EL CONCEPTO DE DATO PERSONAL EN LA UNIÓN EUROPEA: UNA PIEZA CLAVE EN SU PROTECCIÓN

PILAR CONCELLÓN FERNÁNDEZ

Investigadora postdoctoral[1]

Universidad de Oviedo

concellonpilar@uniovi.es

RESUMEN: Vinculada inicialmente a las libertades del mercado único, la protección de datos personales forma parte de los derechos fundamentales garantizados en la Unión Europea. A través de una jurisprudencia evolutiva, el TJUE ha contribuido a la configuración del concepto de dato personal. En esta tarea, el Tribunal se ha adaptado a los cambios normativos y a la evolución tecnológica. Por su parte, el nuevo Reglamento (UE) 2016/679 ha actualizado la definición de dato personal para tener en cuenta las aportaciones jurisprudenciales y los nuevos retos derivados de las exigencias sociales y técnicas.

PALABRAS CLAVE: Dato personal; Protección de datos; Directiva 95/46, Reglamento 2016/679; TJUE.

THE PERSONAL DATA DEFINITION IN THE EUROPEAN UNION: A KEY IN ITS PROTECTION

ABSTRACT: Initially linked to the freedoms of the single market, the protection of personal data forms part of the fundamental rights guaranteed in the European Union. Through an evolutionary jurisprudence, the CJEU has contributed to the configuration of the concept of personal data. In this task, the Court has adapted to the regulatory changes and to the technological evolution. On the other hand, the new Regulation (EU) 2016/679 has updated the definition of personal data to take into account the jurisprudential contributions and new challenges arising from social and technical requirements.

KEYWORDS: Personal data; Data Protection; Directive 95/46, Regulation 2016/679, CJEU.

El derecho a la protección de los datos personales, también denominado derecho a la autodeterminación informativa[2], supone la protección jurídica de las personas en lo que concierne al tratamiento de sus datos de carácter personal[3] y con ello el poder del sujeto de determinar qué información sobre su persona y sus circunstancias puede ser comunicada a terceros en cada momento[4].

---

[1] El presente trabajo se adscribe al Proyecto de I+D "Obstáculos a la movilidad de personas en los nuevos escenarios de la UE", Ref. DER2017-86017-R.

[2] Algunos autores se refieren al derecho a la protección de los datos personales como el derecho a la "intimidad informática"; véase CONDE ORTIZ, C., "*La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad"*, Universidad de Cádiz, Madrid, 2005, p. 27 y SARDINA VENTOSA, F., "El derecho a la intimidad informática y el tratamiento de datos personales para la prevención del fraude", *Actualidad Informática Aranzadi*, nº 25, 1997, p. 3.

[3] Para CONDE ORTIZ y SARDINA VENTOSA el reconocimiento de este derecho supondría además de la protección jurídica de las personas en lo que concierne al tratamiento de sus datos, la tutela debida a los ciudadanos contra la posible utilización por terceros, no autorizados, de sus datos personales. CONDE ORTIZ, C., *op. cit.*, p. 27; SARDINA VENTOSA, F., *op. cit.,* p. 3.

[4] RUIZ MIGUEL, C. "El derecho a la protección de los datos personales", *RDCE*, nº 14, 2003, p. 32.

El reconocimiento de este derecho en el ordenamiento de la Unión Europea se ha hecho de manera progresiva, diferenciándose varias etapas, tanto en la jurisprudencia como a nivel normativo[5]. En la actualidad, la entrada en vigor 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[6] ha supuesto un salto cualitativo de gran trascendencia práctica. Son muchos los aspectos de interés en este Reglamento; entre ellos, el concepto de dato personal es una pieza clave.

I. LA PROTECCIÓN DE LOS DATOS PERSONALES EN EL ORDENAMIENTO COMUNITARIO: DE LA DIRECTIVA 95/46 AL REGLAMENTO 2016/679

Una vez establecido el mercado único y en conexión con sus libertades, se planteó la necesidad de armonizar las regulaciones estatales en materia de protección de datos. En 1995, el Parlamento y el Consejo aprobarían el que sería el primer acto normativo en relación al tratamiento de datos personales, 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 (en adelante la Directiva 95/46)[7].

En sus considerandos, la Directiva 95/46 hacía hincapié en que la integración económica y social resultante del establecimiento y funcionamiento del mercado interior iba a implicar necesariamente un aumento notable de los flujos transfronterizos de datos personales entre todos los agentes de la vida económica y social de los Estados miembros, de manera que las administraciones nacionales de los diferentes Estados miembros estarían destinadas a colaborar y a intercambiar datos personales.

Apuntaba también que para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debía ser equivalente en todos los Estados miembros; lo cual no podía lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta, en particular, las grandes diferencias existentes por aquel entonces entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales fuera regulado de forma coherente y de conformidad con el objetivo del mercado interior.

Este enfoque justifica que la base jurídica elegida fuera el art. 100 A TCE[8]. A la Directiva 95/46 se sumaron posteriormente la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)[9] y el Reglamento 45/2001/CE del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos[10].

No obstante, no fue hasta la reforma operada por el Tratado de Ámsterdam cuando la protección de los datos personales fue reconocida expresamente como derecho. El entonces artículo 213b TCE, actual art. 16 del TFUE, proclama que:

---

[5] *Ibid*, p. 15.

[6] *DOUE* L 119, de 4 de mayo de 2016. Sobre este Reglamento, puede verse CHEN, Y. H., "The EU Data Protection Law Reform: Challenges for Service Trade Liberalization an Possible Approaches for Harmonizing Privacy Standards into the Context of GATS", *SYbIL*, nº 19, 2015, pp. 211-220; DAVARA RODRÍGUEZ, M. A., "Reglamento Europeo sobre protección de datos", *Actualidad administrativa*, nº 7-8, 2016, pp. 52-57; KUMAR DAS, A., "European Union's General Data Protection Regulation, 2018: A brief overview", *Annals of Library and Information Studies*, nº 65, 2018, pp. 139-140; PIÑAR MAÑAS, J. L. (dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Editorial Reus, 2016; TRONCOSO REIGADA, A., "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *REDE*, nº 43, pp. 25-184; VOIGT, P. y VON DEM BUSSCHE, A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer, 2017.

[7] *DOUE* n° L 281, de 23 de noviembre de 1995.

[8] "1. No obstante, lo dispuesto en el artículo 100, y salvo que el presente tratado disponga otra cosa, se aplicarán las disposiciones siguientes para la consecución de los objetivos enunciados en el artículo 8 A. El Consejo, por mayoría cualificada a propuesta de la Comisión y en cooperación con el Parlamento Europeo y previa consulta al Comité económico y social, adoptará las medidas relativas a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros que tengan por objeto el establecimiento y el funcionamiento del mercado interior…".

[9] *DOUE* nº L 201, de 31 de julio de 2002.

[10] *DOUE* nº L 8, de 12 de enero de 2001.

> "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos".

Este posterior reconocimiento del derecho provocó que algún autor pusiera en duda la base jurídica de las normas de Derecho derivado hasta entonces adoptadas[11]. Para RUIZ MIGUEL, en el momento de adopción de las Directivas 95/46 y 2002/58 la por aquel entonces Comunidad Europea no tenía competencia para aprobar tales directivas que afectaban a un derecho fundamental:

> "En ese momento los tratados ni habían consagrado específicamente el derecho a la protección de datos personales cuyo destinatario fueran dos Estados, ni siquiera habían otorgado a las Comunidades o a la Unión competencia en materia de derechos fundamentales"[12]

No obstante, como ha explicado MARTÍN Y PÉREZ NANCLARES, la existencia de estas normas no significaba que del Derecho comunitario pudiese deducirse un derecho subjetivo a la protección de datos:

> "En realidad la Directiva únicamente encomienda a los Estados miembros la tarea de garantizar, con arreglo a los criterios armonizados por ella, la protección de las libertades y de los derechos fundamentales de las personas en lo que respecta al tratamiento de los datos personales (art. 1) con el objetivo de no obstaculizar entre ellos la libre circulación de datos personales por motivos de protección de los derechos fundamentales como derivación de una exigencia del mercado interior, ya que su base jurídica competencial fue el entonces art. 100 (actualmente art. 95 TCE)"[13].

En la Carta de los Derechos Fundamentales, el consenso sobre la inclusión del derecho a la protección de datos no tardó en manifestarse. Desde los primeros trabajos, los diferentes documentos de trabajo de la Carta elevaron la protección de datos a la categoría de derecho fundamental. Así, el art. 15 del Proyecto de Carta de los Derechos Fundamentales de la Unión Europea, disponía que "toda persona física tiene derecho a la protección de sus datos de carácter personal". En sus Explicaciones, se señalaba que parecía preferible enunciar una norma general en lugar de recoger una lista detallada de principios que estarían sujetos a cambios en razón del progreso técnico y proponía una redacción alternativa más completa y cercana a la de los textos comunitarios, al tiempo que planteaba la creación de un órgano independiente de control:

> "Se garantiza el respeto de los derechos y libertades previstos en la presente Carta, y en particular el derecho a la vida privada, con respecto al tratamiento por cualquier medio de toda información relativa a una persona física identificada o identificable. La información debe tratarse con lealtad, con fines determinados y a reserva del consentimiento de las personas afectadas o de otro fundamento legítimo previsto por la ley"[14].

Finalmente, el derecho a la protección de datos se consagró en el art. 8 de la Carta:

> "Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Estos datos se tratarán de modo leal, para fines determinados 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 su rectificación. El respeto de estas normas quedará sujeto al control de una autoridad independiente"[15].

---

[11] Como veremos más adelante, el propio Abogado General TIZZANO, en el marco del asunto *Österreichischer Rundfunk y otros* consideró que la Directiva 95/46 no podía ser aplicada más allá de los supuestos en los que estuviera en juego la libre circulación.

[12] RUIZ MIGUEL, C., *op. cit.*, p. 18.

[13] MARTÍN PÉREZ DE NANCLARES, J., "Artículo 8. Protección de datos de carácter personal" en MANGAS MARTÍN, A., *Carta de los derechos fundamentales de la Unión Europea. Comentario artículo por artículo*, BBVA, Bilbao, 2008, p. 226.

[14] CHARTE 4137/00 CONV 8, de 4 de febrero de 2000, art. 15. Disponible en http://data.consilium.europa.eu/doc/document/ST-4137-2000-INIT/es/pdf (visitado por última vez el 17 de octubre de 2018).

