiento para responsabilizar a la Comisión Europea por no haber efectuado las comprobaciones necesarias que hubieran permitido determinar con exactitud que los EE. UU. no gozaban de un nivel de protección adecuado para ser el destinatario de los datos personales de ciudadanos de la Unión.

En los años venideros a las revelaciones efectuadas por E. Snowden, se propiciaron una serie de instrumentos normativos en el ordenamiento jurídico estadounidense tendentes a reaccionar ante las acusaciones que se habían vertido sobre las prácticas abusivas que se llevaban a cabo en materia de vigilancia y obtención de información por parte de las agencias de inteligencia norteamericanas. Dichos esfuerzos legislativos realizados no serían suficientes para garantizar el nivel de protección adecuado de los EE. UU. Tal y como tendría ocasión de constatar posteriormente el propio TJUE[896], recordando que una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización no daría cobertura suficiente de protección sobre el derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la CDFUE.

No obstante a lo anterior, tras más de dos años de negociaciones, el 16 de julio de 2016 se aprueba el segundo acuerdo de intercambio de datos entre la Unión Europea y los EE. UU., a través de la Decisión de Ejecución (UE) nº 2016/1250, emitida por parte de la Comisión Europea. A pesar de introducir una serie de novedades en virtud de los mandamientos contenidos en el pronunciamiento del TJUE, las mismas no resultarían suficientes. En idénticos términos que le había sucedido a su antecesor, desde un primer momento fue objeto de críticas por parte de distintos organismos comunitarios —como

[896] *Vid*. STJUE. Asunto C-362/14 (Schrems I), cit., apdos. 93-94.

el GT29, el SEPD y el propio Parlamento Europeo— motivadas precisamente por las deficientes garantías que se establecían en su contenido respecto la protección de los derechos y libertades de los afectados situados en la Unión.

Dichas deficiencias serían sucesivamente puestas de manifiesto en las distintas revisiones que se efectuaban sobre la eficacia del acuerdo por parte del GT29 o la propia Comisión, entre otros organismos comunitarios. La situación se sustanciará nuevamente con la invalidación del acuerdo vigente entre ambos territorios, esto es, la Decisión de Ejecución (UE) nº 2016/1250. Entre las diversas cuestiones que fundamentaran el pronunciamiento por parte del TJUE, se puede encontrar la ausencia de límites tangibles que impusieran restricciones a las actuaciones realizadas por las agencias de inteligencia norteamericanas bajo el mandato de la Sección 702 de la FISA[897], así como la inexistencia de garantías específicas que pusieran de manifiesto la efectividad e independencia de la figura del Defensor del Pueblo respecto al poder ejecutivo[898]. Como se ha comprobado, el pronunciamiento del TJUE obligará a que múltiples organismos comunitarios tengan que pronunciarse al respecto.

SEXTA. – Se puede manifestar que las iniciativas legislativas que se han producido en el contexto comunitario en relación con la protección del derecho fundamental a la protección de los datos personales han supuesto un notable impulso para la regulación de este derecho a nivel internacional. Como se ha apuntado, una especie de "efecto Bruselas" parece haberse apoderado de los poderes legislativos de distintos Estados para proceder al desarrollo de su contenido. Pero este interés de terceros países no es fortuito, sino que tiene como objetivo la obtención de la categorización como "adecuada" de su respectiva legislación nacional que desarrolle la materia. Lo que equivale a admitir que los datos personales podrán circular libremente desde la Unión Europea y/o los países integrantes del EEE a ese tercer país, y que, por lo tanto, su explotación será susceptible de valoración económica.

Dicha concepción no ha pasado inadvertida en el contexto asiático, sino que en los últimos años ciertos países de dicho continente han ido mostrando paulatinamente su interés en obtener tal "homologación". Un buen ejemplo de ello, lo encontramos con el

[897] *Vid.* Apartados 291, 292 y 297 de las conclusiones del Abogado General Sr. Henrik Saugmandsgaard Øe sobre el asunto C-311/18.

[898] *Ibidem,* apdo. 337.

último de los casos avalados con una decisión de adecuación, esto es, Japón, que hace escasamente un año ha obtenido la consideración de país con un nivel de protección adecuado. Al anterior, se le sumará en breve Corea del Sur, que se encuentra en trámites para su obtención —después de sendas negociaciones efectuadas desde el pasado año 2015—. Con todo ello, podemos advertir que no se trata pues de un hecho puntual y meramente anecdótico, sino que el creciente interés de ciertos países asiáticos en conseguir la "categorización" a la que venimos haciendo alusión se ha convertido en una realidad claramente contrastada.

No obstante, al abordar el contexto asiático, debe tenerse en cuenta que estamos analizando un sistema político, económico y social diferente al que se puede encontrar en el ámbito comunitario. En este último encontramos democracias consolidadas, dotadas de sistemas electorales que velan por garantizar un relevo de los partidos políticos gobernantes y de las instituciones judiciales —con sus correspondientes imperfecciones—. En contraposición, en Asia podríamos llegar a afirmar que estas "realidades" europeas no se corresponden con la situación existente en los países asiáticos. Si bien alguno de ellos dispone de un sistema democrático parecido al europeo, la mayoría se encuentran en proceso de consolidación de lo que se vendría a denominar como un "estado de derecho". Lo que dificulta la consolidación del derecho a la protección de datos como fundamental.

Las Directrices elaboradas por la OCDE, como el propio Convenio 108 y la Directiva 95/46/CE, sentaron las bases de la evolución de este derecho en los territorios asiáticos, a pesar de que no disponen de acuerdos vinculantes sobre la materia, así como tampoco de tribunales que velen por el cumplimiento de un derecho fundamental a la protección de los datos de carácter personal. Si bien es cierto que, en general, las Constituciones de la mayoría de los países asiáticos que han podido avanzar más en la consecución de ese "estado de derecho" al que se hacía mención reconocen un derecho fundamental a la protección de los datos de carácter personal, ya sea manifestado de manera expresa o indirectamente, según el caso.

Los únicos acuerdos internacionales que existen en Asia sobre la materia se reducen a las escasas palabras que se contienen en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos. Pero, en cualquier caso, no pueden compararse en exceso con el régimen que se establece al respecto en la Unión Europea, pues se trata de sistemas antagónicamente diferentes. Lo anterior se hace más evidente, si tenemos en cuenta las

prácticas que han ido extendiéndose entre los países asiáticos en relación con la vigilancia sistemática de sus ciudadanos. Situación que la pandemia ha evidenciado de manera flagrante.

Por lo tanto, se puede concluir que la brecha en garantía de derechos y libertades entre la Unión Europea y el gigante asiático se agranda aún más tras esta crisis global sanitaria y que, salvo en casos excepcionales como el de Japón —y próximamente Corea del Sur—, la legislación de protección de datos existentes en los países asiáticos no daría cumplimiento a las consideraciones establecidas por el RGPD, aspecto que imposibilitaría la obtención por parte de estos países asiáticos del nivel de protección adecuado avalado por parte de la Comisión Europea. Esta falta de homologación con la legislación europea, del mismo modo que ocurre con otros países asiáticos, tiene un impacto muy negativo en las transacciones comerciales con la Unión altamente ligadas a la "economía del dato", tal y como se ha podido ir observando a través de los distintos apartados del presente estudio.

BIBLIOGRAFÍA

MONOGRAFÍAS Y OBRAS COMPUESTAS

ALCARAZ VARÓ, E., *El inglés jurídico norteamericano*, Barcelona: Ed. Ariel, 2001, pp. 13-17

ALDECOA LUZÁRRAGA, F. y GUINEA LLORENTE, M., *La Europa que viene: el Tratado de Lisboa*, Madrid: Ed. Marcial Pons, 2010

ALMUZARA ALMAIDA, C., *Estudio práctico sobre la protección de datos de carácter personal,* Valladolid: Ed. Lex Nova, 2007, pp. 383-417

ALONSO BLAS, D., "La aplicación de la directiva europea de protección de datos en España: reformas necesarias en la L.O.R.T.A.D.", en *X Encuentro sobre Informática y Derecho*, Madrid: Ed. Universidad Pontificia Comillas, 1996

ALONSO GARCÍA, R., "Derechos fundamentales y Comunidades Europeas", en *Estudios sobre la Constitución española. Homenaje al Profesor E. García de Enterría*, Tomo II, Madrid: Ed. Civitas, 1991

ALONSO GARCÍA, R., "Las cláusulas horizontales de la Carta de los derechos Fundamentales de la Unión Europea", en GARCÍA DE ENTERRÍA, E. y ALONSO GARCÍA, R. (Dirs.), La *encrucijada constitucional de la Unión Europea*, Madrid: Ed. Civitas, 2002, pp. 151-210

ÁLVAREZ CIENFUEGOS, J. M., *La defensa de la intimidad de los ciudadanos y la tecnología informática*, Pamplona: Ed. Aranzadi, 1999

ÁLVAREZ CIVANTOS, O. J., *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*, Granada: Ed. Comares, 2001, pp. 88-111

ÁLVAREZ CONDE, E., *Curso de Derecho Constitucional I*, Madrid: Ed. Tecnos, 2006, pp. 385-389

ÁLVAREZ HERNANDO, J., *Prácticum Protección de Datos 2018*, Navarra: Ed. Aranzadi, 2017

APARICIO SALOM, J., *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Cizur Menor (Navarra): Ed. Aranzadi, 2002, pp. 57-59, 109-119

ARENAS GARCÍA, R. y PÉREZ FRANCESCH, J. L., "Extranjería (II) entrada en el espacio Schengen y permanencia en España", en GETE-ALONSO Y CALERA, M. C. y SOLÉ RESINA, J. (Coord.), *Tratado de Derecho de la Persona Física*, Vol. II, Navarra: Ed. Civitas, 2013, pp. 467-536

ARENAS RAMIRO, M., *El derecho fundamental a la protección de datos personales en Europa*, Valencia: Ed. Tirant lo Blanch, 2006

ARIZMENDI GUTIÉRREZ, M. E., "El cumplimiento de la normativa de protección de datos en el sector público: Protección de datos y Administración electrónica. El cumplimiento de la normativa de protección de datos en la administración electrónica", en VV.AA., *20 años de protección de datos en España*, Madrid: Ed. Agencia Española de Protección de Datos, 2015, p. 235

ARRIBAS LUQUE, J. M., "Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los EE. UU.: El sistema de principios de Puerto Seguro", en Diario La Ley, nº 5497 (Sección Doctrina) (2002), p. 3

ARZOZ SANTIESTEBAN, X., "Artículo 8: derecho al respeto de la vida privada y familiar", en *Convenio Europeo de Derechos Humanos. Comentario sistemático*, Navarra: Ed. Thomson-Reuters (Civitas), 2009

AYALA, J. E., "Lisboa, por fin: el tratado abre una nueva era en la UE", en *Política exterior 24*, nº 133 (2010), pp. 13-20

BAYO DELGADO, J., "Derecho comunitario sobre protección de datos", en GÓMEZ MARTÍNEZ, C. (Dir.), en *"Derecho a la intimidad y nuevas tecnologías"*, Madrid: Ed. Cuadernos de Derecho Judicial IX-2004, Consejo General del Poder Judicial, 2004, pp. 59-60

BENNY, Y. Y. T., "Hong Kong: Maintaining a Common Law Legal System in a Non-Western Culture", en BLACK A. y BELL G., *Law and Legal Institutions of Asia: Traditions, Adaptions and Innovations,* Cambridge: Ed. Cambridge University Press, 2011, pp. 62 y ss

BRAGE CAMEZANO, J., "Aproximación a una teoría general de los derechos fundamentales en el Convenio Europeo de Derechos Humanos", en *Revista Española de Derecho Constitucional,* nº 74 (2005)

BUENO GALLARDO, E., *La configuración constitucional del derecho a la intimidad. En particular, el derecho a la intimidad de los obligados tributarios,* Madrid: Ed. Centro de Estudios Políticos y Constitucionales, 2009, pp. 424-434

CAMP, L. J., *Trust and Risk in Internet Commerce*, Cambridge: Ed. Massachusetts Institute of Technology Press, 2000, pp. 99-114

CAMPUZANO, H., *Vida privada y datos personales,* Madrid: Ed. Tecnos, 1999

CÁRDENAS ARTOLA, I., FERRERO RECASENS, E. y VV.AA., *Memento experto. Protección de datos,* Madrid: Ed. Francis Lefebvre, 2012, p. 130

CARRILLO LÓPEZ, M., *El derecho a no ser molestado. Información y vida privada*, Cizur Menor (Navarra): Ed. Thomson-Aranzadi, 2003, pp. 91-101

CASAS BAAMONDE, M. E., "El derecho a la Protección de Datos de carácter personal en la Jurisprudencia del Tribunal Constitucional", en VV. AA., *20 años de protección de datos en España,* Madrid: Ed. Agencia Española de Protección de Datos, 2015, pp. 91-129

CATALINA BENAVENTE, M. A., "La transmisión de los datos PNR en la lucha contra el terrorismo y otras formas de delincuencia grave", en COLOMER HERNÁNDEZ, I. (Dir.), OUBIÑA BARBOLLA, S. (Coord.), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Ed. Thomson Reuters-Aranzadi, 2015, pp. 301-356

CATE, F. H., *Privacy in the Information Age*, Washington: Ed. Brookings Institution Press, 1997, p. 22

CHARLESWORTH, A., "Data Privacy in Cyberspace: Not National vs. International but Commercial vs. Individual", en EDWARDS, L. y C. WAELDE, C. (Coord.), *Law and the Internet,* Oxford: Ed. Hart, 2000, pp. 79-122

CHEMERINSKY, E., *Constitutional Law: Principles and Policies,* Nueva York: Ed. Wolters Kluwer (Aspen Publishing Co.), 2015

CHESTERMAN, S. (Ed.), *Data Protection Law in Singapore. Privacy and Sovereignity in a Interconnected World*, Singapur: Ed. Academy Publishing, 2014

CHIBA, M. "Japan", en Tan, Poh-Lin (Ed.), *Asian Legal Systems: Law, Society and Pluralism in East Asia*, Ed. Butterwoths, 1997

CHUECA SANCHO, A. G., "Por una Europa de los derechos humanos: la adhesión de la Unión Europea al Convenio Europeo de Derechos Humanos", en *Unión Europea y Derechos fundamentales en perspectiva constitucional*, Madrid: Ed. Dykinson, 2004, pp. 37-58

COOLEY, T. M., *A Treatise on the Constitutional Limitations Which Rest upon the Legislative Power of the States of the American Union*, Boston: Ed. Brown & Co., 1879, pp. 299-305

COOLEY, T. M., *A Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract*, Chicago: Callaghan & Co., 1879

CORCUERA, J., *La protección de los derechos fundamentales en la Unión Europea*, Madrid: Ed. Dykinson, 2002

CURTIS, G. T., *History of the Origin, Formation, and Adoption of the Constitution of the United States; with Notices of its Principal Framers*, Nueva York: Ed. Harper and Brothers, 2010

D'ATENA, A., "La Constitución oculta de Europa (antes y después de Lisboa)", en *Revista de derecho constitucional europeo*, nº 13 (2010), pp. 17-46

DAVARA RODRÍGUEZ, A. (Dir.), *Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones (TIC)*, Madrid: Ed. Fundación Vodafone, 2004, pp. 15-27, 38-56

DAVARA RODRÍGUEZ, A., *El abogado y la protección de datos*, Madrid: Ed. Ilustre Colegio de Abogados de Madrid, 2004, p. 34

DAVARA RODRÍGUEZ, A., *La protección de datos en Europa*, Madrid: Ed. Grupo ASNEF-Equifax / Universidad Pontificia de Comillas, 1988

DAVARA RODRÍGUEZ, M. A., *Derecho Informático*, Pamplona: Ed. Aranzadi, 1993, p. 64.; GARZÓN CLARIANA G., "La protección de los datos personales y la

función normativa del Consejo de Europa", en *Revista de Instituciones Europeas*, vol. 8, nº 1 (enero-abril de 1981), p. 18

DE CASTRO Y BRAVO, F., "Los llamados derechos de la personalidad", en *Anuario de Derecho Civil,* 1959, pp. 1237-1275

DE LA IGLESIA GARCÍA, J., "La entrada en vigor del Tratado de Lisboa", en *Revista Universitaria Europea*, nº 12 (2010), pp. 45-60

DE MIGUEL ASENSIO, P. A., "Nota a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal", en *Anuario de Derecho internacional Privado,* Vol. I (2001), Madrid: Ed. Iprolex, pp. 626-627

DEL CASTILLO VÁZQUEZ, I. C., *Protección de datos: cuestiones constitucionales y administrativas: el derecho a saber y la obligación de callar*, Madrid: Ed. Civitas, 2007, pp. 136-139

DEL PESO NAVARRO, E. y RAMOS GONZÁLEZ, M. A., *La seguridad de los datos de carácter personal,* Madrid: Ed. Díaz de Santos, 2002, pp. 112-117

DEL PESO NAVARRO, E. y RAMOS, M. A., *LORTAD. Análisis de la Ley*, Ed. Díaz de Santos, 1994, pp. 169-180

DURÁN CARDO, B., *La figura del responsable en el derecho a la protección de datos. Génesis y evolución normativa ante el cambio tecnológico y en perspectiva multinivel*, Barcelona: Ed. Universidad Autónoma de Barcelona, 2015, p. 301

ESPÍN TEMPLADO, E., "Los derechos de la esfera personal", en *Derecho Constitucional, Vol. I*, Valencia: Ed. Tirant lo Blanch, 1994, p. 208

ESTADELLA YUSTE, O., "La transmisión internacional de datos personales y su control", en *Jornadas sobre Derecho Español de Protección de Datos Personales,* Madrid: Ed. Agencia de Protección de Datos, 1996, p. 195

ESTADELLA YUSTE, O., "La transmisión internacional de datos y su control", en *Jornadas sobre el Derecho español de la Protección de Datos Personales*, Madrid: Agencia de Protección de Datos, 1996, págs. 197 y ss.