[15] *DOUE* nº C 364 de 18 de diciembre de 2000. La Carta ha sido publicada con posterioridad en *DOUE* C 303 de 14 de diciembre de 2007, *DOUE* C 83 de 30 de marzo de 2010, *DOUE* C 326 de 26 de octubre de 2012 y *DOUE* C 202 de 7 de junio de 2016.

Tal como señalaban las Explicaciones del Praesidium[16], el art. 8 de la Carta se basa en el artículo 16 del TFUE y en la Directiva 95/46, así como en el artículo 8 del CEDH y en el Convenio del Consejo de Europa de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

En definitiva, durante mucho tiempo la Directiva 95/46 constituyó el texto de referencia, a escala europea, en materia de protección de datos personales. Creaba un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea. Con ese objeto, la Directiva fijaba límites estrictos para la recogida y utilización de los datos personales y solicitaba la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la supervisión de cualquier actividad relacionada con el tratamiento de los datos personales.

La Directiva 95/46 vertebraba el derecho a la protección de los datos personales en torno a varios principios. En primer lugar, el *principio de consentimiento*, pues el art. 7 de la Directiva precisaba que los datos personales de una persona sólo podrían "tratarse" si la persona en cuestión había dado su consentimiento "inequívoco" de manera previa. Lo cual significa que a diferencia de lo dispuesto en el Convenio de 1981 del Consejo de Europa[17], el consentimiento no se podía solicitar de manera simultánea al tratamiento de los datos, sino que debía otorgarse *ad futurum*.

En segundo lugar, el *principio de información* aseguraba que los responsables del tratamiento de los datos debían comunicar a la persona afectada la identidad del responsable del tratamiento de los datos y los fines del tratamiento[18].

Además, los datos debían ser exactos y actuales, debiendo ser tratados de "manera leal y lícita":

> "deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados"[19].

Sin restricciones y con una periodicidad y sin retrasos ni gastos excesivos, los titulares de los datos debían poder confirmar "la existencia o inexistencia del tratamiento de datos que les concerniesen"[20], los fines de dichos tratamientos, así como los destinatarios o las categorías de destinatarios a quienes se iban a comunicar dichos datos.

Finalmente, se debía imponer el *principio de seguridad y confidencialidad*, lo que significa que se debían adoptar las medidas necesarias para asegurar la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados[21].

A pesar de la vocación armonizadora de la Directiva, la trasposición de su contenido no resultó del todo satisfactoria. Tal como señalaba la Comisión, los Estados miembros siguieron adoptando normativas divergentes que tenían como resultado diferentes niveles de protección:

> "Es 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. En determinadas disposiciones el margen de acción de los Estados miembros es muy reducido o inexistente y pese a ello se han producido divergencias: véanse, por ejemplo, las «definiciones» o las listas cerradas de la Directiva, como las de los artículos 7 (motivo de legitimación del tratamiento), el apartado 1 del artículo 8 (datos sensibles), o los artículos 10 (información al interesado), 13 (excepciones) y 26 (excepciones relativas a las transferencias a terceros países, etc.). Ello hace pensar en una falta de conformidad

---

[16] CHARTE 4333/00 CONV 36, de 4 de junio de 2000. Las Explicaciones actualizadas se publicaron en *DOUE* C 303 de 14 de diciembre de 2007.

[17] Convenio de 1981 para la protección de los individuos respecto al tratamiento automatizado de datos personales, *BOE* núm. 274 de 15 de noviembre de 1985.

[18] U otra información tal como: "los destinatarios o las categorías de destinatarios de los datos, el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder, la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado" (art. 10).

[19] Art. 6 d).

[20] Art. 12 a).

[21] Art. 17.1.

con la legislación comunitaria. El artículo 4 (Derecho nacional aplicable) también ha sido transpuesto de manera incorrecta en una serie de casos"[22].

La Comisión comenzaba su primer informe sobre la aplicación de la Directiva 95/46 señalando que en diciembre de 1999 había decidido denunciar a Francia, Alemania, Irlanda Luxemburgo y los Países Bajos ante el TJUE por no haber notificado todas las medidas necesarias para aplicar la Directiva. Denuncias que salvo en el caso de Luxemburgo terminarían archivándose:

"En 2001, los Países Bajos y Alemania notificaron sus medidas y la Comisión archivó las causas instruidas contra dichos Estados. Francia notificó su ley de protección de datos de 1978, por lo que se abandonaron los procedimientos contra dicho Estado. Francia anunció al mismo tiempo su intención de aprobar una nueva ley que aún no se ha adoptado. Respecto a Luxemburgo, la acción de la Comisión dio lugar a la condena de dicho Estado miembro por el Tribunal de Justicia por no cumplir sus obligaciones. Posteriormente se aplicó la Directiva a través de una nueva ley, que entró en vigor en 2002. Irlanda notificó una aplicación parcial en 2001; sin embargo, recientemente se ha aprobado un proyecto de ley completo"[23].

En su segundo informe, la Comisión señalaba que si bien la aplicación había mejorado y todos los Estados miembros habían transpuesto ya la Directiva, algunos países todavía no la habían aplicado correctamente:

"Algunos Estados miembros no han podido incorporar ciertas disposiciones importantes de la Directiva. En otros casos, la transposición o la práctica no se ha llevado a cabo con arreglo a la Directiva o ha quedado fuera del margen de maniobra que se ha dejado a los Estados miembros"[24].

Entre otros aspectos, la Comisión mostraba su preocupación por el hecho de algunas autoridades supervisoras de la protección de datos no actuaran con total independencia y tuvieran poder y recursos suficientes para llevar a cabo sus tareas:

"Estas autoridades son componentes fundamentales en el sistema de protección concebido por la Directiva, y cualquier defecto a la hora de garantizar su independencia y sus poderes tiene un amplio efecto negativo sobre la aplicación de la legislación relativa a la protección de datos"[25].

No obstante, atribuía las divergencias en la trasposición al margen de maniobra que dejaba la Directiva, concluyendo que esas diferencias no planteaban un problema real al mercado interior:

"La Directiva contiene una serie de disposiciones formuladas de manera general y, explícita o implícitamente, deja a los Estados miembros un margen de maniobra para la adopción de la legislación nacional. Dentro de esos límites pueden surgir diferencias en la legislación nacional. Estas divergencias no son mayores en este sector que en otros campos de la actividad económica y son una consecuencia natural de dicho margen"[26].

Las incongruencias en la protección de los datos personales en los diferentes Estados miembros[27], la aprobación del Tratado de Lisboa y los cambios en las tecnologías de la información y la comunicación animaron a la Comisión a modificar el marco normativo de la protección de datos mediante el Reglamento (UE) 2016/679 ya citado, por el que se deroga la Directiva 95/46/CE. Como advirtiera la Comisión:

"La Directiva de la UE de 1995, instrumento legislativo básico para la protección de los datos personales en Europa, marcó un hito en la historia de la protección de datos. Sus objetivos, a saber, asegurar el funcionamiento del mercado único y la protección efectiva de los derechos y las

---

[22] Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46 CE), COM (2003) 265 final, p. 12. Por su parte TRONCOSO REIGADA, denunciaba las diferencias existentes en las normativas de los Estados Miembros en relación con el concepto de dato personal y su ámbito de aplicación: "La mayoría de las leyes se aplican a las personas naturales o físicas, excluyendo a los fallecidos. Algunas leyes lo manifiestan de manera clara refiriéndose a *natural living or living individuals*; en cambio, otras se aplican a personas fallecidas", TRONCOSO REIGADA, A., *op. cit.,* p.74.

[23] Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46 CE), COM (2003) 265 final, p. 3

[24] Comunicación de la Comisión al Parlamento Europeo y al Consejo, de 7 de marzo de 2007, "Seguimiento del Programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos", COM (2007) 87 final, p. 6.

[25] *Ibid.*

[26] *Ibid.*

[27] En este sentido, véase FERRETTI, F., "Data protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights?", *CMLRev*, nº 51, 2014, p. 867.

libertades de los ciudadanos, siguen siendo válidos. No obstante, se adoptó hace diecisiete años, momento en que Internet estaba aún en una fase incipiente. En el nuevo y complejo entorno digital actual, las normas vigentes no aportan ni el grado de armonización requerido ni la eficacia necesaria para preservar el derecho a la protección de datos personales"[28].

II. EL TJUE Y LA PROTECCIÓN DE LOS DATOS PERSONALES

Desde el conocido asunto *Stauder*[29] y mucho antes de su reconocimiento expreso, el TJUE ha tenido que enfrentarse a diferentes cuestiones relativas al derecho a la protección de los datos personales.

1. La interpretación de la Directiva 95/46/CE y la ponderación con otros derechos fundamentales

En un primer momento, el TJUE interpretó la normativa comunitaria de protección de datos haciendo referencia al derecho fundamental a la intimidad o a la necesidad de prevenir cualquier restricción de la libre circulación de datos entre los Estados miembros[30].

Así, en el asunto *Comisión v. Alemania*[31], en el marco de un recurso de incumplimiento instado contra la República Federal de Alemania, sin reconocer la existencia de un derecho a la protección de los datos de carácter personal, el TJUE concluyó que el derecho al respeto de la vida privada y el derecho a la protección del secreto médico constituían derechos fundamentales protegidos por el ordenamiento jurídico comunitario[32].

Dos años más tarde, el TJUE tenía ocasión de conocer del recurso de casación interpuesto por la señora Anna Maria Campogrande en el marco de un litigio directamente relacionado con la protección y la cesión de datos personales. La señora Campogrande había sido sancionada disciplinariamente como consecuencia de su negativa a facilitar a la Comisión, institución para la que trabajaba, la dirección de su domicilio en Bélgica[33].

---

[28] "La protección de la privacidad en un mundo interconectado Un marco europeo de protección de datos para el siglo XXI", COM (2012) 09 final, p. 3.

[29] Sentencia de 12 de noviembre de 1969, C-20/69, ECLI:EU:C:1969:57. En este asunto, a propósito de si los principios generales del Derecho comunitario eran compatibles con una Decisión de la Comisión que supeditaba el suministro de mantequilla a precio reducido a los beneficiarios de determinados regímenes de asistencia social al hecho de que se comunicara a los vendedores el nombre de los beneficiarios, el TJUE evitó identificar un derecho a la vida privada o a la protección de datos personales como tales y señaló que la disposición impugnada debía interpretarse en el sentido de que no imponía ni prohibía la identificación nominal de los beneficiarios, de modo que no se había revelado ningún elemento que permitiera cuestionar los derechos fundamentales de la persona. En este sentido, RUIZ MIGUEL, C., "El derecho a la protección de los datos personales", *op. cit*., p. 15.

[30] En este sentido, véase OLIVER, P. "The protection of privacy in the economic sphere before the European Court of Justice", *CMLRev*, nº 46, 2009, pp. 1443-1483.

[31] Sentencia de 8 de abril de 1992, C-62/90, ECLI:EU:C:1992:169, apdo. 23. En su sentencia, el TJUE señaló que las autoridades nacionales debían controlar, en aras de la protección de la salud pública, la importación de medicamentos suministrados únicamente con receta en el Estado miembro de importación, respetando, no obstante, los derechos al respeto de la vida privada y el derecho a la protección del secreto médico y terminó concluyendo que Alemania no había demostrado que le hubiese sido imposible adoptar medidas de control que respondieran a las exigencias de la protección de la salud pública y de la vida de las personas

[32] Para ello, el TJUE traía a colación el asunto *National Panasonic/Comisión* para reconocer que el derecho a la intimidad reconocido en el 8 de CEDH y en las constituciones de los Estados miembros era un derecho fundamental protegido por el ordenamiento comunitario: "Los derechos fundamentales forman parte integrante de los principios generales del Derecho, cuyo respeto asegura el propio Tribunal, conforme a las tradiciones constitucionales comunes a los Estados miembros, así como a los Tratados internacionales en los que han sido parte o a los que se han adherido los Estados miembros".

[33] La administración de la Comisión había pedido a sus funcionarios residentes en Bélgica que rellenasen un cuestionario destinado a actualizar sus datos personales, a fin de que éstos pudiesen ser transmitidos a las autoridades belgas, de conformidad con el Acuerdo entre las Instituciones de las Comunidades Europeas radicadas en Bélgica y el Gobierno belga en materia de información relativa a los funcionarios de tales Instituciones. La Sra. Campogrande no solo no había rellenado dicho cuestionario sino que había presentado una reclamación pidiendo que se denunciase el Acuerdo, al entender que carecía de base legal. Tras apercibirla varias veces y ante su negativa a facilitar la información, le fue impuesta una

En su sentencia de 21 de abril de 1994[34], el TJ no cuestionó si la cesión de datos sin el consentimiento de los funcionarios entre la Comisión y la administración belga vulneraba el derecho a la protección de datos personales[35] y desestimó por completo las pretensiones de la recurrente, señalando que la Comisión tenía el derecho y "también la obligación de comunicar a las autoridades belgas la dirección particular de la Sra. Campogrande"[36].

Por contra, ese mismo año y poco antes de adoptarse la Directiva 95/46, en el asunto *X/Comisión*[37], el TJUE volvió a recordar que el derecho al respeto de la vida privada, en particular, el derecho a mantener en secreto su estado de salud, constituía uno de los derechos fundamentales protegidos por el ordenamiento jurídico[38].

No obstante, la primera vez que el TJ tuvo ocasión de delimitar el ámbito de aplicación de la Directiva 95/46 fue en los asuntos acumulados *Österreichischer Rundfunk y otros*[39]. En el marco de un contencioso entre el Tribunal de Cuentas y un gran número de organismos sujetos a su control, entre los que figuraban varias entidades territoriales (un Land y dos municipios), empresas públicas, así como una cámara de comercio, el Verfassungsgerichtshof (Tribunal Constitucional austriaco), que era uno de los órganos jurisdiccionales remitentes, solicitó al TJUE que interpretara varias disposiciones de la Directiva 95/46. El TJUE aprovechó su sentencia de 20 de mayo de 2003 para señalar que el recurso a la base jurídica del artículo 100 A del Tratado[40] no presuponía la existencia de un vínculo efectivo con la libre

---

sanción de amonestación que impugnaría en primer lugar ante el Tribunal de Primera Instancia y que desembocaría finalmente en un recurso ante el Tribunal de Justicia.

[34] Campogrande/Comisión, C-22/93 P, ECLI:EU:C:1994:164.

[35] Así lo apunta RUIZ MIGUEL, C., *op. cit.,* p. 17.

[36] Apdo. 27 de la sentencia.

[37] Sentencia de 5 de octubre de 1994, C-404/92, ECLI:EU:C:1994:361.

[38] En este caso, el recurrente invocaba directamente la infracción del artículo 8 del CEDH, al entender que pese a su negativa expresa, el médico asesor de la Comisión le había sometido a una prueba indirecta de detección del SIDA, vulnerando de este modo su derecho a la intimidad. El TJUE concluyó que aunque el reconocimiento previo a la contratación servía a un interés legítimo de las Instituciones comunitarias, que debían hallarse en condiciones de realizar su misión, dicho interés no justificaba que se hubiese procedido a realizar una prueba contra la voluntad del recurrente: "Dado que el recurrente se había negado expresamente a someterse a una prueba de detección del SIDA, el mencionado derecho se oponía a que la administración realizara cualquier tipo de prueba que permitiera sospechar o comprobar la existencia de dicha enfermedad, cuya revelación había rehusado aquél" (apdo. 23 de la sentencia).

[39] Sentencia de 20 de mayo de 2003, C-465/00, C-138/01 y C-139/01, ECLI:EU:C:2003:294. El Tribunal de Cuentas reclamaba que los diferentes organismos no le habían comunicado o le habían comunicado en distinto grado información sobre los ingresos de varios empleados. En particular alegaba que los organismos mencionados tenían la obligación de mencionar en el informe que le remitían el nombre de las personas afectadas indicando sus ingresos anuales. En su escrito de planteamiento el Tribunal Constitucional señalaba que una amplia información del público, como la que reclamaba el Tribunal de Cuentas sobre la retribución anual que percibían los empleados de los diferentes organismos, debía considerarse una injerencia en la vida privada que, con arreglo al artículo 8, apartado 2, del CEDH, sólo podía justificarse cuando dicha información sirviese al bienestar económico del país. Sin embargo, el Tribunal Constitucional dudaba si la divulgación, mediante el informe, de datos personales sobre los ingresos favorecía el bienestar económico del país o constituía una injerencia desproporcionada en la vida privada.

[40] El Abogado General TIZZANO entendía que el tratamiento de los datos efectuado por el Tribunal de Cuentas y los órganos sometidos a su control se había efectuado en el ejercicio de una actividad pública de control contable que no estaba comprendida en el ámbito de aplicación del Derecho comunitario y en consecuencia descartaba que la Directiva 95/46 fuera aplicable al litigio principal. Para TIZZANO, la Directiva 95/46 se había adoptado con el fin de promover la libre circulación de los datos personales y en consecuencia aunque la protección de los derechos fundamentales constituía un valor importante y una exigencia que el legislador comunitario había tenido en cuenta al definir el régimen armonizado necesario para el establecimiento y el funcionamiento del mercado interior, no constituía, sin embargo, un objetivo autónomo de la Directiva: "En caso contrario, debería entenderse que la Directiva persigue proteger a los individuos en lo que respecta al tratamiento de datos personales incluso prescindiendo del objetivo de promover la libre circulación de dichos datos, con la paradójica consecuencia de extender su ámbito de aplicación también al tratamiento de datos efectuado en el ejercicio de actividades que no presentan ninguna relación con el establecimiento o el funcionamiento del mercado interior". Según TIZZANO atribuir a la Directiva el objetivo de garantizar el derecho a la intimidad suponía cuestionar la validez de la propia Directiva, dado que en ese caso su base jurídica resultaría claramente inadecuada: "En efecto, el artículo 100 A no puede invocarse como fundamento de medidas que trascienden las finalidades específicas mencionadas en dicha disposición, es decir, de medidas que no encuentran su justificación en el objetivo de promover «el establecimiento y el funcionamiento del mercado interior»" (conclusiones del Abogado General A. Tizzano, presentadas el 14 de noviembre de 2002, ECLI:EU:C:2002:662, apdos. 53 y 54).

circulación entre Estados miembros en cada una de las situaciones contempladas por la Directiva 95/46 sino que:

> "lo importante, para justificar el recurso a la base jurídica del artículo 100 A del Tratado, es que el acto adoptado sobre tal base tenga efectivamente por objeto la mejora de las condiciones de establecimiento y funcionamiento del mercado interior"[41].

De manera que la aplicabilidad de la Directiva 95/46 no podía depender de si una situación concreta estaba relacionada con la libre circulación de los trabajadores:

> "Una interpretación contraria podría hacer que los límites del ámbito de aplicación de la referida Directiva se vuelvan particularmente inciertos y aleatorios, lo que sería contrario al objetivo esencial de ésta, que es la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros con el fin de eliminar los obstáculos al funcionamiento del mercado interior derivados precisamente de las disparidades entre las legislaciones nacionales"[42].

No fue hasta el año 2008, en su sentencia *Promusicae*[43], cuando el TJUE reconoció explícitamente la existencia de un derecho a la protección de datos de carácter personal[44]. A partir de esa sentencia, el TJUE inició una nueva etapa en la que ha tenido que ponderar el derecho a la protección de los datos de carácter personal con otros derechos fundamentales como el derecho al acceso a documentos, a la propiedad intelectual o el derecho a la libertad de expresión o de información.

Así, a pesar de que para algunos autores la decisión ponía en peligro el principio de transparencia[45], en el asunto *Bavarian Lager*[46] el TJ priorizó al derecho de protección de datos frente al derecho de acceso a documentos. El TJUE debía conocer del recurso de casación planteado contra una resolución del TPI que anulaba una Decisión denegatoria de acceso a un documento relativo a una reunión celebrada en el marco de un procedimiento por incumplimiento de la Comisión. Mientras que el TPI había considerado que la divulgación de la composición de un comité de evaluación no podía causar un perjuicio concreto y efectivo a la protección de la vida privada de las personas interesadas[47], por su parte, el TJUE concluyó que ante una solicitud para la obtención de documentos que contienen datos personales, el Reglamento 45/2001 debía aplicarse en su totalidad de manera que la Comisión había actuado diligentemente al excluir los nombres de los miembros del comité evaluador que no habían consentido en la difusión de sus datos personales.

Asimismo, en los asuntos *Satamedia*[48] y *Google Spain*[49], el TJUE priorizó nuevamente el derecho a la protección de los datos de carácter personal frente a la libertad de expresión o el derecho a informar. En ambos casos, el TJUE tuvo que evaluar si la divulgación de ciertas informaciones publicadas previamente por terceros ajenos a esa información constituía una forma de tratamiento de datos y por tanto entraban dentro del ámbito de aplicación de la Directiva 95/46[50].