ESTADELLA YUSTE, O., *La protección de la intimidad frente a la transmisión internacional de datos personales,* Madrid: Ed. Tecnos, 1995, pp. 65-66

FERNÁNDEZ TOMÁS, A., *La Carta de Derechos Fundamentales de la Unión Europea. Diez años de jurisprudencia*, Valencia: Ed. Tirant lo Blanch, 2001, pp. 84-89

FERNÁNDEZ-LONGORIA, P. y FERNÁNDEZ-SAMANIEGO, J., *Comentarios a la Ley Orgánica de Protección de Datos Personales*, Pamplona: Thomson Reuters, 2010, p. 1779

FLAHERTY, D. H. (1972). *Privacy in Colonial New England*, University Press of Virginia, Charlottesville

FREIXAS GUTIÉRREZ, G., *La protección de los datos de carácter personal en el Derecho español. Aspectos teóricos y prácticos*, Barcelona: Ed. Bosch, 2001, pp. 345-356

GARRIGA DOMÍNGUEZ, A., *La protección de los datos personales en el derecho español*, Dykinson, Madrid, 1999, pp. 295-337

GARRIGA DOMÍNGUEZ, A., *Tratamiento de datos personales y derechos fundamentales*, Madrid: Ed. Dykinson, 2004, pp. 177-181

GARZÓN, G., *El marco jurídico del flujo de datos transfronteras*, Doc. TDF 102, Roma: Ed. IBI, 1981

GAY FUENTES, C., *Intimidad y tratamiento de datos en las Administraciones Públicas*, Madrid: Ed. Editorial Complutense, 1995, pp. 22-25

GONZÁLEZ CAMPOS, J., SÁNCHEZ RODRIGUEZ, L. y ANDRÉS SÁENZ DE SANTA MARÍA, M. P., *Curso de Derecho Internacional Público*, Madrid: Ed. Thomson-Civitas, 2003, pp. 280-287

GONZÁLEZ FUSTER, G., *"The Emergence of Personal Data Protection as a Fundamental Right of the EU"*, Suiza: Springer, 2014, pp. 163-205

GREENLEAF, G. "Singapore—Uncertain Scope, Strong Powers", en *Asian Data Privacy Laws*, Oxford, 2017, pp. 25 y 26

GREENLEAF, G., "The Right to Privacy in Asian Constitutions", en *Oxford Handbook of Constitutional Law in Asia*, Oxford: Ed. Oxford University Press, 2020

GREENLEAF, G., *Asian Data Privacy. Trade and Human Rights Perspectives*, Oxford: Ed. Oxford University Press, 2014

GUERRERO PICÓ, M. C., *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Navarra: Ed. Thomson-Reuters (Civitas), 2006, p. 50

GUICHOT, E., *Datos personales y Administración Pública*, Madrid: Ed. Civitas, 2005, pp. 226-234

HEREDERO HIGUERAS, M., *La Directiva Comunitaria de protección de los datos de carácter personal*, Madrid: Ed. Tecnos, 1998, p. 188

HEREDERO HIGUERAS, M., *La Directiva Comunitaria de Protección de los Datos de Carácter Personal. Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/C.E., 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*, Pamplona: Ed. Aranzadi, 1997

HEREDERO HIGUERAS, M., *La Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal: comentarios y textos*, Madrid: Ed. Tecnos, 1996

HERRÁN ORTIZ, A. I., "La protección de datos personales en la jurisprudencia constitucional", en ECHANO BASALDÚA, J. I. (Coord.), *Estudios jurídicos en memoria de José María Lidón*, Universidad de Deusto, 2002, pp. 985-1000

HERRÁN ORTIZ, A. I., *El derecho a la intimidad en la nueva Ley orgánica de protección de datos personales*, Dykinson, Madrid, 2002, pp. 115-194

HERRÁN ORTIZ, A. I., *El derecho a la protección de datos personales en la sociedad de la información*, Bilbao: Ed. Cuadernos Deusto de derechos Humanos, Universidad de Deusto, 2003, p. 181

KERR, O. S., *Computer Crime Law*, Ed. West Academic Publishing, 2ª Edición, 2013, p. 813

KONEFSKY, S. J., *The Legacy of Holmes and Brandeis*, Nueva York: Macmillan & Co., 1956

KRIS, D. S. y WILSON, J. D., *National Security Investigations and Prosecutions*, Ed. Thomson-Reuters, 2019

LESMES SERRANO, C., *La ley de protección de datos. Análisis y comentario de su jurisprudencia*, Valladolid: Ed. Lex Nova, 2007, pp. 50-58

LESSIG, L., *El código y otras leyes del ciberespacio*, Taurus: Ed. Madrid, 2001

LO, C., "Taiwan-External Influences Mixed with Traditional Elements to Form Its Unique Legal System", en BLACK A. y BELL G., *Law and Legal Institutions of Asia: Traditions, Adaptions and Innovations*, Cambridge: Ed. Cambridge University Press, 2011, p. 94

LÓPEZ RAMÓN, L., "La Agencia de Protección de Datos como Administración Independiente en el Derecho Español y Comunitario Europeo", en *Jornadas sobre el Derecho Español de la Protección de Datos Personales*, Madrid: Ed. Agencia de Protección de Datos, 1996, pp. 252-254

LUCAS MURILLO DE LA CUEVA, P., "La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad", en *El derecho a la autodeterminación informativa*, Madrid: Ed. Fundación Coloquio Jurídico Europeo, 1993, pp. 81-179

LUCAS MURILLO DE LA CUEVA, P., "Las Funciones de la Agencia de Protección de Datos", en *Jornadas sobre el Derecho Español de la Protección de Datos Personales*, Madrid: Ed. Agencia de Protección de Datos, 1996, pp. 263-267

LUCAS MURILLO DE LA CUEVA, P., "Las vicisitudes del Derecho de la protección de datos personales", en VV. AA., *La democracia constitucional: estudios en homenaje al profesor Rubio Llorente*, Vol. I, Madrid: Ed. Centro de Estudios Políticos y Constitucionales, 2001, pp. 513-515

LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa*, Madrid: Ed. Tecnos, 1990, p. 26

LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales*, Madrid: Ed. CEC, 1993, pp. 64-69

MACDONALD, D. A., "Privacy, Self-Regulation, and the Contractual Model: A Report from Citicorp Credit Services, Inc.", en WELLBERY, B. S. (Coord.), *Privacy and Self-Regulation in the Information Age*, U.S. Department of Commerce, 1997

MADEC, A., *Les flux transfrontières de dones*, París, 1982

MANGAS MARTÍN, A., "El compromiso con los derechos fundamentales", en MANGAS MARTÍN, A. (Dir.), *Carta de los Derechos Fundamentales en la Unión Europea*, Madrid: Ed. Fundación BBVA, 2008, pp. 31-75

MARTÍN CASALLO, J. J. y MARTÍN PALLÍN, J. A., "Intimidad, privacidad y protección en la nueva Ley Orgánica 15/1999", en DAVARA RODRÍGUEZ, A. (Coord.), *XIV Encuentros sobre Informática y Derecho 2000-2001*, Navarra: Ed. Aranzadi, 2001, pp. 51-53, 55-59

MARTÍN-CASALLO, J. J., "La Directiva 95/46/C.E. y su incidencia en el ordenamiento jurídico español", en *Jornadas sobre el Derecho Español de la protección de datos personales*, Madrid: Ed. Agencia de Protección de Datos, 1996

MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica a la autodeterminación informativa*, Madrid: Ed. Civitas, 2004, pp. 237-244

MATUS ARENAS, J., "Transferencias internacionales a países con niveles adecuados y no adecuados de protección Aspectos prácticos", en *Ponencia para el Seminario Regional de Protección de Datos*, Uruguay, 2010, p. 4

MEDINA GUERRERO, M., "La articulación de las jurisdicciones constitucional y ordinaria en la tutela de las libertades de expresión e información", en VV. AA., *La democracia constitucional: estudios en homenaje al profesor Rubio Llorente*, Vol. II, Madrid: Ed. Centro de Estudios Políticos y Constitucionales, 2002, pp. 1669-1700

MEDINA GUERRERO, M., *La vinculación negativa del legislador a los derechos fundamentales*, Madrid: Ed. MCGraw-Hill, 1996, p. 11

MILLÁN MORO, L., "El ordenamiento jurídico comunitario: del Tratado Constitucional al Tratado de Lisboa", en *Revista de Derecho Comunitario Europeo*, nº 36 (2010), pp. 401-438

MILLER, A. R. y ARBOR, A., *The Assault on Privacy: Computers, Data Banks and Dossiers,* Ed. The University of Michigan Press, 1971, p. 170

MIRABELLI, G., "In tema di tutela dei dati personali (note a margine della proposta modificata di direttiva C.E.E.", en *Il diritto dell'informazione e dell'informatica*, 1993, pp. 609-615

MONTOTO I MANENT, J., *Gihadisme: l'amenaça de l'islamisme radical a Catalunya,* Barcelona: Ed. Angle Editorial, 2012

MORRISON, T. W., *The Story of United States v. United States District Court (Keith): The Surveillance Power*, Nueva York (Estados Unidos): Ed. Schroeder C.H. & Bradley C.A., Presidential Power Stories, 2008

MULLIGAN, D. K. y GOLDMAN, J., "The Limits and the Necessity of Self-Regulation: The Case for Both", en WELLBERY, B. S., (Coord.) *Privacy and Self-Regulation in the Information Age*, U.S. Department of Commerce, 1997

N. LUGARESI, N., *Internet, Privacy e Pubblici Poteri negli Stati Uniti,* Milán: Ed. Giufrè, 2000, pp. 107-128

OLLERO TASSARA, A., *De la protección de la intimidad al poder de control sobre los datos personales. Exigencias jurídico-naturales e historicidad en la jurisprudencia constitucional,* Madrid: Ed. Real Academia de Ciencias Morales y Políticas, 2008, p. 127

ORTEGA GIMÉNEZ, A., *Código de Protección de Datos de Carácter Personal*, Madrid: Ed. Difusión Jurídica, 2008, pp. 337-449

ORTEGA GIMÉNEZ, A., *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*, Madrid: Ed. Agencia Española de Protección de Datos, 2015, p. 27

PÉREZ FRANSCESCH, J. L., GIL MÁRQUEZ, T., GACITÚA ESPÓSITO, A., "Informe sobre el PNR. La utilización de datos personales contenidos en el registro de nombre de pasajeros: ¿fines represivos o preventivos?", en *Working Paper*, nº 297 (2011), Ed. ICPS, Barcelona

PÉREZ LUÑO, A. E., "El consentimiento de los menores: Título II. Principios de la Protección de Datos. artículo 6", en TRONCOSO REIGADA, A. (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid: Civitas, 2010, pp. 473-494

PÉREZ LUÑO, A. E., "El derecho a la autodeterminación informativa", *Anuario de jornadas 1989-1990*, Ed. Servicio de Estudios del IVAP, 1991, pp. 299-331

PÉREZ LUÑO, A. E., "Libertad informática y derecho a la autodeterminación informativa", en *I Congreso sobre Derecho Informático*, Ed. Facultad de Derecho de la Universidad de Zaragoza, 1989, pp. 359-375

PÉREZ LUÑO, A. E., *Cibernética, informática y derecho. Un análisis metodológico*, Bolonia: Ed. Publicaciones del Real Colegio de España, 1976, pp. 133-142

PÉREZ LUÑO, A. E., *Derechos humanos, estado de derecho y Constitución*, Madrid: Ed. Tecnos, 2005, pp. 378-385

PÉREZ LUÑO, A. E., *La tercera generación de derechos humanos*, Cizur Menor (Navarra): Ed. Thomson-Aranzadi, 2006, pp. 31-32

PÉREZ LUÑO, A. E., *Los derechos humanos en la sociedad tecnológica*, Madrid: Ed. Universitas, 2012, pp. 175-180

PÉREZ LUÑO, A. E., LOSANO, M. y GUERRERO MATEUS, M. F., *Libertad informática y leyes de protección de datos personales*, Madrid: Ed. Centro de estudios constitucionales, 1989

PÉREZ LUÑO, A. E., *Manual de Informática y Derecho*, Barcelona: Ed. Ariel, 1996, p. 45

PÉREZ LUÑO, A. E., *Problemas actuales de la documentación y la informática jurídica: actas del coloquio internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986*, Madrid: Ed. Fundación Cultural Enrique Luño Peña, 1987, pp. 268-276

PÉREZ ROYO, J., *Lecciones de Derecho Político I*, Sevilla: Ed. Minerva, 1993, p. 24

PIÑAR MAÑAS, J. L. y RECIO GAYO, M., *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, Ed. Wolters Kluwer, 2018, pp. 156-160

PIÑAR MAÑAS, J. L., "Introducción Hacia un nuevo modelo europeo de Protección de Datos", en PIÑAR MAÑAS, J. L. (Dir.)., *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad*, Madrid: Ed. Reus, 2016, p. 17

PIÑAR MAÑAS, J. L., "Protección de datos: origen, situación actual y retos de futuro", en *El derecho a la autodeterminación informativa*, Madrid: Ed. Fundación Coloquio Jurídico Europeo, 2009, pp. 98-105

PIÑAR MAÑAS, J. L., "Transferencias de datos personales a terceros países u organizaciones internacionales", en PIÑAR MAÑAS, J. L. (Dir.)., *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad*, Madrid: Reus, 2016, pp. 431-460

PIÑOL I RULL, J. y ESTADELLA YUSTE, O., "La regulación de la transmisión internacional de datos en la L.O. 5/1992 de 29 de octubre", en RIPOLL I CARULLA, S. (Coord.), *La protección de los datos personales: regulación nacional e internacional de la seguridad informática*, Barcelona: Ed. Universitat Pompeu Fabra, 1993, pp. 78-79

PIÑOL RULL, J. L. y ESTADELLA YUSTE, O., "La regulación del flujo internacional de datos", en *La protección de los datos personales: regulación nacional e internacional de la seguridad informática*, Barcelona: Ed. Centro de Investigación de la Comunicación de la Universidad Pompeu Fabra, 1993, pp. 75-91

PIÑOL RULL, J., *Los flujos internacionales de datos: aproximación a su regulación jurídica*, Tomo IV, Barbastro: Ed. U.N.E.D., 1987, págs. 137 y ss.