---

[41] Apdo. 41 de la sentencia.
[42] Apdo. 42 de la sentencia.
[43] Sentencia de 29 de enero de 2008, C-275/06, ECLI:EU:C:2008:54.
[44] Aunque de manera tímida, en su sentencia el TJUE apuntaba que "el art. 8 de CDFUE proclamaba expresamente el derecho a la protección de los datos personales". No obstante, en el resto de la sentencia el TJUE volvía a referirse al derecho al respeto de la intimidad.
[45] Para ANDRÉS SÁENZ DE SANTA MARÍA el resultado de la sentencia *Bavarian Lager* estaba demasiado escorado y alimentaba "los temores relativos a los efectos negativos que una interpretación excesivamente restrictiva de las normas sobre protección de los datos personales puede tener sobre el principio de transparencia". Para esta autora, "la búsqueda de la ponderación a través de un test de proporcionalidad hubiera permitido un equilibrio más ajustado", ANDRES SÁENZ DE SANTA MARÍA, P., "Acceso a los documentos y protección de datos personales en la Unión Europea: una conciliación difícil", AZNAR GÓMEZ, M., *Estudios de Derecho Internacional y Derecho europeo en homenaje al profesor Manuel Pérez González*, Tomo II, Tirant lo Blanch, p. 1376. En este mismo sentido, KRANENBORG, H., "Access to documents and data protection in the European Union: On the public nature of personal data", *CMLRev*, nº 45, 2008, p. 1090.
[46] Sentencia de 29 de junio de 2010, C-28/08 P, ECLI:EU:C:2010:378.
[47] EL TPI consideraba que los miembros del comité de evaluación habían sido nombrados en calidad de representantes de los servicios interesados y no a título personal.
[48] Sentencia de 16 de diciembre de 2008, C-73/07, ECLI:EU:C:2008:727.
[49] Sentencia de 13 de mayo de 2014, C-131/12, ECLI:EU:C:2014:317.
[50] Como motores de búsqueda, la actividad desarrollada por Google Spain y Google Inc consistía en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado. Por su parte Satamedia, había establecido un servicio de mensajes a través del cual lo usuarios podían acceder la información fiscal de determinados particulares previamente publicada

En ambos casos, el TJUE recordó que en cuanto que la información divulgada versaba sobre una persona física identificada o identificable, resultaba claro que la actividad desarrollada por el motor de búsqueda y por el servicio de mensajería estaba comprendida en la definición de tratamiento de datos. De este modo, tal como señalara JOZWIAK,

> "it is concluded that the default solution adopted in the Directive, aimed at subjecting certain communication to the special data protection regime, is now perpetuated at an even larger scale through the judicial interpretation of the Directive. The more data is shared, the more risks it brings about from the perspective of the CJEU and such inherent risks seem to justify the emphasis placed on the data protection side of the scale"[51].

Por su parte, los asuntos *Scarlet Extended*[52] y *SABAM*[53] tuvieron como resultado la prevalencia del derecho a la protección de los datos personales frente al derecho a la propiedad intelectual. En ambos asuntos el TJUE debía examinar si el establecimiento de sistemas de filtrado para la salvaguarda de la propiedad intelectual contravenía el derecho a la protección de los datos personales de los usuarios y tiene interés señalar que el Tribunal reformuló las cuestiones planteadas por el órgano remitente de manera que los casos se analizaron partiendo de la existencia de un derecho fundamental a la protección de los datos personales y no del art. 8 del CEDH.

El Tribunal señaló que el establecimiento de dichos sistemas implicaría la identificación, el análisis sistemático y el tratamiento de la información relativa a los perfiles creados en la red social por los clientes de ésta, dándose la circunstancia de que las informaciones relativas a esos perfiles eran datos protegidos de carácter personal, ya que permitían identificar a los clientes. El TJUE terminó concluyendo que un requerimiento judicial obligando al prestador de servicios de almacenamiento y a los proveedores de acceso a Internet a establecer el sistema de filtrado controvertido, no respetaría el requisito de garantizar un justo equilibrio entre, por un lado, el derecho de propiedad intelectual y, por otro, la libertad de empresa, el derecho a la protección de datos de carácter personal y la libertad de recibir o comunicar informaciones[54].

Recientemente, el TJUE ha vuelto a ampliar el ámbito de aplicación de la Directiva 95/46 en el asunto *Jehovan todistajat*[55], señalando que los tratamientos de datos personales que se efectúan durante la predicación puerta a puerta que realiza la comunidad religiosa de los Testigos de Jehová deben respetar la normativa de la Unión en materia de protección de datos personales.

En este caso el TJ debía examinar si el hecho de que la actividad de predicación quedase protegida por el derecho fundamental a la libertad de conciencia y de religión, consagrado en el artículo 10, apartado 1, de la Carta de los Derechos Fundamentales dotaba a la misma de carácter "exclusivamente personal o doméstico". Sin embargo, el Tribunal ha vuelto a priorizar el derecho a la protección de datos y ha descartado que la actividad de predicación esté comprendida entre las excepciones previstas en la normativa de la Unión de protección de datos.

De este modo, tal como señalara PEERS, esta nueva sentencia es coherente con la amplia interpretación del alcance de la legislación de protección de datos de la UE que el Tribunal de Justicia ha venido

---

en el periódico Veropörssi. En concreto el diario Veropörssi publica cada año el nombre y apellido de alrededor de 1.200.000 personas físicas cuyos ingresos superan determinados umbrales, los datos relativos a las rentas derivadas de sus rendimientos del trabajo y del capital, así como indicaciones relativas a la imposición de su patrimonio.

[51] JOZWIAK, M., "Balancing the Rights to Data Protection and Freedom of Expression and Information by the Court of Justice of the European Union: The Vulnerability of Rights in an Online Context", *MJ*, nº 3, 2016. Sobre estos dos asuntos véase también GÖMANN, M., "The new territorial scope of EU data protection law: Deconstructing a revolutionary achievement", *CMLRev*, nº 54, 2017, pp. 567-590; DE HERT, P. y PAPAKONSTANTINOU, V., "Google Spain:Addressing Critiques and Misunderstanding One Year Later", *MJ*, nº 22, pp. 624-638; HINS, W. "Case C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, judgment of the Grand Chamber of 16 December 2008", *CMLRev*, nº 47, pp. 215-237 y KUNER, C. B., "Google Spain in the EU and international context", *MJ*, nº 22, 2015, pp. 158-164.

[52] Sentencia de 24 de noviembre de 2011, C-70/10, ECLI:EU:C:2011:771.

[53] Sentencia de 16 de febrero de 2012, C-360/10, ECLI:EU:C:2012:85.

[54] Apartado 51 de la sentencia SABAM. En este sentido, GONZALEZ FUSTER, G., "Equilibrio entre propiedad intelectual y protección de datos: el peso oscilante de un nuevo derecho", *Revista de internet, Derecho y Política*, nº 14, 2012, pp. 47-60.

[55] Sentencia de 10 de julio de 2018, C-25/17, ECLI:EU:C:2018:551.

haciendo hasta ahora[56]. No obstante, para PEERS la sentencia *Jehovan todistajat*; complicará la labor de los "llamadores de puerta", sean del tipo que sea:

> "they must be aware not only of the inspiring words of Jesus Christ or Jeremy Corbyn, but also the infinitely drier text of the GDPR, a prospect which surely enthuses not the many, but the (very, very) few"[57].

2. El concepto de dato personal en la jurisprudencia del TJUE

Junto a las aportaciones anteriores, el TJUE se ha pronunciado también sobre el concepto de dato personal. En esta tarea, el Tribunal no sólo ha tenido que adaptar su jurisprudencia a los cambios normativos, también ha tenido que adaptar sus respuestas a la evolución tecnológica y mediática acontecida. El desarrollo de los medios de comunicación ha obligado al TJUE a adaptar el concepto de dato personal a las necesidades del momento, de manera que más allá del nombre, apellidos o número de identificación personal, el concepto reconociera otras realidades emergentes.

2.1 Una jurisprudencia evolutiva, con luces y sombras

Desde el asunto *Lindqvist*[58], el TJ había venido señalando la necesidad de dar una interpretación amplia al concepto de datos personales. En su sentencia de 6 de noviembre de 2003, el TJUE señaló que el concepto de dato personal incluía, "sin duda", el nombre de una persona junto a su número de teléfono o a otra información relativa a sus condiciones de trabajo o a sus aficiones y que la indicación de que una persona se hubiese lesionado un pie y estuviera en situación de baja parcial constituía un dato personal relativo a la salud[59]. A partir de entonces el TJ ha reiterado en todos sus pronunciamientos que cualquier información sobre una persona identificada o identificable constituiría un dato personal en el sentido del art. 2, letra a) de la Directiva[60].

Con todo, sería en el ya comentado asunto *Scarlet Extended*[61] en el que por primera vez el Tribunal de Justicia tendría que hacer frente a los nuevos avances tecnológicos. En este caso, estaba llamado a pronunciarse sobre la viabilidad, desde el punto de vista del Derecho de la Unión, de determinadas

---

[56] PEERS, S., "Is Data Protection Coming Home? The CJEU on data protection law and Jehovah's Witnesses – and political canvassing?", *EU Law Analysis: Expert insight into EU law developments*, http://eulawanalysis.blogspot.com/2018/07/is-data-protection-coming-home-cjeu-on.html (visitado por última vez el 17 de octubre de 2018). En este mismo sentido, GONZALO DOMENECH, J. J. y ORTEGA GIMENEZ, A., "¿Deben los Testigos de Jehová cumplir las normas establecidas por el Derecho de la Unión Europea en materia de Protección de Datos Personales?", *Diario La Ley*, nº 9274, 2018.

[57] PEERS, S., *op. cit.*

[58] Sentencia de 6 de noviembre de 2003, C-101/01, ECLI:EU:C:2003:596. El TJUE daba respuesta a las cuestiones planteadas por el Göta hovrätt de Suecia. En este caso las cuestiones se habían suscitado en el marco de un proceso penal seguido ante dicho órgano jurisdiccional contra la Sra. Lindqvist, acusada de haber infringido la normativa sueca relativa a la protección de datos personales al publicar en su sitio Internet diversos datos de carácter personal sobre varias personas que, como ella, colaboraban voluntariamente con una parroquia de la Iglesia protestante de Suecia. Mediante la primera de sus cuestiones, el órgano jurisdiccional remitente preguntaba si la conducta que consistía en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones constituía un "tratamiento total o parcialmente automatizado de datos personales". El TJUE determinó que el "tratamiento" de datos comprendía "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales", entre las que figuraba la comunicación por transmisión, la difusión o cualquier otra forma que facilite el acceso a los datos, de manera que la conducta consistente en hacer referencia, en una página web, a datos personales debía considerarse un tratamiento de esta índole.