PIZZORUSSO, A., "Sul diritto alla riservatezza nella Costituzione italiana", en *Prassi e teoría*, 1976

PUENTE ESCOBAR, A., "Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal", en PIÑAR MAÑAS, J. L. (Dir.), *Protección de datos de carácter personal*

en Iberoamérica, Valencia: Ed. Agencia Española de Protección de Datos / Tirant lo Blanch, 2006, pp. 37-67

QUILEZA AGRADA, E., "El derecho a la protección de los datos en la jurisprudencia constitucional", en DAVARA RODRÍGUEZ, A. (Coord.), *III Jornadas sobre informática y sociedad*, Madrid, 2001, pp. 187-196

RAUSTIALA, K., *Does the Constitution Follow the Flag? The Evolution of Territoriality in American Law*, Ed. Oxford University Press, 2009, pp. 157-186

REBOLLO DELGADO, L. y SERRANO PÉREZ, M. M., *Introducción a la protección de datos*, Madrid: Ed. Dykinson, 2008, pp. 32-33

REBOLLO DELGADO, L. y SERRANO PÉREZ, M. M., *Manual de protección de datos*, Madrid: Ed. Dykinson, 2014, pp. 72-73

REBOLLO DELGADO, L., *Derechos fundamentales y protección de datos*, Madrid: Ed. Dykinson, 2004, p. 132

REMOLINA ANGARITA, N., *Recolección internacional de datos personales: un reto del mundo post-internet*, Madrid: Ed. Agencia Estatal Boletín Oficial del Estado, 2015, pp. 95-97

RIPOLL CARULLA, S., "El Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal: Balance a los siete años de su apertura a la firma", en *Actas del Congreso sobre Derecho Informático*, Zaragoza: Ed. Facultad de Derecho, 1989, pp. 395-413

RODRÍGUEZ BEREIJO, A. y GARCÍA DE ENTERRÍA, E., "El valor jurídico de la Carta de los Derechos Fundamentales de la Unión Europea después del Tratado de Niza", en GARCÍA DE ENTERRÍA, E. y ALONSO GARCÍA, R. (Dirs.), *La encrucijada constitucional de la Unión Europea*, Madrid: Ed. Civitas, 2002, p. 210

RUBIN, P. H. y LENARD, T. M., *Privacy and the commercial use of personal information*, Boston: Ed. Wolters Kluwer, 2002, p. 100

RUBIO LLORENTE, F., *La forma del poder. Estudio sobre la constitución*, Madrid: Ed. Centro de Estudios Políticos y Constitucionales, 2013, pp. 5-41

RUÍZ CARRILLO, A., *"Los datos de carácter personal. Concepto, requisitos de circulación, procedimientos y formularios"*, Barcelona: Ed. Bosch, 1999, p. 109

RUIZ CARRILLO, A., *La protección de datos de carácter personal*, Barcelona: Ed. Bosch, 2001

RUIZ MIGUEL, C., *El Derecho a la Protección de la Vida Privada en la Jurisprudencia del Tribunal Europeo de Derechos Humanos*, Ed: Thomson - Reuters (Civitas), 1994

RUIZ MIGUEL, C., *La Configuración Constitucional del Derecho a la Intimidad*, Madrid: Ed. Tecnos, 1995

SANCHO VILLA, D., *Negocios Internacionales de Tratamiento de Datos Personales*, Cizur Menor (Navarra): Ed. Civitas, 2010, p. 27

SANCHO VILLA, D., *Transferencia internacional de datos personales*, Madrid: Ed. Agencia de Protección de Datos, 2003, pp. 47-52

SCHWABE, J., "Jurisprudencia del Tribunal Constitucional Federal Alemán Extractos de las sentencias más relevantes", *Programa estado de Derecho para Latinoamérica*, 2009

SCHWARTZ, P. M. y SOLOVE, D. J., *Information Privacy: Statutes and Regulations 2010-2011*, Ed. Wolters Kluwer (Aspen Publishing Co.), 2009

SERRANO PÉREZ, M. M., *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid: Ed. Civitas, 2003

SERRERA COBOS, P., *Buenas prácticas en protección de datos*, Madrid: Ed. Fundación DINTEL, 2007, pp. 28-31

SIMITIS, S., "Analyse du project de directive pour l'harmonisation des legislations", en *XII Conférence Internationale des Commissaires à la Protection des Données*, París, 1991

SOLOVE, D. J. y SCHWARTZ, P. M., *Information Privacy Law*, Nueva York: Ed. Wolters Kluwer, 2018, pp. 35-37

TÉLLEZ AGUILERA, A., *La protección de datos en la Unión Europea*, Madrid: Ed. Edisofer, 2002, pp. 59-65

TÉLLEZ AGUILERA, A., *Nuevas tecnologías, intimidad y protección de datos. Estudio sistemático de la Ley Orgánica 15/1999*, Madrid: Ed. Edisofer, 2001, pp. 107-164

TOMÁS Y VALIENTE, F., "La Constitución de 1978 y la historia del constitucionalismo español", en *Anuario de Historia del Derecho Español*, Madrid, 1980, pp. 721-751

TRONCOSO REIGADA, A., *La protección de datos personales: en busca del equilibrio*, Valencia: Ed. Tirant lo Blanch, 2010, pp. 58-59

VACCA, J. R., "The European Data Protection Directive: A Roadblock to International Trade", en R. HEROLD, R. (Coord.), en *The Privacy Papers. Managing Technology, Consumer, Employee, and Legislative Actions*, Nueva York: Ed. Auerbach publications, 2000, pp. 569-581

VELÁZQUEZ BAUTISTA, R., *Protección jurídica de datos personales automatizados*, Madrid: Ed. Colex, 1993, p. 184

VILARIÑO PINTOS, E., "La Ley de regulación del tratamiento automatizado de datos de datos de carácter personal ante el Derecho Internacional", en *La protección de datos personales. Regulación nacional e internacional de la seguridad informática*, Ed. Centro de Investigación de Comunicación, Universidad Pompeu Fabra, Generalitat de Catalunya, 1993, pp. 49-74

VILLAVERDE MENÉNDEZ, I., "La jurisprudencia del Tribunal Constitucional sobre el derecho fundamental a la protección de datos de carácter personal", en FARRIOLS I SOLÁ, A. (Coord.), *La protección de datos de carácter personal en los centros de trabajo*, 2006, pp. 48-63

VIZCAÍNO CALDERÓN, M., *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid: Ed. Civitas, 2001

WANG, J., "China: Legal Reform in an Emerging Socialist Market Economy", en BLACK, E. A., y F. BELL. G., *Law and Legal Institutions of Asia: Traditions,*

Adaptions and Innovations, Cambridge: Ed. Cambridge University Press, 2011, pp. 24 y ss

WARREN, S. D. y BRANDEIS, L., *El derecho a la intimidad*, Madrid: Ed. Thomson-Reuters, Civitas, 1890

WESTIN, A., *Privacy and Freedom*, New York: Ed. Atheneum, 1970

WOOD, G. S., *The Creation of the American Republic, 1776-1787*, University of North Carolina Press, 1998

YOON, D., "Korea", en TAN, P. (Ed.), Asian Legal Systems: Law, Society and Pluralism in East Asia, Ed. Butterwoths, 1997

YOUNGJOON, K., "Korea: Bridging the Gap between Korean Substance and Western Form", en BLACK A. y BELL G., *Law and Legal Institutions of Asia: Traditions, Adaptions and Innovations*, Cambridge: Ed. Cambridge University Press, 2011

ZABÍA DE LA MATA, J. (Coord.). y VV. AA., *Protección de datos: Comentarios al Reglamento*, Ed. Lex Nova, 2008

REVISTAS

ADAMS, A., MURATA, K. y ORITO, Y., "The Devolpment of Japanese Data Protection", en *Policy and Internet*, nº 2 (2) (2010), pp. 95-126

ALONSO GARCÍA, R., "Constitución española y Constitución europea: guion para una colisión virtual y otros matices sobre el principio de primacía", en *Revista Española de Derecho Constitucional*, nº 73 (2005), pp. 339-343

ALONSO GARCÍA, R., "El triple marco de protección de los derechos fundamentales en la Unión Europea", en *Cuadernos de Derecho Público*, nº 13 (2001), pp. 13-17

ALONSO GARCÍA, R., "La Carta de los Derechos Fundamentales de la Unión Europea", en *Gaceta jurídica de la Unión Europea y de la competencia*, nº 209 (2000), pp. 3-7

ÁLVAREZ ALONSO, C., "Los derechos y sus garantías (1812-1931)", en *Ayer*, nº 34 (1999), pp. 177-216

ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M., "Notas a la nueva regulación de la protección de datos de carácter personal", en *Revista La Ley*, nº 5036 (2000), p. 1716

ANCOS FRANCO, H., "La regulación de las transferencias internacionales de datos de carácter personal como barrera al comercio internacional: De la Directiva 95/46 a los acuerdos UE-terceros Estados", en *Revista de Derecho Comunitario Europeo*, nº 6 (1996), pp. 497-516

ARENAS RAMIRO, M., "El derecho a la protección de datos personales en la jurisprudencia del TJCE", en *Revista de Derecho y Nuevas Tecnologías*, Vol. IV, Ed. Aranzadi, 2006, pp. 95-119

ARENAS RAMIRO, M., "La protección de datos personales en los países de la Unión Europea", en *Revista jurídica de Castilla y León*, nº 16 (2008), pp. 113-168

ARGOMARIZ, J., "When the EU in the 'Norm-taker': the Passenger Name records Agreement and the EU's Internalization of US Border Security Norms", en *Journal of European Integration*, 31 (1) (2009), pp. 119-136

ARREBOLA, C., MAURICIO, A. J., JIMÉNEZ PORTILLA, H., "An Econometric Analysis of the Influence of the Advocate General on the Court of Justice of the European Union", en *Cambridge Journal of Comparative and International Law*, Vol. 5, nº 1 (2016), University of Cambridge

ARZOZ SANTISTEBAN, X., "La relevancia del Derecho de la Unión Europea para la interpretación de los derechos fundamentales constitucionales", en *Revista Española de Derecho Constitucional*, nº 74 (2005), pp. 63-74

ATKINSON, L. R., "The Fourth Amendment's National Security Exception: Its History and Limits", en *Vanderbilt Law Review*, Vol. 66, nº 5 (2009), pp. 1343-1353

BALAGUER CALLEJÓN, F., "El Tratado de Lisboa en el diván. Una reflexión sobre estatalidad, constitucionalidad y Unión Europea", en *Revista española de derecho constitucional*, nº 83 (2008), pp. 57-92

BERTHOLD, M. y WACKS, R., Hong Kong Data Privacy Law: Territorial Regulation in a Borderless Word, Ed. Thomson, Sweet & Maxwell Asia, 2002

BIGNAMI, F. y RESTA, G., "Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance", en *George Washington Law School Public Law and Legal Theory Paper*, nº 2016-67 (2017), pp. 10-11

BIGNAMI, F. y RESTA, G., "Transatlantic Privacy Regulation: Conflict and Cooperation", en *Law and Contemporary Problems*, nº 78 (2015), p. 252

BIGNAMI, F., "The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens", en *George Washington Law School Public Law and Legal Theory Paper*, nº 2015-54 (2015), Washington (Estados Unidos), p. 20

BLAS, F., "Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales", en *Revista Derecho del Estado*, nº 23 (2009), p. 43

BOCK, K. *et. al.*, "Data Protection Impact Assessment for the Corona App", en *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF)*, vol. 1.6 46 e. V. (29 de abril de 2020). Consultado el 15.10.2020 desde https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3588172

BRADBURY, S. G., "Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata Under Section 215 and Foreign-Targeted Collection Under Section 702", en *Lawfare Research Paper Series*, nº 1 (2013)

BRADFORD, L., ABOY, M. y LIDDELL, K, "COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR and Data Protection Regimes", en *Journal of Law and the Biosciences, University of Cambridge Faculty of Law Research Paper*, nº 23/2020 (2020), p. 3. Consultado el 15.10.2020 desde: https://ssrn.com/abstract=3617578

BRATMAN, B. E., "Brandeis and Warren's «The Right to Privacy» and The Birth of The Right to Privacy", en *Tennessee Law Review*, nº 69 (2002), pp. 623-651

BRETAL VÁZQUEZ, M., "Convenio para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal, de 28 de enero", en *B.L.E.*, nº 4 (1982), pp. 50-76

BROUWE, E., "The EU Passenger name record System and Human Rights: Transferring passenger data or passenger freedom", en *CEPS Working Document*, nº 320 (2009), p. 5

BROUWE, E., "The EU Passenger name record System and Human Rights: Transferring passenger data or passenger freedom", en *CEPS Working Document*, nº 320 (septiembre de 2009), p. 29

CALLEWAERT, J., "To accede or not to accede: European protection of fundamental rights at the crossroads", en *Journal européen des droits de l'homme*, Vol. 2014, nº 4 (2014), pp. 500-510

CAÑABATE PÉREZ, J., "La Directiva 2016/681 de la Unión Europea sobre los datos del PNR (Passenger Register Number): ¿se ha roto el frágil equilibrio entre garantía de la protección de datos personales y seguridad?", en *Working Papers*, Ed. ICPS, Universitat Autònoma de Barcelona, 2017, p. 4

CARLIN, F. M., "The Data Protection Directive: the introduction of common privacy standards", en *European Law Review*, 1996

CARRASCOSA GONZÁLEZ, J., "Circulación internacional de datos personales informatizados y la Directiva 95/46/CE", en *Actualidad Civil*, nº 23 (1997), p. 512

CARRASCOSA GONZALEZ, J., "La Directiva 95/46/CE: Entre la protección de la intimidad y la libre transferencia internacional de datos personales automatizados", en *Economist & Jurist*, p. 30-35

CARRERA, S. y GEYER, F., "El Tratado de Lisboa y un Espacio de Libertad, Seguridad y Justicia: Excepcionalismo y Fragmentación en la Unión Europea", en *Revista de Derecho Comunitario Europeo*, nº 29 (2008), pp. 133-162

CARRILLO SALCEDO, J. A., "Notas sobre el significado político y jurídico de la Carta de los Derechos Fundamentales de la Unión Europea", en *Revista de Derecho Comunitario Europeo*, nº 9 (2001), pp. 8-9

CASTÁN TOBEÑAS, J., "Los derechos de la personalidad", en *Revista General de Legislación y Jurisprudencia*, nº julio-agosto (1952), pp. 5-62

CASTAÑO SUÁREZ, R., "Directiva 95/46, 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: Similitudes y diferencias con la Ley Orgánica 5/1992, de 29 de octubre (LORTAD)", en *Noticias de la Unión Europea*, nº 162 (1998), pp. 9-16

CATALINA BENAVENTE, M. A., "La Directiva Europea (UE) 2016/681, de 27 de abril de 2016, relativa a la utilización de los datos por en la lucha contra el terrorismo y la delincuencia grave", en *Diario La Ley*, nº 8801 (2016), p. 5

CHEN, Y. y CHEUNG, A., "The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System", en *The Journal of Comparative Law*, vol. 12, nº 2 (2017), pp. 356-378. Consultado el 15.09.2020 desde: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2992537

CHEUNG, A., "An Evaluation of Personal Data Protection in Hong Kong Special Administrative Region (1995-2012)", en *International Privacy Law*, 3 (1) (2013), pp. 29-41

CHLAPOWSKI, F. S., "The Constitutional Right to Informational Privacy", en *Boston University Law Review*, nº 71 (1991), pp. 133-136

CONDE ORTÍZ, C., *La protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad*, Madrid: Ed. Dykinson-UCA, 2005, pp. 40-47

COOLEY, T. M., "Inviolability of Telegraphic Correspondence", en *American Law Register*, nº 27 (1879), pp. 65-78

CORDERO ÁLVAREZ, C. I., "La transferencia internacional de datos con terceros Estados en el nuevo Reglamento europeo: Especial referencia al caso estadounidense y la Cloud Act", en *Revista Española de Derecho Europeo*, nº 70 (2019), Madrid: Ed. Civitas, p. 42

CRESPI, S., "The Applicability of Schrems Principles to the Member States: National Security and Data Protection within the EU Context", en *European Law Review*, nº 5 (2018), pp. 669-686

CUBERO MARCOS, J. I. y ABERASTURI GORRIÑO, U., "Protección de los datos personales en las comunicaciones electrónicas: especial referencia a la Ley 25/2007 sobre conservación de datos", en *Revista Española de Protección de Datos*, nº 83, 2008, pp. 175-197

DARANAS, M., *Boletín de Jurisprudencia Constitucional (BJC)*, nº 33 (1984), pp. 126-170

DARCY, S., "Battling for the Rights to Privacy and Data Protection in the Irish Courts", en *Utrecht Journal of International and European Law*, Vol. 31, nº 80 (2015), p. 131

DAVARA RODRÍGUEZ, A., "El escudo de privacidad", en *El Consultor de los Ayuntamientos*, nº 19 (2016), Madrid: Wolters Kluwer, 2016, p. 7

DAVARA RODRÍGUEZ, A., "La transferencia internacional de datos", en *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal*, nº 8 (2010), pp. 1320-1328

DAVARA RODRÍGUEZ, A., "La transferencia internacional de datos", en *Revista Española de Protección de Datos*, nº 1 (2007), Madrid: Ed. Agencia de Protección de Datos de la Comunidad de Madrid-CIVITAS, pp. 27-28

DAVIS M.C., "The Political Economy and Culture of Human Rights in East Asia", (2011) 1(1), en *Jindal Journal of International Affairs*, pp. 48–72

DE BURCA, G., "After the EU Charter of Fundamental Rights: the Court of Justice as a Human Rights Adjudicator?", en *Maastricht Journal of European and Comparative Law*, Vol. 20, nº 2 (2013), p. 174

DE MIGUEL ASENSIO, P. A., "Avances en la interpretación de la normativa comunitaria sobre protección de datos personales", en *La Ley Unión Europea*, nº 5964 (2003), Madrid, pp. 1-4

DE MIGUEL ASENSIO, P. A., "La protección de datos personales a la luz de la reciente jurisprudencia del TJCE", en *Revista de la Facultad de Derecho de la Universidad de Granada*, Granada, nº 7 (2003), pp. 397-417

DÍAZ DÍAZ, E., "El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones", en *Revista Aranzadi Doctrinal,* nº 6 (2016), pp. 155-190

DÍEZ PICAZO, L. M., "¿Una Constitución sin declaración de derechos? (Reflexiones constitucionales sobre los derechos fundamentales en la Comunidad Europea)", en *Revista Española de Derecho Constitucional,* nº 32 (1991)

DONOHUE, L. K., "Section 702 and the Collection of International Telephone and Internet Content", en *Harvard Journal of Law & Public Policy*, Vol 38, nº 1 (2015), pp. 119-246

DWORKIN, R., "Terror and the Attack on Civil Liberties", en *The New York Review of Books*, Vol. 50, nº 17 (2003)

ESTADELLA YUSTE, O., "The Draft Directive of the European Community Regarding the Protection of Personal Data", en *International and Comparative Law Quarterly,* nº 41 (1992), pp. 170-179

FAUGEROLAS, L., *L'accés international à des banques de dones*, París: G.L.N., 1989

FERNÁNDEZ LÓPEZ, J. M., "Flujo internacional de datos", en *Informática y Derecho: Revista Iberoamericana de Derecho Informático*, nº 30-32 (1999), págs. 189 y ss.