[59] "Teniendo en cuenta el objeto de esta Directiva, es preciso dar una interpretación amplia a la expresión «datos relativos a la salud», empleada en su artículo 8, apartado 1, de modo que comprenda la información relativa a todos los aspectos, tanto físicos como psíquicos, de la salud de una persona" (apdo. 50 de la sentencia).

[60] Véanse entre otras, las sentencias de 20 de mayo de 2003, Österreichischer Rundfunk y otros, ya citada, apdo. 64; sentencia de 16 de diciembre de 2008, Huber, C-524/06, ECLI:EU:C:2008:724, apdo. 43 y sentencia de 7 de mayo de 2009, Rijkeboer, C-553/07, ECLI:EU:C:2009:293, apdo. 42.

[61] Sentencia de 24 de noviembre de 2011, ya citada.

medidas técnicas de lucha contra el pirateo[62]. El TJUE debía examinar si un tribunal nacional podía ordenar a un proveedor de acceso a Internet que estableciera un sistema de filtrado y de bloqueo de las comunicaciones electrónicas o si por el contrario tal medida suponía una vulneración de las disposiciones del Derecho de la Unión sobre la protección de datos de carácter personal y la confidencialidad de las comunicaciones.

Empero, tal como señalara el Abogado General, evaluar la incidencia concreta de un sistema de filtrado y de bloqueo sobre el derecho a la protección de los datos personales entrañaba la dificultad de determinar si las direcciones IP constituían datos personales, puesto que hasta ese momento, el TJ sólo había tenido que conocer de asuntos en los que se cuestionaban datos nominativos vinculados a las direcciones IP[63].

El Abogado General CRUZ VILLALÓN consideraba que en la medida en que una Dirección IP podía permitir la identificación de una persona, por referencia a un número de identificación o a cualquier otro dato propio de una persona, debía ser calificada de dato de carácter personal[64]. Siguiendo su opinión[65], en su sentencia de 24 de noviembre de 2011 el TJUE declaró que las direcciones IP constituían datos protegidos de carácter personal, de manera que el establecimiento de un sistema de filtrado afectaría al derecho de los clientes a la protección de sus datos personales, al tiempo que supondría una limitación de su libertad para recibir o comunicar informaciones[66].

De esta forma, tras la sentencia *Promusicae*, el Abogado General y el TJUE no solo volvían a proclamar la existencia de un derecho a la protección de los datos de carácter personal sino que aseveraban que los sistemas de filtrado constituían -más allá de la vulneración de la intimidad de los usuarios- una transgresión del derecho a la protección de datos de carácter personal. Para GONZÁLEZ FUSTER, la sentencia *Scarlet* suponía, por fin, la priorización del derecho a la protección de los datos personales frente al derecho a la vida privada del art. 8 del CEDH[67]:

Cuatro años más tarde, en el asunto *Breyer*[68], el TJUE tendría ocasión de analizar si las direcciones IP dinámicas, aquellas asignadas de manera temporal por los proveedores de acceso a la red a sus clientes, seguían constituyendo un dato personal cuando el encargado de almacenarlas, en este caso el titular de un sitio web, no disponía de los datos adicionales necesarios para la identificación del usuario concreto, sino que estaban en posesión de un tercero[69].

---

[62] Hasta ese momento, el Tribunal de Justicia sólo había tenido que conocer casos en los que se cuestionaban datos nominativos vinculados a direcciones IP y no había tenido nunca ocasión de examinar si una dirección IP podía considerarse, en cuanto tal, un dato personal.

[63] Conclusiones del Abogado General P. Cruz Villalón, presentadas el 14 de abril de 2011, ECLI:EU:C:2011:255, apdo. 74.

[64] Para el Abogado General, la consideración de las direcciones IP como datos personales era consecuencia necesaria del artículo 5 de la Directiva 2006/24/CE, que imponía a los proveedores de acceso a Internet, entre otras obligaciones, la de conservar, con fines de investigación, detección y sanción de las infracciones graves, cierto número de datos, entre los que se encontraba el nombre y la dirección del abonado o usuario registrado, la fecha y hora de la conexión y desconexión del servicio de acceso a Internet, así como la dirección IP dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación (apdos. 77 y 78 de las conclusiones).

[65] En sus conclusiones, para apoyar la calificación de las direcciones IP de datos personales a los efectos de la Directiva 95/46, el Abogado General traía a colación diferentes dictámenes, del Supervisor Europeo de Protección de Datos y del denominado "Grupo de trabajo del "artículo 29", que apoyaban la idea de que las direcciones IP debían ser consideradas como datos personales: "el Supervisor Europeo de Protección de Datos tuvo ocasión de indicar que la supervisión del comportamiento de los usuarios de Internet y la recopilación de sus direcciones IP equivale a una injerencia en su derecho a que se respeten su vida privada y su correspondencia. El Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, creado por la Directiva 95/46, considera igualmente que las direcciones IP constituyen, sin ningún género de dudas, datos de carácter personal en el sentido del artículo 2, letra a), de dicha Directiva" (apdo. 76).

[66] Apdo. 51 de la sentencia. En este sentido, ORDOÑEZ SOLIS, D., "Comentario de jurisprudencia reciente del Tribunal de Justicia de la Unión Europea", Cuadernos Europeos de Deusto, nº 46, 2012, pp. 189-190.

[67] GONZALEZ FUSTER, G., *op. cit.*, p. 58.

[68] Sentencia de 19 de octubre de 2016, Breyer, C-582/14, ECLI:EU:C:2016:779.

[69] Para prevenir ataques y posibilitar la persecución penal de los agresores, la mayor parte de los portales de internet de las instituciones alemanas almacenaban todos los accesos en ficheros o registros de protocolo. En ellos conservaban, incluso después de acabada la operación, el nombre del fichero o de la página solicitados, los conceptos introducidos en los campos de búsqueda, el momento de la llamada, la cantidad de datos transmitidos, la constatación del éxito de la llamada y la dirección IP del ordenador desde el que se ha hecho.

La controversia en cuestión había surgido como consecuencia de que el Sr. Breyer hubiese instado contra la República Federal de Alemania una acción de cesación por el registro de direcciones IP. El Sr. Breyer había consultado varios portales de internet de instituciones alemanas y solicitaba en su demanda que la República Federal fuera condenada a poner fin al registro de las direcciones IP[70].

A diferencia del asunto *Scarlet Extended*, tal como señaló el Abogado General CAMPOS SÁNCHEZ-BORDONA, el TJUE debía dilucidar si las direcciones IP eran datos protegidos de carácter personal, en un contexto en el que la recogida y la identificación de las direcciones IP no las realizaba el proveedor de acceso a la red, sino un proveedor de contenidos[71].

Para el Gobierno alemán, la pregunta merecía una respuesta negativa. A su juicio, las direcciones IP dinámicas no revelarían a una persona identificada, en el sentido del artículo 2[72]. El Gobierno alemán entendía que el concepto de datos de carácter personal, en el sentido del artículo 2, letra a), de la Directiva 95/46, debía interpretarse a la luz de la finalidad de la Directiva, esto es, garantizar el respeto de los derechos fundamentales. La necesidad de protección de las personas físicas podría verse de manera diferente en función de quién posea los datos y de si dispone, o no, de los medios para servirse de ellos a efectos de identificarlas:

> "El Sr. Breyer no es identificable a partir de las direcciones IP combinadas con los otros datos que conservan los proveedores de contenidos. Para eso se habría de manejar la información que poseen los proveedores de acceso a Internet, quienes, en ausencia de base legal, no pueden facilitarla a los proveedores de contenidos"[73].

La Comisión y los gobiernos austriaco y portugués se inclinaban, por el contrario, por una respuesta afirmativa[74]. Apoyándose en la solución adoptada por el Tribunal de Justicia en el asunto *Scarlet Extended*, la Comisión señaló que puesto que almacenar las direcciones IP servía para identificar a los usuarios en caso de ataques cibernéticos, el empleo de los datos suplementarios que registran los proveedores de acceso a Internet supondría un medio que podría ser utilizado "razonablemente", en el sentido del considerando 26 de la Directiva 95/46. En definitiva, a juicio de la Comisión, tanto el objetivo perseguido por la Directiva como los artículos 7 y 8 de la Carta de los derechos fundamentales de la Unión Europea militaban en favor de una interpretación amplia del artículo 2, letra a), de la Directiva 95/46.[75]

El Sr. Breyer alegaba que eran datos de carácter personal incluso aquellos cuya combinación era únicamente posible desde el punto de vista teórico, es decir, partiendo de la base de un peligro potencial abstracto, importando poco si en la práctica esa combinación se llevaba en efecto a cabo. A su juicio, que

---

[70] A pesar de que la demanda del Sr. Breyer había sido desestimada en primera instancia, su recurso de apelación, sin embargo, fue estimado parcialmente, condenándose a la República Federal a cesar en el registro más allá del término de cada operación de acceso. La orden de cese se condicionó a que el demandante facilitara, durante la operación de acceso, sus datos personales, incluso en forma de dirección de correo electrónico, y a que el registro no fuera imprescindible para restablecer la disponibilidad del servicio de telecomunicación. No obstante, interpuesto recurso de casación por ambas partes, la Sala VI del Bundesgerichtshof (Tribunal Supremo Civil y Penal de Alemania) preguntó al TJUE si el artículo 2, letra a), de la Directiva 95/46/CE debía interpretarse en el sentido de que una dirección de protocolo de Internet (dirección IP) almacenada por un prestador de servicios en relación con un acceso a su página web constituía para este un dato personal desde el momento en que un tercero (en este caso, un proveedor de acceso) dispusiera de los datos adicionales que permitían identificar al interesado.

[71] Conclusiones del Abogado General M. Campos Sánchez Bordona, presentadas el 12 de mayo de 2016, apdo. 63.

[72] Para decidir si informan sobre una persona «identificable», en el sentido de ese mismo precepto, el examen de la identificabilidad debe realizarse con un criterio «relativo». Así se desprende, a su juicio, del considerando 26 de la Directiva 95/46, según el cual únicamente han de tenerse en cuenta los medios susceptibles de ser «razonablemente» utilizados por el responsable del tratamiento, o por un tercero, para la identificación de una persona. Tal puntualización indicaría que el legislador de la Unión no ha querido incluir en el ámbito de aplicación de la Directiva 95/46 aquellas situaciones en las que una identificación es objetivamente posible por parte de cualquier tercero (apdos. 33 y 35 de las conclusiones).