FERNÁNDEZ-MIRANDA LOZANA, P., "Bibliografía sobre la transición política española", en *Revista de derecho político,* nº 42 (1996), pp. 213-223

FISHMAN, W., *Legal Issues of Transborder Data Transmisión*, 74 h Meeting, P.A.S.I.L., 1980, p. 175

FLAHERTY, D. H., "On the Utility of Constitutional Rights to Privacy and Data Protection", en *Case Western Reserve Law Review*, nº 41 (1991), pp. 831-855

FRIED, C., «Privacy», en *The Yale Law Journal,* nº 77 (1968), pp. 475-493

FROSINI, V., "Banco de datos y tutela de la persona", en *Revista de Estudios Políticos*, Vol. XXX, Ed. Nueva Época, 1982, p. 21

GARCÍA BEATO, M. J., "Flujo internacional de datos personales", en *La protección del derecho a la intimidad de las personas (ficheros de datos), Cuadernos de Derecho Judicial,* Ed. Consejo General del Poder Judicial, 1997, p. 198

GARCÍA DEL POYO, R. y GARI, F., "Régimen jurídico aplicable a las transferencias internacionales y sus implicaciones en la actividad mercantil de las empresas multinacionales", en *Revista Española de Protección de Datos,* nº 2 (2007), Madrid: Ed. Agencia de Protección de Datos de la Comunidad de Madrid-Thomson-Civitas, pp. 239-266

GARZÓN CLARIANA G., "La protección de los datos personales y la función normativa del Consejo de Europa", en *Revista de Instituciones Europeas,* vol. 8, nº 1 (enero-abril de 1981), p. 18

GARZÓN CLARIANA, G. y VILARIÑO PINTOS, E., *Las leyes de protección de datos personal y su incidencia en la circulación transnacional de datos*, Roma: Ed. IBI, 1980, pp. 5-11

GAVISON, R., "Privacy and the Limits of Law", en *The Yale Law Journal,* nº 89 (1980), pp. 421-471

GLANCY, D. J., "The Invention of the Right to Privacy", en *Arizona Law Review*, Vol. 21, nº 1 (1979), pp. 1-39

GOLDMAN, L. (2006). "The Constitutional Right to Privacy", *Denver University Law Review*, nº 84, pp. 601-644

GONZÁLEZ MURÚA, A. R., "Comentario a la S.T.C. 254/1993, de 20 de julio, algunas consideraciones en torno al artículo 18.4 de la Constitución y la protección de los datos personales", en *Informática y derecho: Revista iberoamericana de derecho informático*, nº 6-7 (1994), p. 213. Consultado el 28.06.2020 desde: https://dialnet.unirioja.es/descarga/articulo/248368.pdf

GRANDE SANZ, M., "La transferencia internacional de datos personales: presente y futuro", en *Diario La Ley*, nº 8808 (2016), pp. 1-10

GREENLEAF, G. y HUI-LING, C., "Data privacy enforcement in Taiwan, Macau and China", en *Privacy Laws & Business International Report,* nº 117, 11-13, pp. 1-6

GREENLEAF, G. y LIVINGSTON, S., "PRC's New Data Export Rules: «Adequacy with Chinese Characteristics? »", en *Privacy Laws & Business International Report*, nº 147 (2017), pp. 1-8. Consultado el 15.09.2020 desde: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3026914

GREENLEAF, G., "'European' data privacy standards implemented in laws outside Europe", en *UNSW Law Research Paper*, nº 149 (2017), pp. 1-3. Consultado el 15.09.2020 desde: http://www.ssrn.com/link/UNSW-LEG.html

GREENLEAF, G., "Ch. 7. China-From Warring States to Convergence?", en *Asian Data Privacy. Trade and Human Rights Perspectives*, Oxford: Ed. University Press, 2014, pp. 191-226

GREENLEAF, G., "China's Personal Information Standard: The Long March to a Privacy Law", en *Privacy Law & Business International Report*, nº 150 (2017), pp. 1-8. Consultado el 15.09.2020 desde: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3128593

GREENLEAF, G., "Five Years of the APEC Privacy Framework: Failure or Promise?", en *Computer Law & Security Report*, nº 25 (2009), pp. 28-43. Consultado el 15.09.2020 desde: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2022907

GREENLEAF, G., "Regulations with Data Export Limitations Bring Singapore's Data Privacy Law into Force", en *Privacy Laws & Business International Report*, nº 130 (2014), pp. 1-4. Consultado el 15.09.2020 desde: https://ssrn.com/abstract=2516735

GREENLEAF, G., "Taiwan revises its Data Protection Act", en *Privacy Laws & Business International Report*, nº 108 (2010) y 109 (2011), pp. 1-9

GREENLEAF, G., "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108", en *International Data Privacy Laws*, 2012, pp. 68–92. Consultado el 15.09.2020 desde: https://papers.ssrn.com/sol3/papers.cfm?abstract_id= 2992537

GREENLEAF, G., y LIVINGSTON, S., "China's Cibersecurity Law – also a data privacy law?", en *Privacy Law & Business International Report*, nº 144 (2016), pp. 1-7. Consultado el 15.12.2020 desde: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2958658

GREENLEAG, G. y WHON-IL, P. "Korea's New Act: Asia's Toughest Data Privacy Law", en *Privacy Laws & Business International Report*, nº 117 (2012), pp. 1-6. Consultado el 15.09.2020 desde: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2120983

GUASCH PORTAS, V. y SOLER FUENSANTA, J. R., "Cloud computing: cláusulas contractuales y reglas corporativas vinculantes", en *Revista de Derecho – Universidad Nacional de Educación a Distancia (UNED)*, nº 14 (2014), pp. 257-260

GUASCH PORTAS, V., "La transferencia internacional de datos de carácter personal", en *Revista de Derecho – Universidad Nacional de Educación a Distancia*, nº 11 (2012), p. 423

HEREDERO HIGUERAS, M., "Ante la ratificación del Convenio de protección de datos del Consejo de Europa", en *Documentación Administrativa*, nº 199 (1983), pp. 753-764

HEREDERO HIGUERAS, M., "Estudio crítico de la transposición de la Directiva 95/46/CE en el ordenamiento jurídico español por la L.O. 15/1999 de 13 de diciembre", en *Revista Jurídica de Navarra*, nº 31 (2001), pp. 124-139

HEREDERO HIGUERAS, M., "La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del Censo de la Población de 1983", en *Documentación Administrativa*, nº 198 (1983), pp. 139-158

HOLMES, B. P., "US criticizes EC Data Directive's Potential Burdens and Barriers", en *Transnational Data and Communications Report*, Vol. XIV, nº 6 (1991), pp. 8-9

JAEGERA, P. T., BERTOTA, J. C. y MCCLUREA, C. R., "The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act", en *Government Information Quarterly*, pp. 295-314

JAEGERA, P. T., BERTOTA, J. C., MCCLUREA, C. R., "The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act", en *Government Information Quarterly*, Vol. 20 (2003), Issue 3, pp. 295-314

JÁUREGUI BERECIARTU, G. y UGARTEMENDÍA ECEIZABARRENA, J. I., "Europa en el lecho de Procusto: de la Constitución europea al Tratado de Lisboa", en *Revista Vasca de Administración Pública*, nº 79 (2007), pp. 105-126

JIMÉNEZ ASENSIO, R., *El Constitucionalismo: proceso de formación y fundamentos del derecho constitucional,* Madrid: Ed. Marcial Pons, 2005

JORDÁN, J., "Evolución organizativa de la militancia yihadista en España", en *Análisis del Real Instituto Elcano,* nº 12 (2014)

JORDÁN, J., "Evolución organizativa de la militancia yihadista en España", en *Análisis del Real Instituto Elcano,* nº 12/2014 (5 de marzo de 2014)

KANG, J., "Information Privacy in Cyberspace Transactions", en *Stanford Law Review*, nº 50 (1998), pp. 1193-1294

KAUNERT, C., LEONARD, S., MCKENZIE, A., "The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the cases of PNR and SWIFT", en *European Security,* nº 21 (4) (2012), pp. 474-496

KAUNERT, C., LEONARD, S., y MCKENZIE, A., "The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the cases of PNR and SWIFT", en *European Security,* nº 21 (4) (2012), pp. 474-496

KOSTA, E., COUDERT, F., DUMORTIER, J., "Data Protection in the Third Pilar: In the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive", en *International Review of Law Computer & Technology,* Volume 21 (3) (2007), pp. 347-362

KRAMER, I. R., "The Birth of Privacy Law: A Century Since Warren and Brandeis", en *Catholic University Law Review*, nº 39 (1990), pp. 703-724

KRIS, D. S., "On the Bulk Collection of Tangible Things", en *Journal of National Security Law & Policy,* Vol. 7, nº 209 (2014), pp. 209-295

KRIS, D. S., "On the Bulk Collection of Tangible Things", en *Lawfare Research Paper Series,* nº 1 (2013)

KUNER, C., "Reality and Illusion in EU Data Transfer Regulation Post Schrems", *German Law Journal,* Vol. 18, nº 14 (2017), pp. 881-918

LAWSON, C., "Japan's New Privacy Act in Context", en *University of New South Wales Law Journal*, 29 (2) (2006), pp. 88-113. Consultado el 01.06.2020 desde: http://www.austlii.edu.au/au/journals/UNSWLJ/2006/17.pdf

LÓPEZ GARRIDO, D., "Aspectos de inconstitucionalidad de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal", en *RDP*, nº 38 (1993)

LOWE, D., "The European Union's Passenger Name Record Data Directive 2016/681: Is It Fit for Purpose", en *International Crime Law Review*, Vol. 16, nº 5 (2016), pp. 856-884

LUCAS MURILLO DE LA CUEVA, P., "El derecho a la autodeterminación informativa y la protección de datos personales", en *Azpilcueta Cuadernos de Derecho*, nº 20 (2008), pp. 43-58

LUCAS MURILLO DE LA CUEVA, P., "La Constitución y el derecho a la autodeterminación informativa", en *Cuadernos de Derecho Público*, nº 19-20 (2003), pp. 27-32

LUCAS MURILLO DE LA CUEVA, P., "La Constitución y el derecho a la autodeterminación informativa", en *Cuadernos de Derecho Público*, nº 19-20 (2003), pp. 27-44

LUCAS MURILLO DE LA CUEVA, P., "La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad", en *El derecho a la autodeterminación informativa*, Madrid: Ed. Fundación Coloquio Jurídico Europeo, 2009, pp. 11-80

LUCAS MURILLO DE LA CUEVA, P., "La construcción del derecho a la autodeterminación informativa", en *Revista de estudios políticos*, nº 104 (1999), pp. 35-60

LUCAS MURILLO DE LA CUEVA, P., "Las vicisitudes del Derecho de la protección de datos personales", en *Revista Vasca de Administración Pública*, nº 58-II (2000), pp. 211-219

LUCAS MURILLO DE LA CUEVA, P., "Perspectivas del derecho a la autodeterminación informativa", en *Revista de Internet, Derecho y Política*, nº 5 (2007)

LUQUE GONZÁLEZ, J. M., "Schengen Un espacio de libertad, seguridad y justicia", en *Revista de derecho*, Ed. División de Ciencias Jurídicas de la Universidad del Norte, nº 21 (2004), pp. 139-149

MAESTRO BUELGA, G., "Los derechos sociales en la Unión Europea: una perspectiva constitucional", en *Revista Vasca de Administración Pública*, nº 46 (1996)

MARGULIES, P., "Evolving Relevance: The Metadata Program and the Delicate Balance of Secrecy, Deliberation, and National Security", en *Legal Studies Research Paper Series*, nº 146 (2014), Roger Williams Univ. Sch. of Law

MARGULIES, P., "The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism International Counterterrorism", en *Fordham Law Review*, Vol. 82, nº 5 (2014), pp. 2140-2141

MARROIG POL, L., "La Agencia de Protección de Datos. Reflexiones sobre la Administración de Datos de Carácter Personal", en *X Años de Encuentros sobre Informática y Derecho*, nº 1996-1997 (1997), Ed. Aranzadi, pp. 173-178

MARTÍN PALLÍN, J. A., "La Ley Orgánica de Regulación del tratamiento automatizado de datos de carácter personal. Una visión crítica", en *Informática Judicial y Protección de Datos Personales*, Vitoria: Ed. Gobierno Vasco, 1994, pp. 80-86

MARTÍNEZ MARTÍNEZ, R., "El derecho fundamental a la protección de datos: perspectivas", en *Revista de Internet, Derecho y Política*, nº 5 (2007), pp. 48-50

MATÍA PORTILLA, F. J., "Los derechos fundamentales de la Unión Europea en tránsito: de Niza a Lisboa, pasando por Bruselas", en *Revista Española de Derecho Europeo*, nº 39 (2011), Westlaw-Aranzadi, pp. 1-17

MEDINA GUERRERO, M., "Escritos sobre derechos fundamentales", en *Revista Española de Derecho Constitucional*, nº 41 (1994), pp. 323-324

MILANOVIC, M., "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age", en *Harvard International Law Journal*, nº 56 (2015), p. 86

NAVARRO RUIZ, J. C., "Algunas consideraciones sobre la tramitación de la LORTAD", en *Cuadernos de la Cátedra de Fadrique Furió Ceriol*, nº 1 (1992), pp. 98-107

NIEVES SALDAÑA, M., "«The right to privacy». La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis", en *Revista de Derecho Político,* Universidad Nacional de Educación a Distancia (UNED), nº 85 (2012), Madrid, pp. 209-210

NIEVES SALDAÑA, M., "El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego", en *Teoría y Realidad Constitucional,* Universidad Nacional de Educación a Distancia (UNED), nº 28 (2011), Madrid, p. 306

NOREÑA SALTO, J. R., "Acerca del contenido esencial de los derechos fundamentales de configuración legal", en *Repertorio Aranzadi del Tribunal Constitucional,* nº 18 (2004), p. 10

O'CONNOR, T. (1968). "The Right to Privacy in Historical Perspective", *Massachusetts Law Review*, nº 53, pp. 101-110

ORTEGA JIMÉNEZ, A., "La transferencia internacional de datos de carácter personal y el Derecho internacional privado", en *Diario La Ley*, nº 6237 (2005), pp. 1-5

ORTI VALLEJO, A., "El nuevo derecho fundamental (y de la personalidad) a la libertad informática (a propósito de la STC 254/1994, de 20 de julio)", en *Derecho privado y Constitución,* nº 2 (1994), p. 305

PACE, A., "¿Para qué sirve la Carta de Derechos Fundamentales de la Unión Europea?", en *Teoría y Realidad Constitucional,* nº 7 (2001), p. 174

PARDO FALCÓN, J., "Los derechos del art. 18 de la Constitución española en la jurisprudencia del Tribunal Constitucional", en *Revista Española de Derecho Constitucional,* nº 34 (1992), pp. 141-178

PAREJO NAVAJAS, T., "La Carta de los derechos fundamentales de la Unión Europea", en *Derechos y Libertades: Revista de filosofía del derecho y derechos humanos* (2010), pp. 205-239

PATEL, F. y KOREH, R., "Enhancing Civil Liberties Protections in Surveillance Law", en *New York University – Annual Survey of American Law*, Nueva York, 2020. Consultado el 20.08.2020 desde: https://www.brennancenter.org/our-work/analysis-opinion/enhancing-civil-liberties-protections-surveillan ce-law

PAVÓN PÉREZ, J. A., "La protección de datos personales en el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales", en *Anuario de la Facultad de Derecho (Universidad de Extremadura)*, nº 19-20 (2002), pp. 235-252

PENG, S., "Privacy and the Construction of Legal Meaning in Taiwan", en *International Lawyer*, nº 37, p. 1037, 2003. Consultado el 01.06.2020 desde: https://ssrn.com/abstract=957800

PÉREZ CAMBERO, R., "Aspectos más destacables de la Decisión de Ejecución 2016/1250 de la Comisión Europea, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU.", en *Actualidad Administrativa*, nº 4 (2017), Wolters Kluwer, p. 19

PÉREZ DE NANCLARES, J. M. y URREA CORRES, M., "Tratado de Lisboa" (Recensión), en *Revista De Las Cortes Generales*, nº 70-72 (2007), pp. 1249-1252

PÉREZ LUÑO, A. E., "Comentario legislativo: La LORTAD y los derechos fundamentales", en *Derechos y Libertades*, nº 1 (1993), p. 409

PÉREZ LUÑO, A. E., "Del habeas corpus al habeas data", en *Informática y derecho: Revista iberoamericana de derecho informático*, nº 1 (1992), p. 162

PÉREZ LUÑO, A. E., "Informática jurídica y derecho de la informática en España", en *Informatica e Diritto*, nº 2 (1983), pp. 93-95

PÉREZ LUÑO, A. E., "Informática y Libertad. Comentario al artículo 18.4 de la Constitución española", en *Revista de Estudios Políticos (Nueva Época)*, nº 24 (1981), pp. 33-41

PÉREZ LUÑO, A. E., "La juscibernética en España", en *Revista jurídica de Catalunya*, nº 2 (1972), pp. 303-310

PÉREZ LUÑO, A. E., "La nueva normativa europea para la protección de los datos personales", en *Derechos y libertades,* nº 40 (2019), p. 233

PÉREZ LUÑO, A. E., "La protección de la intimidad frente a la informática en la Constitución española de 1978", en *Revista de Estudios Políticos (Nueva Época),* nº 9 (1979), pp. 73-79

PÉREZ LUÑO, A. E., "La protección de los datos personales del menor en Internet", en *Anuario de la Facultad de Derecho (Universidad de Alcalá),* nº 2 (2009), pp. 143-175

PIERCE, G y PLATTEN, N., "Achieving Personal Data Protection in the European Union", en *Journal of Common Market Studies,* Vol. 36, nº 4 (1998), pp. 529-547

PLESSER, R. L. y CIVIDANES, E. W., "EC Personal Data Privacy: US Concerns", en *Transnational Data and Communications Report,* Vol. XIII, nº 9 (1990), p. 19

POST, R. C., "Three Concepts of Privacy", en *Georgetown Law Journal,* nº 89 (2001), pp. 2087-2098

POULLET, Y., "Flujos de datos transfronterizos y extraterritorialidad: la postura europea", en *Revista Española de Protección de Datos,* nº 1 (2006), pp. 99-105

PRIETO GUTIÉRREZ, J. M., "La Directiva 95/46/CE como criterio unificador", en *Revista del Poder Judicial,* nº 48 (1998), pp. 165-243

PRIETO GUTIÉRREZ, J. M., "Objeto y naturaleza jurídica del derecho fundamental a la protección de datos personales", en *Estudios del Ministerio de Justicia,* Boletín nº 1971-1972 (2003), p. 25

PROSSER, W., "Privacy", en *California Law Review,* nº 48 (1960)

PULIDO QUECEDO, M., "La catequista y los riesgos de Internet", en *Actualidad Jurídica Aranzadi,* nº 602 (2003), Cizur Menor (Navarra): Ed. Aranzadi, pp. 14-15

RALLO LOMBARTE, A., "El terrorismo internacional y sus conflictos: Seguridad vs. Privacidad", en *Inteligencia y seguridad. Revista de análisis y prospectiva,* nº 3 (2007), pp. 113-131

RALLO LOMBARTE, A., "El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en Internet", en *Teoría y Realidad Constitucional,* nº 39 (2017), Ed. Universidad Nacional de Educación a Distancia (UNED), p. 585

RECIO GAYO, M. y ÁLVAREZ CARO, M., "Hacia un acuerdo Safe Harbor renovado para la transferencia internacional de datos entre EE. UU. y la UE", nº 25 (2015), en *Instituto de Derecho Europeo e Integración Regional (IDEIR)*, Madrid: Ed. Universidad Complutense, 2015, p. 7

RECIO GAYO, M., "Nivel adecuado para transferencias internacionales de datos", en *Revista de la Facultad de Derecho de la Pontificia Universidad Católica del Perú*, nº 83 (2019), p. 5. Consultado el 28.06.2020 desde: https://doi.org/10.18800

REINARES, F., "¿Cuál es la amenaza que el terrorismo yihadista supone actualmente para España?", en *Boletín Elcano,* nº 90 (2007), pp. 3-7.

REINARES, F., "¿Cuál es la amenaza que el terrorismo yihadista supone actualmente para España?", en *Boletín Elcano,* 2007 (90), 7 páginas. Consultado el 10. 12. 2017 en: http://biblioteca.ribei.org/1151/1/ARI-33-2007-E.pdf

REQUEJO ISIDRO, M., "La aplicación privada del derecho para la protección de las personas físicas en materia de tratamiento de datos personales en el Reglamento (UE) 2016/679", en *Revista La Ley Mercantil,* nº 42 (2017), pp. 1-25

RICHARDS, N. M., "The Dangers of Surveillance", en *Harvard Law Review*, Vol. 126, No. 7 (2013), pp. 1934-1935

RIGAUX, F., "Le régime des données informatisées en droit international privé", en *Journal du droit international,* Vol. 113 (1986), pp. 311-328

RILEY, T., "Data Protection Clash on EC Directives", en *Transnational Data and Communications Report,* Vol. XIII, n º 9 (1990), pp. 5-11

RIPOLL CARULLA, S., "El Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal: Balance a los siete años de su apertura a la firma", en *Actas del Congreso sobre Derecho Informático,* Zaragoza: Ed. Facultad de Derecho, 1989, pp. 395-413

RIPOLL CARULLA, S., "El Movimiento Internacional de Datos en la Ley Española de Protección de Datos", en *Informática y Derecho. Revista Iberoamericana de Derecho Informático*, nº 6-7 (1994), Mérida: Ed. Universidad Nacional de Educación a Distancia, Centro Regional de Extremadura, pp. 313-322

RODRÍGUEZ BEREIJO, A., "La Carta de Derechos Fundamentales", en *Revista de Derecho de la Unión Europea*, nº 1 (2002), pp. 45-57

RODRÍGUEZ-IZQUIERDO SERRANO, M., "El Tribunal de Justicia y los derechos en la sociedad de la información: Privacidad y protección de Datos frente a libertades informativas", en *Revista de Derecho Constitucional Europeo*, nº 24 (2015)

ROVIRA FERRER, I., "La Administración electrónica tributaria: implantación y respuesta ciudadana", en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 17 (2008), Westlaw-Aranzadi, pp. 1-3

RUBENFELD, J., "The Right of Privacy", en *Harvard Law Review*, nº 102 (1989), pp. 737-807

RUBIO LLORENTE, F., "Mostrar los derechos sin destruir la Unión", en *Revista Española de Derecho Constitucional*, nº 64 (2002), pp. 13-22

RUGER, T. W., "Chief Justice Rehnquist's Appointments to the FISA Court: An Empirical Perspective", en *Northwestern University Law Review*, Vol. 101, nº 1 (2007), pp. 239-244

RUIZ MIGUEL, C., "El derecho a la intimidad informática en el ordenamiento español", *Revista general de Derecho*, nº 607 (1995), pp. 3207-3233

RUIZ MIGUEL, C., "El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico", en *Revista de Derecho Comunitario Europeo*, nº 14 (2003), pp. 7-43

RUÍZ MIGUEL, C., "El largo y tortuoso camino hacia la Carta de los Derechos Fundamentales de la Unión Europea", en *Revista europea de derechos fundamentales*, nº 2 (2003), pp. 61-90

S. RUBINSTEIN, I., "The End of Privacy or a New Beginning?", en *International Privacy Law*, Vol. 3, nº 2 (2013), pp. 74-87

SÁIZ ARNÁIZ, A., "La Carta de los Derechos Fundamentales de la Unión Europea y los ordenamientos nacionales: ¿qué hay de nuevo?", en *Cuadernos de Derecho Público*, nº 13 (2001), pp. 153-159

SANCHO LÓPEZ, M., "Consideraciones procesales del ejercicio del derecho al olvido: examen de jurisprudencia reciente y del nuevo marco legal", en Revista Aranzadi de Derecho y Nuevas Tecnologías, nº 41 (2016), pp. 1-17.

SCHULHOFER, S. F., "An International Right to Privacy? Be Careful What You Wish For", *Working paper nº 15-15*, Ed. New York University. School of Law, 2015, pp. 238-258

SCHWARTZ, P. M., "Internet privacy and the State", en *Connecticut Law Review*, nº 32 (2000)

SCHWARTZ, P. M., "Privacy and Democracy in Cyberspace", en *Vanderbilt Law Review*, nº 52 (1999)

SERRA CRISTÓBAL, R., "Los derechos fundamentales en la encrucijada de la lucha contra el terrorismo yihadista. Lo que el constitucionalismo y el Derecho de la Unión Europea pueden ofrecer en común", en *XIV Congreso Asociación de Constitucionalistas de España*, 2016

SEVERSON, D., "American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change", en *Harvard International Law Journal*, Vol. 56, nº 2 (2015), pp. 465-514

SHEN, F. ("Cris"), TSUI, L. "Public Opinion toward Internet Freedom in Asia: A Survey of Internet Users from 11 Jurisdictions", en *Research Publication, nº* 8 (2016), The Berkman Center for Internet and Society at Harvard University. Consultado el 01.06.2020 desde: http://ssrn.com/abstract=2773802

ŠKRINJAR, M., "Schrems v. Data Protection Commissioner (Case C-362/14): Empowering National Data Protection Authorities", en *Croatian Yearbook of European Law and Policy*, nº 11 (2015), p. 265

SOLAR CALVO, M. P., "La protección de datos en la Unión Europea: análisis y perspectivas de futuro", en *Revista Aranzadi Unión Europea*, nº 2 (2012), p. 8

SOLOVE, D. J., "Conceptualizing privacy", en *California Law Review*, nº 90 (2002), pp. 1087-1155

SOMA, J. T., RYNERSON, S. D. y BEALL-EDER, B. D., "An analysis of the Use of Bilateral Agreements Between Transnational Trading Groups: The U.S./EU E-Commerce Privacy Safe Harbor", en *Texas International Law Journal*, nº 39 (2004), pp. 194-207

SUNOSKY, J. T., "Privacy Online: A Primer on the European Union's Directive and United States' Safe Harbor Privacy Principles", en *International Trade Law Journal*, nº 9 (2000), pp. 80-82

TRONCOSO REIGADA, A., "Hacia un nuevo marco jurídico europeo de protección de datos personales", en *Revista Española de Derecho Europeo*, nº 43 (2012), pp. 42-43

TRONCOSO REIGADA, A., "La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional", en *Cuadernos de Derecho Público*, nº 19-20 (2003), pp. 231-334

TURKINGTON, R. C., "Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy", en *Northern Illinois University Law Review*, nº 10 (1990), pp. 496-503

URÍA GAVILÁN, E., "Derechos fundamentales versus vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 (Schrems I)", en *Revista de Derecho Comunitario Europeo*, nº 53 (2016), pp. 267-268

VALERO TORRIJOS, J., "De la digitalización a la innovación tecnológica: valoración jurídica del proceso de modernización de las administraciones públicas españolas en la última década (2004-2014)", en *Revista de los Estudios de Derecho y Ciencia Política*, nº 19 (2014), pp. 117-126

VICIANO PASTOR, R., "El largo camino hacia una constitución europea", en *Revista de Derecho de la Unión Europea*, nº 2 (2002), pp. 105-123

VILLAVERDE MENÉNDEZ, I., "Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo a propósito de la STC 254/1993", en *Revista Española de Derecho Constitucional*, nº 41 (1994), pp. 187-202

WARREN, S. D. y BRANDEIS, L., "The Right to Privacy", en *Harvard Law Review*, Vol. 4, nº 5 (1890), pp. 194-220

WATER, N., "The APEC Asia-Pacific Privacy Initiative: A New Route to Effective Data Protection or a Trojan Horse for Self-Regulation?", en *UNSW Law Research Paper*, nº 59 (2008), pp. 1-15. Consultado el 15.09.2020 desde: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1402445

WEBER. A., "La Carta de los Derechos Fundamentales de la Unión Europea", en *Revista Española de Derecho Constitucional*, nº 64 (2002), pp. 79-84

WHITMAN, J. Q., "The Two Western Cultures of Privacy: Dignity versus Liberty", en *Yale Law Journal*, nº 113 (2004), pp. 1151-1221

WHITMAN, J. "The Two Western Cultures of Privacy: Dignity versus Liberty", en *Yale Law Journal*, nº 113 (1) (2004), pp. 1011-1221

PUBLICACIONES ELECTRÓNICAS

ALDAMA, Z., "Privacidad y datos. El sistema de crédito social chino salta de la teoría a la práctica", en *El País*, 23 de julio de 2018. Consultado el 15.09.2020 desde: https://retina.elpais.com/retina/2018/03/27/tendencias/1522145305_569868.html

BOWDEN, C., "The US Surveillance Programmes and their Impact on EU Citizens' Fundamental Rights", Bruselas: Ed. Parlamento Europeo, 2013, pp. 12-15. Consultado el 15.08.2020 desde: https://op.europa.eu/es/publication-detail/-/publication/0a3aa9b5-1fe9-4f85-aaae-cc515408cf97

CADWALLADR C. y GRAHAM-HARRISON E., "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach", *The Guardian*. Consultado el 15.08.2020 desde: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

CADWALLADR C., “Google, Democracy and the Truth About Internet Search”, *The Guardian*. Consultado el 15.08.2020 desde: https://www.theguardian.com/technology/2016/dec/04/google-democracy-truth-internet-search-facebook

CADWALLADR, C. y GRAHAM-HARRISON, E., “Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach”, en *The Guardian,* 17 de marzo de 2018. Consultado el 22.08.2019 desde: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

CHIA, K. y CELESTE, A., “Data Privacy Enforcement Trends”. Consultado el 05.05.2020 desde: http://www.bakermckenzie.com/en/insight/publications/2017/01/data--privacy--enforcement--newsletter/

CHIANG, A., “Reviewing the Personal Data (Privacy) Ordinance through Standstill and Crisis. (Speech delivered by Mr. Allan Chiang, Privacy Commissioner for Personal Data at ONC Conference on Law Reform «Does Law Reform need Reforming in Hong Kong?» (on 17 September 2011 at Rayson Huang Theatre, The University of Hong Kong)”. Consultado el 15.09.2020 desde: https://www.pcpd.org.hk/english/files/infocentre/speech_20110917.pdf

CREEMERS, R., “Big data, meet Big Brother China invents the digital totalitarian state. The worrying implications of its social-credit Project”, en *The Economist,* 17 de septiembre de 2016. Consultado el 15.09.2020 desde: https://www.economist.com/briefing/2016/12/17/china-invents-the-digital-totalitarian-state

CREEMERS, R., “What Could China’s ‘Social Credit System’ Mean for its Citizens?”, en *Foreign Policy,* 15 de agosto de 2016. Consultado el 15.09.2020 desde: https://foreignpolicy.com/2016/08/15/what-could-chinas-social-credit-system-mean-for-its-citizens/

DAMIANA, J. “Indonesia to step up data protection with new bill amid booming digital economy”, en Reuters, 28 de enero de 2020. Consultado el 01.06.2020 desde:

https://www.reuters.com/article/us-indonesia-data/indonesia-to-step-up-data-protection-with-new-bill-amid-booming-digital-economy-idUS KBN1ZR1NL

DAVIDSON, H. "China's coronavirus health code apps raise concerns over privacy", en *The Guardian*, 1 de abril de 2020. Consultado el 05.05.2020 desde: https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy

EDITOR. "Surveillance: Look who's listening", en *The Economist*, 15 de junio de 2013. Consultado el 20.08.2020 desde: https://www.economist.com/briefing/2013/06/15/look-whos-listening

ELOKSARI, E. A. "Tokopedia data breach exposes vulnerability of personal data", en *The Jakarta Post*, 5 de mayo de 2020. Consultado el 01.06.2020 desde: https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-person al-data.html

ENISA, "The Value of Personal Online Data", 23 de abril de 2018. Consultado el 22.08.2019 desde: https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data

FACHRIANSYAH, R. y SYAKRIAH, A., "COVID-19: Indonesia develops surveillance app to bolster contact, tracing, tracking", en *The Jakarta Post*, 30 de marzo de 2020. Consultado el 01.06.2020 desde: https://www.thejakartapost.com/news/2020/03/30/covid-19-indonesia-develops-surveillance-app-to-bolster-contact-tracing-tracking.html