[73] Así lo recoge el Abogado General en el apdo. 35 de sus conclusiones.

[74] Para el Gobierno austriaco, de acuerdo con el considerando 26 de la Directiva 95/46, para que una persona fuera tenida por identificable no se precisaba que todos sus datos de identificación se encontrasen en manos de una sola entidad. Así, una dirección IP podría ser un dato de carácter personal si un tercero (como, por ejemplo, el proveedor de acceso a Internet) dispone de los medios para identificar al titular de esa dirección, sin desplegar esfuerzos desmedidos. A su vez, el Gobierno portugués estimaba que la dirección IP, en combinación con la fecha de la sesión de consulta, era un dato de carácter personal, en la medida en que podía conducir a la identificación del usuario por una entidad distinta de la que ha guardado la dirección IP (apdos. 36 y 37 de las conclusiones).

[75] Apdo. 38 de las conclusiones.

un organismo pudiera ser relativamente incapaz de identificar a una persona valiéndose de la dirección IP no significaba que no existiera un peligro para dicha persona[76].

De acuerdo con lo expuesto por el Abogado General, el TJUE consideró que el núcleo de la cuestión planteada se ceñía a resolver si era relevante, para calificar las direcciones IP dinámicas de datos personales, la circunstancia de que un tercero muy específico —el proveedor de acceso a Internet— dispusiera de datos adicionales que, combinados con esas direcciones, tenían aptitud para identificar al usuario que ha visitado una determinada página web.

En su sentencia de 19 de octubre de 2016, el TJUE señaló que a la luz del artículo 2, el uso por el legislador de la Unión del término "indirectamente" mostraba que, para calificar una información de dato personal, no era necesario que dicha información permitiera, por sí sola, identificar al interesado. El Tribunal recordó que el considerando 26 de la Directiva 95/46 enunciaba que, para determinar si una persona era identificable, había que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a dicha persona. De manera que en la medida en que el citado considerando hacía referencia a los medios que pudiesen ser razonablemente utilizados tanto por el responsable del tratamiento como por "cualquier otra persona", su tenor sugeriría que, para que un dato pudiera ser calificado de dato personal, no era necesario que toda la información debiera encontrarse en poder de una sola persona:

> "El hecho de que la información adicional necesaria para identificar al usuario de un sitio de Internet no esté en poder del proveedor de servicios de medios en línea, sino del proveedor de acceso a Internet de ese usuario, no parece que pueda excluir que las direcciones IP dinámicas registradas por el proveedor de servicios de medios en línea constituyan, para éste, datos personales en el sentido del artículo 2, letra a), de la Directiva 95/46"[77].

Al igual que el Abogado General, el TJUE consideró que la cuestión era determinar si la posibilidad de combinar una dirección IP dinámica con dicha información adicional en poder del proveedor de acceso a Internet constituía un medio que pudiese ser razonablemente utilizado para identificar al interesado[78]. El Tribunal recordó que existían vías legales que permitían al proveedor de servicios dirigirse, en particular en caso de ataques cibernéticos, a la autoridad competente a fin de que ésta llevara a cabo las actuaciones necesarias para obtener información del proveedor de acceso a Internet.

En consecuencia, el Tribunal concluyó que el artículo 2, letra a), de la Directiva 95/46 debía interpretarse en el sentido de que:

> "una dirección IP dinámica registrada por un proveedor de servicios de medios en línea con ocasión de la consulta por una persona de un sitio de Internet que ese proveedor hace accesible al público constituye respecto a dicho proveedor un dato personal, en el sentido de la citada disposición, cuando éste disponga de medios legales que le permitan identificar a la persona interesada gracias a la información adicional de que dispone el proveedor de acceso a Internet de dicha persona"[79].

Por otro lado, más allá de los medios tecnológicos, se ha planteado si el concepto de dato personal ha de extenderse a aspectos que sin ser estrictamente personales, comentan o valoran los datos o circunstancias personales de un individuo. En el asunto *YS y otros*[80] la Abogada General SHARPTON y el TJUE tuvieron ocasión de seguir profundizando en el análisis del concepto de dato personal.

En este caso, M y S nacionales de terceros países habían solicitado la residencia legal en los Países Bajos. A pesar de que la solicitud de YS fue desestimada y las de M y S sí fueron atendidas, todos ellos invocaron el Derecho de la Unión para obtener acceso a un documento –minuta- redactado por un funcionario de la autoridad competente (acta), que incluía un análisis jurídico en forma de recomendación interna sobre la concesión de la residencia. En concreto YS, M y S alegaban que el análisis jurídico constituía un dato personal, por lo que, en virtud del Derecho de la Unión, tenían derecho a acceder al acta.

El Rechtbank Middelburg (tribunal de Middelburg) y el Raad van State (Consejo de Estado), órganos jurisdiccionales encargados de resolver de los recursos planteados en sendos procedimientos decidieron interrogar al TJUE sobre la extensión del artículo 2, letra a), de la Directiva 95/46. Los órganos remitentes

---

[76] Apdo. 32 de las conclusiones.
[77] Apdo. 44 de la sentencia.
[78] Lo cual no sucedería cuando la identificación del interesado estuviese prohibida por la ley o fuese prácticamente irrealizable: "los medios de acceso razonables que menciona la Directiva 95/46 han de ser, por definición, medios lícitos" (apartado 73 de las conclusiones del Abogado General).
[79] Apdo. 49 de la sentencia.
[80] Sentencia de 17 de julio de 2014, C-141/12, ECLI:EU:C:2014:2081.

deseaban que el TJ concretara si el art. 2, letra a), de la Directiva 95/46 debía interpretarse en el sentido de que los datos relativos al solicitante del documento de residencia y el análisis jurídico incluidos en la minuta eran datos personales en el sentido de dicha disposición.

Tanto YS, M y S como los Gobiernos helénico, austriaco y portugués, así como la Comisión Europea estimaban que, dado que ese análisis jurídico se refería a una persona física concreta y se basaba en su situación y características individuales, estaba también comprendido en dicho concepto[81].

Para el TJUE, el que los datos relativos al solicitante del documento de residencia que figuraban en una minuta, como su nombre, fecha de nacimiento, nacionalidad, sexo, etnia, religión e idioma, eran una información que se refería a esa persona física y por tanto debían calificarse, en consecuencia, como datos personales, no planteaba dudas. Sí las suscitaba, en cambio, el análisis jurídico que figura en una minuta.

Empero, siguiendo la posición de la Abogada General[82], el TJUE consideró que el análisis jurídico del acta no constituía en sí mismo un dato de este tipo en el sentido del artículo 2, letra a), de la Directiva 95/46 porque:

> "tal análisis jurídico no es una información relativa al solicitante del documento de residencia, sino, todo lo más, siempre que no se limite a una interpretación meramente abstracta del Derecho, una información referida a la apreciación y a la aplicación, por la autoridad competente, de ese Derecho a la situación de ese solicitante, situación que se acredita, en particular, mediante los datos personales relativos a su persona con los que cuenta esa autoridad"[83].

Para el TJ, esta interpretación del concepto de datos personales no sólo resultaba del tenor del artículo 2, letra a), sino que venía también corroborada por el objetivo y la estructura de la Directiva:

> "Según el artículo 1 de esa Directiva, la misma tiene por objeto proteger las libertades y los derechos fundamentales de las personas físicas, y, en particular, su intimidad, en lo que respecta al tratamiento de los datos personales y permitir de este modo la libre circulación de esos datos entre los Estados miembros. Según el vigesimoquinto considerando de la Directiva 95/46, los principios de la protección de las personas físicas establecidos por la misma tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas que efectúen tratamientos relativos a dichas personas y, por otra parte, en los derechos otorgados a las

[81] El Gobierno griego y la Comisión precisaban, no obstante, que esto sólo valía para los análisis jurídicos que incluyeran información relativa a una persona física y no para los que incluyeran únicamente una interpretación jurídica abstracta, mientras, M y S estimaban que incluso tal interpretación abstracta entraba en el ámbito de aplicación de dicha disposición si era determinante para apreciar la solicitud del documento de residencia y se aplicaba al caso concreto del solicitante (apdo. 35 de la sentencia). Según los Gobiernos neerlandés, checo y francés, el análisis jurídico incluido en una minuta no estaba comprendido en el concepto de datos personales (apdo. 36 de la sentencia)

[82] Para la Abogada General "una persona tiene derecho a acceder a sus datos personales porque tiene un interés en proteger sus derechos y libertades fundamentales, en particular, su derecho a la intimidad, cuando los Estados miembros traten información que les afecte. Denegar el acceso a los datos personales tratados o a la información sobre dicho tratamiento privaría de eficacia a otras partes de la Directiva 95/46. Por ejemplo, podría hacer imposible comprobar si los datos personales están siendo tratados sólo en la medida necesaria para el cumplimiento de una misión de interés público en el ejercicio del poder público conferido al responsable del tratamiento, o bien conseguir la rectificación o supresión de los datos. En cambio, el análisis jurídico en sí no se inserta en la esfera del derecho de una persona física a la intimidad, por lo que no hay motivo para considerar que dicha persona sea la única habilitada para verificarla y rectificarla y para pedir que sea suprimida o bloqueada. Es la autoridad judicial independiente a quien compete revisar la decisión para la cual se redactó el análisis jurídico". Según la Abogada General, la Directiva no exigía a los Estados miembros conceder acceso a los análisis jurídicos cuando están incluidos en un documento interno, como el acta, que contenía datos personales, porque el análisis jurídico no constituiría en sí mismo un dato personal. Para SHARPTON, sólo la información relativa a hechos referidos a una persona física podría ser considerada como dato personal y un análisis jurídico sería sólo el razonamiento en que se basa la resolución de una cuestión de Derecho: "La propia resolución puede adoptar la forma de un asesoramiento, opinión o decisión (y puede ser jurídicamente vinculante o no). Aparte de los hechos en que se basa (algunos de los cuales pueden ser datos personales), dicho análisis contiene la explicación de la resolución. La explicación en sí no es información relativa a una persona identificada o identificable. A lo sumo, puede calificarse como información acerca de la interpretación y aplicación de la legislación pertinente en virtud de la cual se valora y (acaso) se decide la situación jurídica de una persona. Es muy posible que en el proceso que lleva a resolver la cuestión entren en consideración datos personales y otros elementos de hecho, pero eso no convierte el propio análisis jurídico en datos personales" (apdos. 59 y 60 de las conclusiones).