GOITEIN, E. y PATEL, F., "What Went Wrong with the FISA Court", Ed. Brennan Center for Justice, New York University School of Law, 2015. Consultado el 20.08.2017 desde: https://www.brennancenter.org/our-work/research-reports/what-went-wrong-fisa-court

GREENLEAF, G. y PARK, W. "Korea's New Act: Asia's Toughest Data Privacy Law", en *Privacy Laws & Business International Report*, nº 117 (2012), pp. 1-6. Consultado el 15.09.2020 desde: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2120983

GRIMM, A. N., "Trends in U.S. Trade in Information and Communications Technology (ICT) Services and in ICT-Enabled Services", Ed. Bureau of Economic Analysis, U.S. Department of Commerce, 2015

HAN, B., "Por qué a Asia le va mejor que a Europa en la pandemia: el secreto está en el civismo", en *El País,* 25 de octubre de 2020. Consultado el 29.10.2020 desde: https://elpais.com/ideas/2020-10-24/por-que-a-asia-le-va-mejor-que-a-europa-en-la-pandemia-el-secreto-esta-en-el-civismo.html?ssm=TW_CC

HAN, B., "El virus es un espejo, muestra en qué sociedad vivimos", en *El Tiempo,* 16 de mayo de 2020. Consultado el 09.07.2020 desde: https://www.eltiempo.com/mundo/asia/byung-chul-han-habla-del-efecto-del-coronavirus-en-las-personas-y-sociedades-496296

HUSTINX, P., "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", 2014, p. 3. Consultado el 12.07.2020 desde: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_ENpdf

ICO. "Investigation into the use of data analytics in political campaigns", 11 de julio de 2018. Consultado el 24.08.2019 desde: https://ico.org.uk/media/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf

ICO. "Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach", 9 de julio de 2019. Consultado el 24.08.2019 desde: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/

KANG C. y FRANKEL S., "Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users", *The New York Times*. Consultado el 15.08.2020 desde: https://www.nytimes.com /2018/04/04/technology/mark-zuckerberg-testify-congress.html

KER, D. y MAZZINI, E., Perspectives on the value of data and data flows, Paris: OECD Digital Economy Papers, No. 299, OECD Publishing, 2020. Consultado el 05.05.2021 desde: https://doi.org/10.1787/a2216bc1-en

MACASKILL, E. y DANCE, G., "NSA Files: Decoded. What the revelations mean for you", en *The Guardian*, 1 de noviembre de 2011. Consultado el 22.08.2019 desde: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

MANYIKA, J. y LUND, S., "How Digital Trade is Transforming Globalisation", California: Ed. McKinsey & Company, 2016. Consultado el 20.08.2020 desde: http://e15initiative.org/publications/how-digital-trade-is-transforming-globalisation

MANYIKA, J., CHUI, M. y VV. AA., "Big data: The next frontier for innovation, competition, and productivity", California: Ed. McKinsey & Company, 2011. Consultado el 20.08.2020 desde: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation

MAX, K. S., "South Korea is watching quarantined citizens with a smartphone app", en *MIT Technology Review*, 06/03/2020. Consultado el 01.05.2020 desde: https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/

MELTZER, J. P., "The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment", Ed. Brookings, 2014, pp. 12-17. Consultado el 20.08.2020 desde: https://www.brookings.edu/research/the-importance-of-the-internet-and-transatlantic-data-flows-for-u-s-and-eu-trade-and-investment/

MONTJOYE, A. *et. al*., "Evaluating COVID-19 contact tracing apps? Here are 8 privacy questions we think you should ask", Ed. Computational Privacy Group, 2 de abril de 2020. Consultado el 11.10.2020 desde: https://cpg.doc.ic.ac.uk/blog/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-thin k-you-should-ask/

MOON, G., "How South Korea Flattened its Coronavirus Curve", en *NBC News*, 24/3/2020. Consultado el 31.05.2020 desde: https://www.nbcnews.com/news/world/how-south-korea-flattened-its-coronavirus-curve-n1167376

MOZUR, P., ZHONG, R. y KROLIK, A., "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags", en *The New York Times,* 1 de marzo de 2020. Consultado

el 15.05.2020 desde: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

PATEL, O. y LEA, N., *EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows*, Londres: Ed. UCL European Institute, 2020, p. 11

PRIVACY INTERNATIONAL, "Universal Periodic Review Stakeholder Report: 24th Session, Singapore The Right to Privacy in Singapore". Consultado el 01.06.2020 desde: https://privacyinternational.org/sites/default/files/2017-12/Singapore_UPR_PI_submission_FINAL.pdf

SHABAN, H. "FedEx delivery unit hit by worldwide cyberattack", en *The Washington Post*, 28 de junio de 2017. Consultado el 22.08.2019 desde: https://www.washingtonpost.com/news/the-switch/wp/2017/06/28/fedex-delivery-unit-hit-by-worldwide-cyberattack/?noredirect=on

THE WHITE HOUSE, "Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies Recommendation", Recommendation 12, 2013, pp. 145-46

UBER. "Información sobre el incidente de seguridad de datos de 2016". Consultado el 22.08.2019 desde: https://help.uber.com/riders/article/informaci%C3%B3n-sobre-el-incidente-de-seguridad-de-datos-de-2016?nodeId=12c1e9d1-4042-4231-a3ec-3605779b8815

REFERENCIAS NORMATIVAS

Internacionales

China. “Cybersecurity Law of the People’s Republic of China, November 6, 2016”. Acceda la versión no oficial en inglés. Consultado el 05.05.2020 desde: https://www.chinafile.com/ngo/laws-regulations/cybersecurity-law-of-peoples-republic-of-china

Convenio de La Haya, de 18 de marzo de 1970, sobre la obtención de pruebas en el extranjero en materia civil o mercantil.

Convenio de La Haya, de 25 de octubre de 1980, tendente a facilitar el acceso internacional a la justicia.

Corea del Sur. Constitución de la República de Corea del Sur de 1987. Consultado el 01.06.2020 desde: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=1&lang=ENG

Declaración Universal de los Derechos Humanos. Artículo 12 de la Declaración Universal de los Derechos Humanos: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”.

Declaración Universal de los Derechos Humanos. Resolución 217 A (III), de 10 de diciembre de 1948. Consultado el 28.06.2020 desde: https://www.unorg/es/universal-declaration-human-rights/

Estados Unidos. *50 U.S. Code, §1881a, Foreign Intelligence Surveillance Act.*

Estados Unidos. *50 U.S. Code, Chapter 36, Foreign Intelligence Surveillance Act*.

Estados Unidos. *Aviation and Transportation Security Act (ATSA), 19 November 2001 (Public Law 107-71, 107th Congress, 49 USC Section 44909(c) (3) (2001)).*

Estados Unidos. *Cable Communication Policy Act (CCPA)* de 1984.

Estados Unidos. *California Consumer Privacy Act (CCPA)* de 2018.

Estados Unidos. *Children’s On-line Privacy Protection Act (COPPA)* de 1998.

Estados Unidos. *Clarifying Overseas Use of Data Act* de 2018.

Estados Unidos. *Data Privacy Act* de 1974.

Estados Unidos. *Data Privacy Act* de 1976.

Estados Unidos. *Driver's Privacy Protection Act (DPPA)* de 1994.

Estados Unidos. *E-Government Act* de 2002.

Estados Unidos. *Electronic Communications Privacy Act (ECPA)* de 1975.

Estados Unidos. *Electronic Communications Privacy Act (ECPA)* de 1986.

Estados Unidos. *Executive Order 12333* de 1981.

Estados Unidos. *Executive Order 13284* de 2003.

Estados Unidos. *Executive Order 13470* de 2008.

Estados Unidos. *Executive Order 13555* de 2004.

Estados Unidos. *Fair and Accurate Credit Transactions Act (FACTA)* de 2003.

Estados Unidos. *Financial Services Modernization Act* de 1999.

Estados Unidos. *Freedom of Information Act (FOIA)*, 5 U.S.C. § 552. Promulgada el 4 de julio de 1966 por parte del Congreso de los Estados Unidos de América. Consultado el 28.06.2020 desde: https://www.govtrack.us/congress/bills/89/s1160

Estados Unidos. *Genetic Information Nondiscrimination Act (GINA)* de 2008.

Estados Unidos. *Gramm-Leach-Bliley Act (GLBA)* de 1999.

Estados Unidos. *Health Insurance Portability and Accountability Act (HIPAA)* de 1996.

Estados Unidos. *Presidential Policy Directive 28* de 2014.

Estados Unidos. *Privacy Act*, 5 U.S.C. § 552 a), *Section* 2. Promulgada del 31 de diciembre de 1974 por parte del Congreso de los Estados Unidos de América. Consultado el 28.06.2020 desde: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1279

Estados Unidos. *Right to Financial Privacy Act (RFPA)* de 1978.

Estados Unidos. *Telecomunications Act* de 1996.

Estados Unidos. *US passed legislation concerning border security (Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSV), 5 May 2002)*

Hong Kong. *Ordinance to protect the privacy of individuals in relation to personal data, and to provide for matters incidental thereto or connected therewith*, de 6 de agosto de 1996 (L.N. 343 of 1996)

Hong Kong. *The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China*. Consultado el 05.05.2020 desde: https://www.basiclaw.gov.hk/en/basiclawtext/images/ basiclaw_full_text_en.pdf

Indonesia. Constitución de la República de Indonesia de 1945. Consultado el 01.06.2020 desde: http://www.humanrights.asia/countries/indonesia/laws/uud1945

Indonesia. Reglamento del Gobierno nº 71 de 2019 relativo a la implementación de Sistema Electrónico de Transacciones.

Indonesia. Reglamento nº 20 de 2016, relativo a la protección de los datos personales en los Sistemas Electrónicos de Transacciones. Consultado el 01.06.2020 desde: https://ppidkemkominfo.files.wordpress.com/2016/12/pm-kominfo-no-20-tahun-2016.pdf

Indonseia. Ley nº 19 de 2016, que modifica la Ley de Información Electrónica. Consultado el 01.06.2020 desde: https://peraturan.bpk.go.id/Home/Details/37582/uu-no-19-tahun-2016

Japón. Constitución del Imperio de Japón, 3 de noviembre de 1946.

Pacto Internacional de los Derechos Civiles y Políticos, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 19 de diciembre de 1966, fue ratificado por España en fecha 28 de septiembre de 1976 y publicado en el Boletín Oficial del Estado en fecha 30 de abril de 1977. Consultado el 28.06.2020 desde: https://www.boe.es/buscar/doc.php?id=BOE-A-1977-10733

Singapur. *Personal Data Protection Act,* de 15 de octubre de 2012.

Comunitarias

CEPD, "Escudo de la privacidad UE-EE. UU. – Tercera revisión conjunta anual", adoptado el 12 de noviembre de 2019, pp. 10-16. Consultado el 11.07.2020 desde:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpbprivacyshield3rdannualreport.pdf _en.pdf

CEPD. "Opinión conjunta emitida por el CEDP y el SEPD sobre la Decisión de Ejecución en relación con las CCT". Consultado el 21 de enero de 2021 desde: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22021-standard_es

CEPD. "Directrices 03/2020 sobre el procesamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19". Consultado el 14 de junio de 2020 desde: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_ en

CEPD. "Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto del brote de COVID-19". Consultado el 14 de julio de 2020 desde: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_es.pdf

CEPD. "Directrices 2/2018 sobre las excepciones al artículo 49 del Reglamento 2016/679", adoptadas el 25 de mayo de 2018. Consultado el 11.07.2020 desde: https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22018-derogations-arti cle-49-under-regulation_en

CEPD. "Directrices 2/2019 sobre el tratamiento de datos personales en virtud del artículo 6(1)(b) RGPD en el marco de la prestación de servicios en línea a interesados", versión 2.0, aprobada el 8 de octubre de 2019, pp. 8-12. Consultado el 11.07.2020 desde: https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22019-processing-personal-data-under-article-61b_es

CEPD. "Escudo de la privacidad UE-EE. UU. – Segunda revisión conjunta anual", adoptado el 22 de enero de 2019, pp. 9-14. Consultado el 11.07.2020 desde: https://edpb.europa.eu/sites/edpb/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf

CEPD. "Guidelines of the European Data Protection Board 04/2020 on the Use of Location Data and Contact Tracing contact tracing tools in the Context of the COVID-19 Outbreak", sec. 2.2. (21 de abril de 2020). Consultado el 5 de mayo de 2020 desde:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_ with_annex_en.pdf

CEPD. "Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE, adoptadas el 10 de noviembre de 2020", p. 2. Consultado el 21.01.2021 desde: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_ supplementarymeasurestransferstools_es.pdf

CEPD. Declaración efectuada como consecuencia de la STJUE en el asunto C-311/18 (Schrems II), en fecha 17 de julio de 2020. Consultado el 15.08.2020 desde: https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en

Comisión Europea. "Comunicación al Parlamento Europeo y al Consejo, Restablecer la confianza en los flujos de datos entre la UE y EE. UU.", de fecha 27 de noviembre de 2013 (COM [2013] 846 final), p. 3. Consultado el 20.08.2017 desde: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2013%3A0846%3AFIN

Comisión Europea. "Comunicación al Parlamento Europeo y al Consejo, sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la Unión Europea y las empresas establecidas en la misma", de fecha 27 de noviembre de 2013 (COM [2013] 847 final). Consultado el 20.08.2017 desde: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com (2013)0847_es.pdf

Comisión Europea. "Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre la transferencia de datos personales de la UE a los Estados Unidos de América con arreglo a la Directiva 95/46/CE de forma consiguiente a la sentencia del Tribunal de Justicia en el asunto C-362/14 (Schrems I)", de fecha 6 de noviembre de 2015 (COM [2015] 566 final). Consultado el 24.08.2017 desde: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML /?uri=CELEX:52015DC0566&from=EN

Comisión Europea. "Documento de trabajo del personal de la Comisión que acompaña al Informe al Parlamento Europeo y al Consejo sobre la segunda revisión anual del funcionamiento del Escudo de la privacidad UE - EE. UU. (COM [2018] 860 final)", de fecha 19 de diciembre de 2018, pp. 26-28.Consultado el 15.08.2020 desde:

https://ec.europa.eu/info/sites/info/files/staff_working_document_-_second_annual_review.pdf

Comisión Europea. "Documento de trabajo del personal de la Comisión que acompaña al Informe al Parlamento Europeo y al Consejo sobre la segunda revisión anual del funcionamiento del Escudo de la privacidad UE - EE. UU. (COM [2019] 495 final)", de fecha 23 de octubre de 2019, pp. 20-22. Consultado el 15.08.2020 desde: https://ec.europa.eu/info/sites/info/files/staff_working_document_-_third_annual_review.pdf

Comisión Europea. "Hacia una economía de los datos próspera", Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones (COM/2014/0442 final), de fecha 2 de julio de 2014. Consultado el 20.08.2017 desde: https://ec.europa.eu/digital-single-market/en/news/communication-data-driven-economy

Comisión Europea. "Informe al Parlamento Europeo y al Consejo sobre la segunda revisión anual del funcionamiento del Escudo de la privacidad UE - EE. UU. (SWD [2018] 497 final)", de fecha 19 de diciembre de 2018, pp. 3-4. Consultado el 15.08.2020 desde: https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_priva cy_shield_ 2018.pdf

Comisión Europea. "Informe al Parlamento Europeo y al Consejo sobre la tercera revisión anual del funcionamiento del Escudo de la privacidad UE - EE. UU. (SWD [2019] 390 final)", de fecha 23 de octubre de 2019, pp. 2-3. Consultado el 15.08.2020 desde:https://ec.europa.eu/info/sites/info/files/report_on_the_third_annual_review_of _the _eu_us_privacy_shield_2019.pdf

Comisión Europea. "Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46 CE)" (COM/2003/0265 final), 2003. Consultado el 11.07.2020 desde: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52003DC0265

Comisión Europea. Decisión (UE) 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes,

publicadas por el Departamento de Comercio de Estados Unidos de América (notificada con el número C [2000] 2441). Consultado el 20.08.2017 desde: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri= CELEX:32000D0520

Comisión Europea. Decisión (UE) 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE.

Comisión Europea. Decisión (UE) 2004/915/CE de la Comisión, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países.

Comisión Europea. Decisión (UE) 2010/87/CE 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/CE del Parlamento Europeo y del Consejo.

Comisión Europea. Proyecto de Decisión de Ejecución, de conformidad con el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, sobre la protección adecuada de los datos personales por parte del Reino Unido. Consultado el 21 de junio de 2021 desde: https://ec.europa.eu/info/sites/ default/files/draft_decision_on_the_ adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_ protection_regulation_19_feb_2020.pdf

Comisión Europea. Proyecto de Decisión de Ejecución, de conformidad con el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, sobre la protección adecuada de los datos personales por parte de la República de Corea en virtud del Ley de Protección de la Información Personal. Consultado el 20.06.2021 desde: https://ec.europa.eu/info/sites/default/files/draft_decision_on_the_adequate_level_of_ protection_of _the_republic_of_korea_with_annexes.pdf

Comisión Europea. Decisión de Ejecución (UE) 2000/518/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa al nivel de protección adecuado de los datos personales en Suiza.

Comisión Europea. Decisión de Ejecución (UE) 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos.

Comisión Europea. Decisión de Ejecución (UE) 2003/490/CE de la Comisión, de 30 de junio de 2003, con con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina.

Comisión Europea. Decisión de Ejecución (UE) 2003/821/CE de la Comisión, de 21 de noviembre de 2003, relativa al carácter adecuado de la protección de los datos personales en Guernsey.

Comisión Europea. Decisión de Ejecución (UE) 2004/411/CE de la Comisión, de 28 de abril de 2004, relativa al carácter adecuado de la protección de los datos personales en la Isla de Man.

Comisión Europea. Decisión de Ejecución (UE) 2008/393/CE de la Comisión, de 8 de mayo 2008, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales en Jersey.

Comisión Europea. Decisión de Ejecución (UE) 2010/146/UE de la Comisión, de 5 de marzo de 2010, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada dada en la Ley de las Islas Feroe sobre el tratamiento de datos personales.

Comisión Europea. Decisión de Ejecución (UE) 2010/625/UE de la Comisión, de 19 de octubre de 2010, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la adecuada protección de los datos personales en Andorra.

Comisión Europea. Decisión de Ejecución (UE) 2011/61/UE de la Comisión, de 31 de enero de 2011, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por el Estado de Israel en lo que respecta al tratamiento automatizado de los datos personales.

Comisión Europea. Decisión de Ejecución (UE) 2012/484/UE de la Comisión, de 21 de agosto de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República

Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales.

Comisión Europea. Decisión de Ejecución (UE) 2013/65/UE de la Comisión, de 19 de diciembre de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por Nueva Zelanda.

Comisión Europea. Decisión de Ejecución (UE) 2016/1250, de la Comisión, de fecha, 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. [notificada con el número C-(2016) 4176]. Consultado el 28.08.2019 desde: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/uri=CELEX:32016D1250 &from=EN

Comisión Europea. Decisión de Ejecución (UE) 2019/419 de la Comisión, de 23 de enero de 2019, con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales por parte de Japón en virtud de la Ley sobre la protección de la información personal. (DOUE, L 76/1, de 19 de marzo de 2019, pp. 1-58. Consultado en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019D0419&from=ES

Comisión Europea. Decisión de Ejecución (UE) 2019/419/UE de la Comisión, de 23 de enero de 2019, con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales por parte de Japón en virtud de la Ley sobre la protección de la información personal.

Comisión Europea. Decisión de Ejecución (UE) 2021/914 de la Comisión, de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. Consultado el 20 de junio de 2021 desde: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32021D0914

Comisión Europea. Declaración efectuada como consecuencia de la STJUE en el asunto C-311/18 (Schrems II), en fecha 16 de julio de 2020. Consultado el 15.08.2020 desde: https://ec.europa.eu/commission/presscorner/detail/en/statement_20_1366

Comisión Europea. GT29. "Transferencias de datos personales a terceros países: Aplicación de los artículos 25 y 26 de la directiva de protección de datos de la UE". Consultado el 19.07.2018

Comisión Europea. GT29. "Dictamen 4/1999 relativo a la inclusión del derecho fundamental a la protección de datos personales en el catálogo europeo de derechos fundamentales". Consultado el 19.07.2020

Comisión Europea. GT29. "Documento de Trabajo (nº 107): Procedimiento de Cooperación para el Establecimiento de una Opinión Común sobre la Adecuación de las Medidas Adoptadas en las Binding Corporate Rules", aprobadas por el Grupo de Trabajo el 14 de abril de 2005.

Comisión Europea. GT29. "Documento de Trabajo (nº 114): relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995", aprobado por el Grupo de Trabajo, el 25 de noviembre de 2005.

Comisión Europea. GT29. "Documento de Trabajo (nº 12): Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE", aprobado por el Grupo de Trabajo el 24 de julio de 1998, p. 5.

Comisión Europea. GT29. "Documento de Trabajo (nº 15): Dictamen 1/99, relativo al nivel de protección de datos en Estados Unidos y a los debates en curso entre la Comisión Europea y el Gobierno de Estados Unidos", aprobado por el Grupo de Trabajo, el 26 de enero de 1999, p. 2.

Comisión Europea. GT29. "Documento de Trabajo (nº 176): Preguntas frecuentes para abordar algunas cuestiones planteadas por la entrada en vigor de la Decisión 2010/87/UE de la Comisión de la UE, 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/CE", aprobadas por el Grupo de Trabajo el 12 de julio de 2010.

Comisión Europea. GT29. "Documento de Trabajo (nº 19): Dictamen 2/99, relativo a la idoneidad de los «Principios internacionales de puerto de seguro» que hizo públicos

el Departamento estadounidense de Comercio el 19 de abril de 1999", aprobado por el Grupo de Trabajo, el 3 de mayo de 1999, p. 5.

Comisión Europea. GT29. "Documento de Trabajo (nº 195): Dictamen 05/2012 sobre la computación en nube", aprobado por el Grupo de Trabajo el 1 de julio de 2012, p. 20

Comisión Europea. GT29. "Documento de Trabajo (nº 215): Dictamen 04/2014 del Grupo de Trabajo del Artículo 29, sobre la vigilancia de las comunicaciones a efectos de inteligencia y seguridad nacional", aprobado por el Grupo de Trabajo, el 10 de abril de 2014, pp. 4-5.

Comisión Europea. GT29. "Documento de Trabajo (nº 238): Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision", aprobado por el Grupo de Trabajo el 13 de abril de 2016, pp. 7-8. Consultado el 24.08.2017 desde: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

Comisión Europea. GT29. "Documento de Trabajo (nº 254): Referencias sobre adecuación", aprobadas por el Grupo de Trabajo, el 28 de noviembre de 2017, revisadas por última vez y adoptadas el 6 de febrero de 2018, p. 3.

Comisión Europea. GT29. "Documento de Trabajo (nº 255): EU – U.S. Privacy Shield – First annual Joint Review", aprobado por el Grupo de Trabajo, el 28 de noviembre de 2017, pp. 7-12. Consultado el 15.08.2020 desde: https://ec.europa.eu/newsroom/ just/ document.cfm?doc_id=48782

Comisión Europea. GT29. "Documento de Trabajo (nº 258): Dictamen sobre algunas cuestiones fundamentales de la Directiva sobre protección de datos en el ámbito penal (UE 2016/680)", aprobado por el Grupo de Trabajo, el 29 de noviembre de 2017, p. 10.

Comisión Europea. GT29. "Documento de Trabajo (nº 259): Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679", aprobadas por el Grupo de Trabajo, el 28 de noviembre de 2017, revisadas por última vez y adoptadas el 10 de abril de 2018, p. 20.

Comisión Europea. GT29. "Documento de Trabajo (nº 27): Dictamen 7/99, relativo al nivel de protección de datos previsto por los principios de «puerto seguro» hechos

públicos, junto con las preguntas más frecuentes y otros documentos relacionados, el 15 y 16 de noviembre de 1999 por el Departamento de Comercio de los EE. UU.", aprobado por el Grupo de Trabajo, el 3 de diciembre de 1999, pp. 7-8.

Comisión Europea. GT29. "Documento de Trabajo (nº 4): Primeras orientaciones sobre la transferencia de datos personales a terceros países. Posibles formas de evaluar la adecuación", aprobado por el Grupo de trabajo el 26 de junio de 1997.

Comisión Europea. GT29. "Documento de Trabajo (nº 7): "Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos en un tercer país?", aprobado por el Grupo de trabajo el 14 de enero de 1998.

Comisión Europea. GT29. "Documento de Trabajo (nº 9): Conclusiones preliminares sobre la utilización de disposiciones contractuales en caso de transferencia de datos personales a terceros países", aprobado por el Grupo de trabajo el 22 de abril de 1998.

Comisión Europea. GT29. "Documento de Trabajo (nº 90): Dictamen 5/2004 sobre comunicaciones no solicitadas con fines de venta directa con arreglo al artículo 13 de la Directiva 2002/58/CE", aprobado por el Grupo de Trabajo, el 27 de febrero de 2004, p. 5.

Comisión Europea. GT29. "Primera orientación sobre transferencias de datos personales a Terceros países: posibles formas de avanzar en la evaluación de la adecuación". Consultado el 19.07.2018.

Comisión Europea. GT29. Declaración relativa a las implicaciones de la Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 6 de octubre de 2015, en el asunto C- 362/14, efectuada en fecha, 16 de octubre de 2015. Consultado el 24.08.2017 desde: http://ec.europa.eu/justice/data-protection/article-29/press-material/pressrelease/
art29press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

Comisión Europea. GT29. Declaración sobre sobre la decisión de la Comisión Europea sobre Escudo de privacidad UE-EE. UU, efectuada en fecha 26 de julio de 2016. Consultado el 24.08.2017 desde: http://ec.europa.eu/justice/article-29/press-

material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf

Consejo de Europa. Artículo 14, apartado primero, del Protocolo de enmienda del Convenio (108) del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, en su versión inicial elaborada en Estrasburgo, el 10 de octubre de 2018.

Consejo de Europa. Artículo 14, apartado tercero, del Protocolo de enmienda del Convenio (108) del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, en su versión inicial elaborada en Estrasburgo, el 10 de octubre de 2018.

Consejo de Europa. Comité de Ministros del Consejo de Europa, reunión nº 224 de los Delegados de los Ministros. Consultado el 28.06.2020 desde: https://rm.coe.int/1680502830

Consejo de Europa. Comité de Ministros del Consejo de Europa, reunión nº 236 de los Delegados de los Ministros. Consultado el 28.06.2020 desde: https://rm.coe.int/16804d1c51.

Consejo de Europa. Comunicado conjunto emitido por parte de Alessandra Pierucci, Presidenta del Comité de la Convención 108 y Jean-Philippe Walter, Comisionado de Protección de Datos del Consejo de Europa respecto de derecho a la protección de datos en el contexto de la pandemia del COVID-19, de fecha 30 de mayo de 2020. Consultado el 15.05.2020 desde: https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter

Consejo de Europa. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981.

Consejo de Europa. Decisión del Consejo relativa a la apertura de negociaciones con vistas a la adhesión de las Comunidades Europeas al Convenio (108) del Consejo de Europa sobre la protección de las personas con respecto al tratamiento automatizado de los datos personales (COM [90] 314, de 24 de septiembre de 1990, DOCE, serie C, nº 277, de 5 de noviembre de 1990).

Consejo de Europa. Propuesta de Decisión del Consejo por la que se autoriza a los Estados miembros a ratificar, en interés de la Unión Europea, el Protocolo que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STCE nº 108) (COM [2018] 451 final). Consultado el 02.04.2021 desde: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018PC0451&from=PL

Consejo de Europa. Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las Autoridades de control y a los flujos transfronterizos de datos, hecho en Estrasburgo el 8 de noviembre de 2001 y ratificado posteriormente el 8 de noviembre de 2001.

Consejo de Europa. Protocolo de enmienda aprobado por el Comité de Ministros del Consejo de Europa, el 18 de mayo de 2018, durante la correspondiente reunión de los Delegados de los Ministros. Consultado el 28.06.2020 desde: https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8

Consejo de Europa. Ratificación del Protocolo de Enmienda, 28 de enero de 2021. Consultado el 02.04.2021 desde: http://www.exteriores.gob.es/RepresentacionesPermanentes/ConsejodeEuropa/es/Noticias/Paginas/Articulos/20210203_NOT1.aspx

Consejo de Europa. Recomendación nº (83) 10, de 23 de septiembre de 1983, relativa a la protección de datos personales utilizados con fines de investigación y estadísticos.

Consejo de Europa. Recomendación nº (89) 2, de 18 de enero de 1989, relativa a la protección de datos personales utilizados con fines laborales.

Consejo de Europa. Recomendación nº (95) 4, de 7 de febrero de 1995, relativa a la protección de datos personales en el sector de telecomunicaciones.

Consejo de Europa. Recomendaciones del Consejo de Europa: la Recomendación nº (83) 10, de 23 de septiembre de 1983, relativa a la protección de datos personales utilizados con fines de investigación y estadísticos; la Recomendación nº (89) 2, de 18 de enero de 1989, relativa a la protección de datos personales utilizados con fines laborales; la Recomendación nº (95) 4, de 7 de febrero de 1995, relativa a la protección de datos personales en el sector de telecomunicaciones.

Consejo de Europa. Resolución nº (76) 3, por la que se constituía un Comité de Expertos en materia de protección de datos.

Consejo de Europa. Resolución nº 73/22, relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector privado.

Consejo de Europa. Resolución nº 74/29, relativa a la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector público.

Finlandia. Constitución de Finlandia de 1919. Consultado el 12.07.2020 desde: http://www.finlex.fi/fi/laki/kaannokset/1999/es19990731.pdf

Parlamento Europeo. Declaración efectuada como consecuencia de la STJUE en el asunto C-311/18 (Schrems II), en fecha 3 de septiembre de 2020. Consultado el 28.09.2020 desde: https://multimedia.europarl.europa.eu/en/committee-on-civil-liberties-justice-and-home-affairs_20200903-1345-COMMITTEE-LIBE_vd?auth_ cloudf=c3e8a8d1-e536-ac08-b5a9-1a4fbc 1f3951

Parlamento Europeo. Resolución nº 2016/2727 (RSP), de 26 de mayo de 2016, sobre los flujos transatlánticos de datos. Consultado el 24.08.2017 desde: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52016IP0233

Parlamento Europeo. Resolución nº 2016/C075/14, de fecha 4 de julio de 2013, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los Estados Unidos, los organismos de vigilancia en varios Estados miembros y su impacto en la vida privada de los ciudadanos de la Unión Europea (2013/2682[RSP]). Consultado el 28.08.2019 desde: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en& reference=2013/2682(RSP)

Parlamento Europeo. Resolución nº 2018/2645 (RSP), de 5 de julio de 2018, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. Consultado el 15.08.2020 desde: https://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_ES.html

Parlamento Europeo. Resolución nº 2020/2616 (RSP), de 17 de abril de 2020, sobre la acción coordinada de la Unión para luchar contra la pandemia de la COVID-19.

Consultado el 7 de julio de 2020 desde: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.pdf

Parlamento Europeo. Resolución nº 2020/2789 (RSP), de 20 de mayo de 2021, sobre la sentencia del Tribunal de Justicia de 16 de julio de 2020, Data Protection Commissioner / Facebook Ireland Limited y Maximillian Schrems («Schrems II»), C-311/18. Consultado el 5 de mayo de 2021 desde: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_ES.html

SEPD. "Dictamen sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves, (2011/C 181/02)", de 25 de marzo de 2011, apdo. 10

SEPD. "Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision", de fecha 30 de mayo de 2016. Consultado el 24.08.2017 desde: https://SEPD.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf

SEPD. "Resumen ejecutivo del dictamen sobre el proyecto de decisión relativo a la adecuación del escudo protector de la intimidad entre la UE y los EE. UU (2016/C 257/05)", de fecha 15 de julio de 2016, p. 3.

SEPD. "Second Opinion 5/2015 on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime", de 24 de septiembre de 2015, apdo. 24.

Unión Europea. Acuerdo de Libre Comercio suscrito entre la Unión Europea y Corea del Sur. Consultado el 15.09.2020 desde https://ec.europa.eu/trade/policy/countries-and-regions/countries/south-korea/

Unión Europea. Acuerdo de Schengen fue inicialmente suscrito el 14 de junio de 1985. Consultado el 12.07.2020 desde: https://www.boe.es/buscar/doc.php?id=BOE-A-1994-7586

Unión Europea. Convenio de Aplicación complementa las disposiciones del Acuerdo de Schengen, determinando las condiciones en las que resulta de aplicación la libre circulación, suscrito el 19 de junio de 1990.

Unión Europea. Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II).

Unión Europea. Decisión 2008/615/JAI del Consejo, 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.

Unión Europea. 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/CE del Parlamento Europeo y del Consejo (notificada con el número C [2010] 593). Consultado el 15.08.2017 desde: En línea: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32010D0087

Unión Europea. Decisión marco 2002/475/JAI del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo (2002/475/JAI).

Unión Europea. Decisión marco 2006/960/JAI del Consejo, de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea (DO L 386 de 29.12.2006), p. 89.

Unión Europea. Decisión marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

Unión Europea. Decisión marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (DO L 350 de 30.12.2008), p. 60.

Unión Europea. Decisión marco 2009/371/JAI del Consejo, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol) (DO L 121 de 15.5.2009), p. 37.

Unión Europea. 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. Consultado el 12.07.2020 desde: https://eurlex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506fd71826e6da6.0005.02/DOC _5&format=PDF

Unión Europea. 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.