[83] Apdo. 40 de la sentencia.

personas cuyos datos sean objeto de tratamiento de ser informadas acerca de dicho tratamiento, de acceder a los datos, de solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias"[84].

El Tribunal consideró que los derechos del interesado a los que se refiere la Directiva 95/46, permiten que esa persona pueda cerciorarse de que sus datos personales son exactos y que son tratados lícitamente:

"Como resulta del cuadragésimo primer considerando de esta Directiva, para poder efectuar las comprobaciones necesarias, cualquier persona disfruta, en virtud de su artículo 12, letra a), del derecho de acceso a los datos que le conciernan y sean objeto de tratamiento. El citado derecho de acceso es indispensable, en particular, para permitir al interesado obtener, en su caso, del responsable del tratamiento de los datos, la rectificación, la supresión o el bloqueo de esos datos y, en consecuencia, ejercer el derecho que se contempla en el artículo 12, letra b), de dicha Directiva"[85].

Sin embargo, a diferencia de los datos relativos al solicitante del documento de residencia que figuraban en la minuta y que podían constituir la base fáctica del análisis jurídico incluido en dicha minuta, el TJUE recordó que el solicitante no podría verificar la exactitud del análisis en sí, por lo que extender el derecho de acceso del solicitante del documento de residencia a ese análisis jurídico no ayudaría, en realidad, al objetivo de la Directiva, consistente en garantizar la protección del derecho a la intimidad de ese solicitante en lo que respecta al tratamiento de sus datos, sino al objetivo de garantizarle un derecho de acceso a los documentos administrativos, que, sin embargo, la Directiva 95/46 no contempla[86].

Para BROUWER y BORGWSIUS, la interpretación del TJUE resultó decepcionante ya que en muchas circunstancias, el acceso a actas era necesario para el disfrute efectivo de los derechos de los solicitantes de asilo. En su opinión, este resultado no debía extrapolarse a otras circunstancias, ya que la sentencia se refería a preguntas específicas con respecto a los procedimientos de asilo:

"The judgment does not imply that data that relate to a person because of a 'result' should generally not be considered as personal data"[87].

2.2 El asunto Nowak: una nueva dimensión en el concepto de dato personal

Recientemente, el TJUE ha vuelto a matizar el concepto de dato personal. El asunto *Nowak*[88], de cierta similitud con el asunto *YS y otros*[89], ha hecho al TJUE replantearse la delimitación del mismo.

Mediante su cuestión prejudicial, el Tribunal Supremo irlandés solicitaba al TJUE que aclarara si la definición de dato personal incluía las respuestas escritas de un aspirante en un examen profesional[90],

---

[84] Apdos. 42 y 43 de la sentencia.
[85] Apdo. 44 de la sentencia.
[86] Apdos. 45 y 46 de la sentencia.
[87] BROUWER, E. y BORGWSIUS, F. Z., "Access to Personal Data and the Right to Good Governance during Asylum Procedures after the CJEU's YS. and M. and S. judgment (C-141/12 and C-372/12)", *European journal of migration and law*, vol. 17, nº. 2-3, 2015, p. 271.
[88] Sentencia de 20 de diciembre de 2017, C-434/16, ECLI:EU:C:2017:994.
[89] Así lo señala la Abogada General en sus conclusiones: "el presente asunto se asemeja a aquel en el que el Tribunal de Justicia denegó la extensión del derecho de acceso al borrador de análisis jurídico de una solicitud de asilo, puesto que no ayuda al objetivo de la Directiva de protección de datos, sino al objetivo de un derecho de acceso a los documentos administrativos. En el caso aquí analizado habría que considerar que el acceso a la información sobre la valoración de un examen escrito debería obtenerse preferentemente en el procedimiento de examen o en un procedimiento especial para reclamar contra las decisiones sobre el examen, y no con arreglo al Derecho de protección de datos. Asimismo, teniendo en cuenta que el procedimiento de examen no viene determinado por el Derecho de la Unión, cualquier posible derecho de información en este ámbito dependería únicamente del Derecho nacional. Además, en la citada sentencia, el Tribunal de Justicia decidió que un análisis jurídico de ese tipo no es una información relativa al solicitante del documento de residencia, sino, todo lo más, una información referida a la apreciación y la aplicación del Derecho, por parte de la autoridad competente, a la situación de ese solicitante. A primera vista, esta conclusión podría aplicarse también a los comentarios sobre la corrección, pues sólo mostrarían la valoración de las respuestas por parte del examinador" (apdos. 58 y 59).
[90] En el marco de un litigio entre el Sr. Peter Nowak y el Data Protection Commissioner (Comisario de Protección de Datos de Irlanda), en relación con la negativa de esa autoridad a permitir al Sr. Nowak el acceso al escrito corregido de un examen en el que éste participó como aspirante la Supreme Court de Irlanda planteó las siguientes cuestiones: "1) ¿La información contenida en las respuestas dadas por un

con la particularidad de que en el examen del candidato se incluían las respuestas del mismo con las valoraciones y correcciones del examinador, el TJUE debía valorar, una vez más, hasta dónde llegaba la extensión del concepto de dato personal[91].

En su Sentencia, el TJUE vuelve a recordar que el empleo de la expresión "toda información" en la definición del concepto de datos personales evidenciaba el objetivo del legislador de la Unión de atribuir a este concepto un significado muy amplio, que no se ceñiría exclusivamente a los datos confidenciales o relacionados con la intimidad, sino que podría abarcar todo género de información, tanto objetiva como subjetiva, en forma de opiniones o apreciaciones, siempre que fueran sobre la persona en cuestión. Requisito que se cumplirá cuando, debido a su contenido, finalidad o efectos, la información estuviera relacionada con una persona concreta.

En el caso particular del Sr. Nowak, en la línea de lo apuntado por los Gobiernos checo, helénico, húngaro, austríaco y portugués, así como por la Comisión Europea, el TJUE consideró que las respuestas escritas proporcionadas por un aspirante en un examen profesional eran datos relacionados con su persona. Para el Tribunal, el contenido de las respuestas revelaba el nivel de conocimientos y el grado de competencia del Sr. Nowak en un área determinada, así como, en su caso, el proceso de reflexión, el discernimiento y la capacidad de análisis del propio aspirante[92].

En cuanto a las anotaciones del examinador sobre las respuestas del aspirante, el TJUE señaló que, al igual que las respuestas proporcionadas durante el examen por el citado aspirante, eran datos que se refieren a este último. Por lo tanto, el contenido de esas anotaciones expresaba la opinión o valoración del examinador sobre los resultados individuales del aspirante en el examen y, en particular, sobre sus conocimientos y competencias en un área concreta:

> "Dichas anotaciones, por lo demás, tienen precisamente la finalidad de documentar la evaluación de los resultados del aspirante por parte del examinador, y pueden tener efectos para ese aspirante"[93].

De este modo, y esto es lo que le diferencia del asunto *YS*, el TJUE consideró que a diferencia del análisis jurídico que acompaña un documento administrativo, las observaciones o correcciones que formula un examinador, sí constituyen una información relativa al candidato y por tanto son un dato de carácter personal[94].

Por otro lado, el TJ concluye que el hecho de que las anotaciones del examinador también sean datos que concernieran al propio examinador, no puede afectar a su calificación como dato personal:

---

candidato durante un examen profesional constituye un dato personal en el sentido de la Directiva 95/46? 2) Si la respuesta a la primera cuestión es que dicha información puede constituir, en todo o en parte, un dato personal en el sentido de la Directiva 95/46, ¿qué factores han de tenerse en cuenta para determinar si, en un caso concreto, un examen escrito constituye un dato personal y qué importancia debe atribuirse a esos factores?"

[91] La Abogada General entendía igualmente que el TJUE tendría que clarificar si el hecho de que el examen fuera manuscrito resultaba relevante para su calificación como dato personal. Para la Abogada General un examen manuscrito es prácticamente una prueba caligráfica, que al menos potencialmente se podría utilizar en un momento posterior como indicio para investigar si otro texto se redactó también con la letra del candidato del examen y por lo tanto, puede proporcionar información sobre la identidad del autor del examen. La Abogada General puntualiza además que el que dicha prueba caligráfica fuera adecuada para identificar de forma certera al autor no impedía que fuera catalogada como datos personales, ya que muchos otros datos personales no permiten por sí solos la identificación inequívoca de las personas (conclusiones de la Abogada General J. Kokott, presentadas el 20 de julio de 2017, ECLI:EU:C:2017:582, apdos. 29 y 30). El TJUE, por su parte, se limitó a afirmar que si el examen está escrito a mano, las respuestas contienen, además, información caligráfica (apdo. 37 de la sentencia).

[92] Más aun cuando el objetivo de las respuestas era valorar la capacidad profesional del aspirante y su aptitud para ejercer un oficio en concreto. De hecho, la utilización de los referidos datos, que se manifiesta, en particular, en el éxito o el fracaso del aspirante en el examen en cuestión, puede tener efectos en sus derechos e intereses, ya que, por ejemplo, puede condicionar sus oportunidades de acceder a la profesión o empleo al que aspira o influir en esas oportunidades (apdos. 37 a 39 de la sentencia).

[93] Apdo. 43 de la sentencia.

[94] Las observaciones del examinador consistirían en la valoración de lo expuesto por el candidato en su hoja de examen y por tanto, supondrían un análisis de los conocimientos que el candidato posee sobre una determinada materia.

> "unos mismos datos pueden concernir a varias personas físicas y, por lo tanto, ser datos personales de cada una de éstas, en el sentido del artículo 2, letra a), de la Directiva 95/46, siempre que tales personas sean identificadas o identificables"[95].

Finalmente, advierte de que la calificación como datos de carácter personal no puede verse alterado por el hecho de que esa calificación permita al aspirante, ejercitar los derechos de acceso y rectificación, con arreglo a lo dispuesto en el artículo 12, letras a) y b), de la Directiva 95/46:

> "del vigesimoquinto considerando de la Directiva 95/46 se desprende que los principios de la protección que ésta contempla tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas que efectúen tratamientos —obligaciones relativas, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento— y, por otra parte, en los derechos otorgados a las personas cuyos datos sean objeto de tratamiento de ser informadas acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias. Por lo tanto, negar la calificación de «datos personales» a la información referente a un aspirante contenida en sus respuestas proporcionadas con ocasión de un examen profesional, y en las anotaciones del examinador en relación con aquellas, supondría —en lo que se refiere a ese tipo de información— eludir por completo la observancia de los principios y garantías en materia de protección de datos personales y, en particular, de los principios relativos a la calidad de los datos y a la legitimación para su tratamiento, establecidos en los artículo 6 y 7 de la Directiva 95/46, así como eludir el respeto a los derechos de acceso, rectificación y oposición de la persona concernida, establecidos en los artículos 12 y 14 de esta Directiva, y a las funciones de la autoridad de control de acuerdo con el artículo 28 de la Directiva"[96].

Por último, el TJUE puntualiza que los derechos de acceso y rectificación, no incluyen las preguntas del examen, que por su propia naturaleza no son datos personales del candidato[97].

---

[95] Apdo. 45 de la sentencia.
[96] Apdo. 48 de la sentencia.
[97] Sobre este aspecto, la Abogada General realiza un análisis más amplio: para KOKOTT la catalogación de la información como datos personales no puede depender de que existan regulaciones específicas sobre el acceso a dicha información. Del mismo modo, tampoco podrían resultar pertinentes para determinar si se consideran datos personales los problemas relacionados con el derecho de rectificación, puesto que si esos factores se tomasen en consideración de manera determinante, algunos datos personales podrían quedar excluidos del sistema integral de protección de la Directiva de protección de datos, a pesar de que las reglas aplicables en su lugar no garantizan una protección uniforme sino, a lo sumo, una de carácter fragmentario. En cuanto al derecho de acceso y la rectificación de los datos personales, KOKOTT señala que este derecho aplicado a un examen escrito no puede utilizarse para exigir, tras el acceso, la rectificación del contenido del examen, es decir, de la respuesta que el candidato del examen plasmó sobre el papel, de acuerdo con el artículo 12, letra b), de la Directiva de protección de datos: "La exactitud e integridad de los datos personales conforme al artículo 6, apartado 1, letra d), deben valorarse de acuerdo con la finalidad para la cual dichos datos fueron recogidos y son tratados. La finalidad de un examen escrito es determinar los conocimientos y las aptitudes del candidato del examen en el momento en que se lleva a cabo, lo cual se desprende precisamente de sus resultados y en concreto de las faltas cometidas. Por lo tanto, los errores en la respuesta no significan que los datos personales materializados en el examen sean erróneos". Sin embargo, para la Abogada General, sí cabría una rectificación si se demostrara que el examen no documenta de manera exacta o completa el resultado del interesado. Este sería el caso por ejemplo, "si se hubiera atribuido al interesado el examen de otro candidato, lo cual se podría demostrar, por ejemplo, mediante la caligrafía, o si se hubieran perdido partes del examen". Por lo demás, no puede descartarse que un candidato del examen tuviera posteriormente un interés legítimo en que se supriman los datos personales que se materializan en el examen, de acuerdo con el artículo 12, letra b), de la Directiva de protección de datos, es decir, que se destruya el examen. Dicho interés puede suponerse a más tardar cuando el examen haya perdido cualquier valor probatorio relacionado con el control de los resultados por el vencimiento de los plazos. Pero ese derecho de supresión también implica el reconocimiento de la materialización de datos personales en el examen. Para la Abogada General la rectificación y los demás derechos que reconoce el artículo 12, letra b), de la Directiva, la supresión y el bloqueo, no son la única finalidad del derecho de acceso: "Si bien el considerando 41 describe como finalidad del acceso que el interesado pueda cerciorarse, en particular, de la exactitud de dichos datos y de la licitud de su tratamiento, al utilizar la expresión «en particular» en la mayoría de las lenguas, el legislador ha querido señalar que la finalidad es más amplia. De hecho, más allá de la rectificación, la supresión o el bloqueo, los interesados tienen generalmente un interés legítimo en averiguar la información sobre ellos que está siendo objeto de tratamiento por el responsable" (apdos. 34, 35, 36 y 95 de las conclusiones).

Por su parte, KOKOTT considera que aunque la necesidad de información que pueda tener un candidato sobre su examen pueda ser, en un primer momento muy limitada, al poder recordar relativamente bien el contenido de sus respuestas, pasados unos años, lo recordado será mucho más vago, por lo que una eventual solicitud de acceso se deberá a una necesidad real de información, con independencia de los motivos[98].

Tal como señalara EL BERHOUMI, la sentencia *Nowak* confirma la tendencia del Tribunal de Justicia a interpretar ampliamente la noción de dato personal. No obstante, sí resulta novedosa para los ámbitos de la educación o de la formación profesional donde el derecho a consultar los exámenes suele partir de otros fundamentos:

> "Là où l'arrêt se révèle davantage innovant, à tel point que ses implications pourraient être importantes, c'est que le raisonnement de la Cour se rapporte à une problématique jusque-là largement étrangère aux enjeux du traitement des données à caractère personnel. En effet, dans la matière de la formation professionnelle, mais aussi dans celle de l'enseignement tout autant concernée par cet arrêt, le droit à la consultation de copies d'examen là où il est reconnu repose sur d'autres fondements, singulièrement le droit d'accès aux documents administratifs"[99].

Por otra parte, las aportaciones de esta Sentencia no se agotan en el caso concreto; como apuntó la Abogada General, aunque la Directiva de protección de datos es sustituida por el Reglamento (UE) 2016/679, "la definición de datos personales no resulta afectada. Por lo tanto también resulta relevante para la aplicación futura del Derecho de la Unión en materia de protección de datos"[100].

III. EL CONCEPTO DE DATO PERSONAL EN EL REGLAMENTO (UE) 2016/679

Como ya señaláramos, tras años de debate sobre la necesidad de adaptar la normativa de la UE en materia de protección de datos a los nuevos tiempos tecnológicos y jurídicos, en abril de 2016, se aprobó el esperado Reglamento general de protección de datos (RGPD), que forma parte del paquete de reformas de la UE sobre la protección de datos, junto con la Directiva sobre protección de datos para las autoridades policiales y de justicia[101].

Sin suscitar apenas discusión sobre su contenido a lo largo del procedimiento legislativo[102], el nuevo artículo 4 del Reglamento recoge las diferentes definiciones de los términos utilizados en el Reglamento. Tal como señalara la propia Comisión en su propuesta de Reglamento, algunas de las definiciones contenidas en el nuevo artículo 4 del Reglamento proceden de la Directiva 95/46/CE y "otras se modifican, complementadas con elementos adicionales"; este sería precisamente el caso del concepto de dato personal, pese a que la propuesta de la Comisión incluía una escueta definición de dato personal:

---

[98] Por otra parte, KOKOTT también considera que con el transcurso del tiempo —en especial, una vez transcurridos los posibles plazos de reclamación y revisión— aumenta la inseguridad de si se conservará aún el examen y en esta situación, el candidato del examen debe poder averiguar, al menos, si su examen aún se conserva (apdo. 41 de las conclusiones).

[99] El BERHOUMI, M., "Arrêt Nowak: les copies d'examen, nouveau terrain de la protection des donnes personnelles", *Journal de droit européen*, nº 247, 2018, p. 90. En este mismo sentido, GARDETTE, J. M., "Précisions sur la protection des données à caractère personnel dans le cadre des examens", *Revue des affaires europeennes*, nº 4, 2017, p. 739-745 y PEERS, S., "Privacy and data protection in universities: recent ECJ and ECtHR rulings", *EU Law Analysis: Expert insight into EU law developments*, http://eulawanalysis.blogspot.com/2017/12/privacy-and-data-protection-in.html (visitado por última vez el 17 de octubre de 2018).

[100] Apdo. 3 de las conclusiones.

[101] Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, *DOUE* nº L 119 de 4 de mayo 2016.

[102] Ni el Comité Económico y Social Europeo ni el Comité de las Regiones hicieron ninguna observación sobre la definición de dato personal incluida en la Propuesta de Reglamento de la Comisión. En su Dictamen de 10 de octubre de 2012, el CR ni siquiera hace mención a la propuesta de art. 4 (Dictamen del Comité de las Regiones sobre el Paquete sobre la protección de datos, *DOUE* nº C 391, de 18 de diciembre de 2012). Por su parte el CESE, en su Dictamen de 23 de mayo de 2012 realiza varias observaciones particulares sobre los conceptos de "consentimiento" o "transferencia de datos", pero no hace ninguna observación sobre el concepto de dato personal (Dictamen del Comité Económico y Social Europeo sobre la «Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)», COM(2012) 11 final — 2012/011 (COD), *DOUE* nº C 229, de 31 de julio 2012).

"'personal data' means any information relating to a data subject"[103]. Sin embargo, en su posición aprobada en primera lectura, el Parlamento Europeo presentó una enmienda al art. 4 del Reglamento que reformulaba la definición de dato personal y que sería la finalmente adoptada casi en los mismos términos[104].

En consecuencia, el nuevo Reglamento ha actualizado la definición de dato personal. A los ya considerados como datos especialmente protegidos como eran la ideología, la religión, la afiliación sindical, las creencias, la salud, el origen racial o la vida sexual, se añaden los datos genéticos y biométricos dirigidos a identificar de manera inequívoca a una persona:

> "A efectos del presente Reglamento se entenderá por: 1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona"[105]

El Reglamento adapta el concepto a las nuevas formas desarrolladas por la tecnología que nos permiten llegar a identificar fácilmente a una persona. Si la Directiva definía como persona identificable a aquella cuya identidad pudiese determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social y limitaba su extensión señalando que no se consideraría identificable si dicha identificación requería plazos o actividades desproporcionados, el nuevo Reglamento añade también la posibilidad de que la persona pueda ser identificada mediante un identificador en línea.

De este modo, el concepto de dato personal se adapta a los nuevos tiempos[106], recogiendo la jurisprudencia del TJUE desarrollada en los últimos años[107] y siguiendo lo dispuesto por el Grupo de Trabajo del art. 29 en su Dictamen sobre el concepto de datos personales:

> "Si bien la identificación a través del nombre y apellidos es en la práctica lo más habitual, esa información puede no ser necesaria en todos los casos para identificar a una persona. Así puede suceder cuando se utilizan otros «identificadores» para singularizar a alguien. Efectivamente, los ficheros informatizados de datos personales suelen asignar un identificador único a las personas registradas para evitar toda confusión entre dos personas incluidas en el fichero. También en Internet, las herramientas de control de tráfico permiten identificar con facilidad