Unión Europea. Directiva (UE) 2016/681 del Parlamento 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 delincuencia grave. Consultado el 12.08.2020 desde: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0681&from =EN

Unión Europea. Directiva 2004/82/CE del Consejo, de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas.

Unión Europea. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, publicada el 23 de noviembre de 1995 en el Diario Oficial nº L 281, pp. 31-50.

Unión Europea. Propuesta de Decisión del Consejo por la que se autoriza a los Estados miembros a ratificar, en interés de la Unión Europea, el Protocolo que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STCE nº 108) (COM [2018] 451 final). Consultado el 02.04.2021 desde: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018PC0451&from=PL

Unión Europea. Propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros con fines represivos (COM/2007/0654 final), de fecha 6 de noviembre de 2007. Consultado el 28.06.2020 desde: https://eur-lex.europa.eu/legal-content/ES/ TXT/HTML/?uri=CELEX:52007PC0654&from=EN

Unión Europea. Propuesta de Directiva del Parlamento Europeo y del Consejo, relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves (COM/2011/0032 final).

Unión Europea. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Unión Europea. Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo.

Unión Europea. Reglamento (UE) nº 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión.

Unión Europea. Tratado de Ámsterdam fue firmado el 2 de octubre de 1997, entrando en vigor el 1 de mayo de 1999. Consultado el 19.07.2020 desde: https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_of_amsterdam_es.pdf

Unión Europea. Tratado de Funcionamiento de la Unión Europea, publicado en el Diario Oficial de la Unión Europea, nº C 326, de 26 de octubre de 2012, p. 0001 – 0390.

Unión Europea. Tratado de la Unión Europea, publicado en el Diario Oficial de la Unión Europea, n° C 191, de 29 de septiembre de 1992, p. 0001 0110.

Unión Europea. Tratado de Lisboa, publicado en el Diario Oficial de la Unión Europea, nº 2007/C 306/01, de 17 de diciembre de 2007, y cuya entrada en vigor se produjo el 1 de diciembre de 2009. Consultado el 12.07.2020 desde: https://www.boe.es/doue/2007/306/Z00001-00271.pdf

Unión Europea. Tratado de Niza, firmado el 7 de diciembre de 2000, publicado en el Diario Oficial de la Unión Europea, en su nº 303, con fecha 14 de diciembre de 2007, p. 0004.

Unión Europea. Tratado por el que se modifican el Tratado de la Unión Europea y el Tratado Constitutivo de la Comunidad Europea, hecho en Lisboa el 13 de diciembre de

2007. Consultado el 12.07.2020 desde: https://www.boe.es/buscar/doc.php?id=BOE-A-2009-18898

Unión Europea. Tratado sobre la Unión Política, cuya firma se produciría el 7 febrero de 1992 por los Estados Miembros, modificándose, en consecuencia, el Acta Única Europea vigente de 1986. Consultado el 12.07.2020 desde: https://www.boe.es/buscar/doc.php?id=BOE-A-1994-626

Nacionales

AEPD. Informe jurídico nº 010308/2019

AEPD. Informe jurídico nº 108/2007

AEPD. Informe jurídico nº 195/2017

AEPD. Informe jurídico nº 2020/0017

AEPD. Informe jurídico nº 518/2006

AEPD. Informe jurídico nº 582/2004

AEPD. Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos. Consultado el 15.08.2017 desde: https://www.boe.es/buscar/doc.php?id=BOE-A-2000-22726

Alemania. Constitución de la República Federal de Alemania, aprobada el 8 de mayo de 1949 por el Consejo Parlamentario y firmada el 23 de mayo de 1949 en la ciudad de Bonn. Consultado el 28.06.2020 desde: https://www.btg-bestellservice.de/pdf/80206000.pdf

Alemania. Ley sobre el recuento de la población, de las profesiones, de las viviendas y de los centros de trabajo, comúnmente denominada como "Ley del Censo de Población de 1983", fue aprobada por el Parlamento Federal (en alemán, "*Bundestag*") el 4 de marzo de 1982 y, posteriormente, publicada en el Boletín Oficial en fecha 31 de marzo de 1982, pp. 369-370

España. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Consultado el 15.08.2017 desde: https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf

España. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Consultado el 12.07.2020 desde: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

España. Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Consultado el 12.07.2020 desde: https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189

España. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Consultado el 11.07.2020 desde: https://www.boe.es/buscar/act.php?id=BOE-A-1985-12666

España. Orden Ministerial de 2 de febrero de 1995. Publicada en el Boletín Oficial del Estado en fecha, 10 de febrero de 1995.

España. Orden Ministerial de 31 de julio de 1998. Publicada en el Boletín Oficial del Estado en fecha, 21 de agosto de 1998.

España. Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

España. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Consultado el 15.08.2017 desde: https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

España. Real Decreto-ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores. Consultado el 05.05.2021 desde: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-6872

España. Real Decreto 190/1996, de 9 de febrero, por el que se aprueba el Reglamento Penitenciario. Consultado el 11.07.2020 desde: https://www.boe.es/buscar/doc.php?id=BOE-A-1996-3307

Finlandia. Constitución de Finlandia de 1919. Consultado el 12.07.2020 desde: http://www.finlex.fi/fi/laki/kaannokset/1999/es19990731.pdf

Paises Bajos. Ley Fundamental del Reino de los Países Bajos. Consultado el 12.07.2020 desde: http://www.wipo.int/wipolex/es/details.jsp?id=7418

REFERENCIAS JURISPRUDENCIALES

Internacionales

Estados Unidos. 133 S. Ct. 1138 (2013)

Estados Unidos. *Barry v. City of New York*, 712 F. 2d 1554 (2d Cir. 1983)

Estados Unidos. *Bartnicki v. Vopper*, 532 U.S. 514, 534 (2001)

Estados Unidos. *Boyd v. United States,* 116 U.S. 616 (1886)

Estados Unidos. *Buckley v. Valeo*, 424 U.S. 1 (1976)

Estados Unidos. *Carpenter v. United States,* 585 U.S. 84 (2018)

Estados Unidos. *Doe v. Bolton*, 410 U.S. 179, 213 (1973)

Estados Unidos. FISC: WL 10945618 (*FISA Ct. [FISA Court]*, 03.10.2011), nota 21.

Estados Unidos. *Fisher v. United States*, 425 U.S. 391 (1976)

Estados Unidos. FTC. *Collectify, LLC*.

Estados Unidos. FTC. *Directors Desk, LLC.*

Estados Unidos. FTC. *ExpatEdge Partners, LLC.*

Estados Unidos. FTC. *Facebook, Inc.*

Estados Unidos. FTC. *Google Inc.*

Estados Unidos. FTC. *Javian Karnani, and Balls of Kryptonite, LLC*.

Estados Unidos. FTC. Myspace, LLC.

Estados Unidos. FTC. *Onyx Graphics, Inc.*

Estados Unidos. FTC. *Progressive Gaitways, LLC*.

Estados Unidos. FTC. *World Innovators, Inc*.

Estados Unidos. *Goldman v. United States,* 316 U.S. 129 (1942)

Estados Unidos. *Gouled v. United States,* 255 U.S. 298 (1921

Estados Unidos. *Griswold v. Connecticut*, 381 U.S. 479, 484-485 (1965)

Estados Unidos. *Katz v. United States*, 389 U.S. 347 (1967)

Estados Unidos. *Kyllo v. United States*, 533 U.S. 27 (2001)

Estados Unidos. *McIntyre v. Ohio Election Comm'n*, 514 U. S. 334 (1995)

Estados Unidos. *Memorandum opinion of United States District Court for the District of Columbia*, de 16 de diciembre de 2013 (*Civil Action No*. 13-0851), p. 9

Estados Unidos. *NAACP v. Alabama*, 357 U.S. 449 (1958)

Estados Unidos. *Olmstead v. United States*, 277 U.S. 438 (1928)

Estados Unidos. *Roe v. Wade*, 410 U.S. 113 (1973)

Estados Unidos. *Shelton v. Tucker*, 364 U.S. 479 (1960)

Estados Unidos. *Slayton v. Willingham*, 726 F. 2d 631 (10th Cir. 1984)

Estados Unidos. *Smith v. Maryland*, 442 US 73 5 (1979)

Estados Unidos. *United States v. Miller*, 425 U.S. 435 (1976)

Estados Unidos. *United States v. United States District Court*, 407 U.S. 297 (1972)

Estados Unidos. *Whalen v. Roe*, 429 U.S. 589 (1977)

Japón. *1965 (A) No. 1187, Judgement of the Grand Bench of the Supreme Court of December 24, 1969*, Keishu Vol. 23, No. 12, p. 1625

Japón. *Judgement of the Grand Bench of the Supreme Court, March 6, 2008*, Minshu, Vol. 62, nº 3, p. 665

Comunitarias

STCE. Sentencia de fecha, 6 de noviembre de 2003, asunto C-101/2001.

TEDH. Asunto Antunes Rocha contra Portugal, de 31 de mayo de 2005

TEDH. Asunto Bernh Larsen Holding AS y otros contra Noruega, nº 24117/08, de 14 de marzo de 2013

TEDH. Asunto Bouchacourt contra Francia, de 17 de diciembre de 2009

TEDH. Asunto Caso L. L. contra Francia, de 10 de octubre de 2006

TEDH. Asunto Caso S. y Marper contra Reino Unido, de 4 de diciembre de 2008

TEDH. Asunto Dimitrov-Kazakov contra Bulgaria, 10 de febrero de 2011

TEDH. Asunto Goggins y otros contra Reino Unido, de 19 de julio de 2011

TEDH. Asunto Haralambie contra Rumanía, nº 21737/03, de 27 de octubre de 2009

TEDH. Asunto Joanna Szul contra Polonia, de 13 de noviembre de 2012

TEDH. Asunto K.H. y otros contra Eslovaquia, nº 32881/04, de 6 de noviembre 2009

TEDH. Asunto Khelili contra Suiza, de 18 de octubre de 2011

TEDH. Asunto Khelili contra Suiza, nº 16188/07, de 18 de octubre de 2011

TEDH. Asunto Klass y otros contra la República de Alemania, de 6 de septiembre de 1978

TEDH. Asunto Leander contra Suecia, nº 9248/81, de 26 de marzo de 1987

TEDH. Asunto M.M. contra Reino Unido, de 13 de noviembre de 2012

TEDH. Asunto N.K.M. contra Hungría, de 14 de mayo de 2013.

TEDH. Asunto Peck contra el Reino Unido, nº 44647/98, de 28 de enero 2003

TEDH. Asunto Rotaru contra Rumanía [GS], nº 28341/95, de 4 de mayo de 2000

TEDH. Asunto Sanoma Uitgevers B.V. contra Países Bajos, 14 de septiembre de 2010

TEDH. Asunto Taylor-Sabori contra Reino Unido, nº 47114/99, de 22 de octubre de 2002

TEDH. Asunto Wasmuth contra Alemania, de 17 de febrero de 2011

TJUE. Conclusiones del Abogado General Sr. Henrik Saugmandsgaard Øe sobre el asunto C-311/18, presentadas el 19 de diciembre de 2019.

TJUE. Conclusiones del abogado general Yves Bot en el asunto C-362/14, presentadas el 23 de septiembre de 2015.

TJUE. Dictamen 1/15, de 26 de julio de 2017, en relación con el proyecto de Acuerdo entre Canadá y la Unión Europea sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros.

TJUE. Sentencia de fecha, 16 de diciembre de 2008, en el asunto C-73/07.

TJUE. Sentencia de fecha, 16 de julio de 2020, en el asunto C-311/18.

TJUE. Sentencia de fecha, 21 de diciembre de 2016, en los asuntos C 203/15 y C 698/15.

TJUE. Sentencia de fecha, 24 de noviembre de 2011, en los asuntos acumulados C-468/10 y C-469/10.

TJUE. Sentencia de fecha, 29 de enero de 2008, en el asunto C-275/06.

TJUE. Sentencia de fecha, 6 de octubre de 2015, en el asunto C- 362/14.

TJUE. Sentencia de fecha, 7 de mayo de 2009, en el asunto C-553/07.

TJUE. Sentencia de fecha, 8 de abril de 2014, en los asuntos acumulados C-293/12 y C-594/12.

TJUE. Sentencia de fecha, 8 de abril de 2014, en los asuntos acumulados C-293/12 y C-594/12.

TJUE. Sentencia de fecha, 9 de noviembre de 2010, en los asuntos acumulados C-92/09 y C-93/09.

TJUE. Sentencia de fecha, 29 de julio de 2019, en el asunto C-40/17.

Nacionales

España. Audiencia Nacional (Contencioso-Administrativo). Sentencia de 15 de marzo de 2002, Sección Primera (nº de recurso: 271/2001)

España. Tribunal Constitucional. Auto nº 155/2009, de 25 de junio

España. Tribunal Constitucional. Auto nº 29/2008, de 28 de enero

España. Tribunal Constitucional. Auto nº 420/2003, de 16 de diciembre

España. Tribunal Constitucional. Sentencia 254/1993, de 20 de julio de 1993 (Recurso de amparo 1827/1990).

España. Tribunal Constitucional. Sentencia nº 110/1984, de 26 de noviembre.

España. Tribunal Constitucional. Sentencia nº 127/2003, de 30 de junio

España. Tribunal Constitucional. Sentencia nº 17/2013, de 31 de enero

España. Tribunal Constitucional. Sentencia nº 231/1988, de 2 de diciembre

España. Tribunal Constitucional. Sentencia nº 233/2005, de 26 de septiembre

España. Tribunal Constitucional. Sentencia nº 254/1993, de 20 de julio

España. Tribunal Constitucional. Sentencia nº 29/2013, de 11 de febrero

España. Tribunal Constitucional. Sentencia nº 290/2000, de 30 de noviembre.

España. Tribunal Constitucional. Sentencia nº 292/2000, de 30 de noviembre

España. Tribunal Constitucional. Sentencia nº 96/2012, de 7 de mayo

España. Tribunal Supremo (Contencioso-Administrativo). Sentencia de 25 de septiembre de 2006, Sección Sexta (Recurso de Casación nº 3223/2002)

DOCUMENTOS DE INTERÉS

AEPD. *Memoria de la Agencia de Protección de Datos*, Madrid: Ed. Agencia de Protección de Datos, 1995, pp. 71-72

APEC Privacy Framework (2015). Consultado el 15.09.2020 desde https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

Asamblea Popular Nacional de la República de China. Comité Permanente de la Asamblea Popular Nacional. Consultado el 15.05.2020 desde http://www.npc.gov.cn/englishnpc/c4166/column.shtml

Comisión Europea. eHealth Network. "Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States", en su versión 1.0, de fecha 15 de abril de 2020, que contiene el conjunto de instrumentos adoptados por parte de la Unión Europea para el uso de aplicaciones móviles de rastreo de contactos y envío de advertencias. Consultado el 7 de junio de 2020 desde: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

Consejo de Europa. "Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", en *Council of Europe Treaty Series*, Nº 223 (2018). Consultado el 28.06.2020 desde: https://rm.coe.int/16808ac91a

Consejo de Europa. "Protección de Datos. Convenio del Consejo de Europa de 1981", en *Documentación Informática: serie amarilla / Tratados internacionales*, nº 3 (1983), Madrid: Ed. Presidencia del Gobierno. Servicio Central de Publicaciones. Servicio Central de informática, p. 31

Consejo de Europa. *Handbook on European data protection law*, Luxemburgo, 2018

Federal Trade Commission. *Self-Regulation and Privacy online: A report to Congress*, Estados Unidos, 1999

Ministerio de Defensa. "Monografías del SOPT. La Guerra electrónica en España. Ministerio de Defensa". Consultado el 20.08.2020 desde: https://www.tecnologiaeinnovacion.defensa.gob.es/Lists/Publicaciones/Attachments/13/monografia_sopt_2.pdf

OCDE. “The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines”, en *OECD Digital Economy Papers*, Ed. OECD Publishing, nº 176 (2011). Consultado el 28.06.2020 desde: http://dx.doi.org/10.1787/5kgf09z90c31-en

OCDE. Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (1980). Consultado el 31.05.2020 desde: https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm

OCDE. *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data*. Consultado el 01.06.2020 desde: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

SEPD. Carta emitida por parte del Supervisor Europeo de Protección de Datos. Consultado el 07.06.2020 desde: https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_covid-19_monitoring_of_spread_en.pdf

U.S. CENSUS BUREAU FOR THE UNITED STATES OF AMERICA. U.S. and World Population Clock. Consultado el 15.08.2020 desde: https://www.census.gov/popclock/

U.S. CONGRESSIONAL RESEARCH SERVICE, “Digital Trade and U.S. Trade Policy”, pp. 20-21

Unión Europea. Estrategias de la Unión Europea en materia de transferencias internacionales de datos a Corea del Sur. Consultado el 15.09.2020 desde: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN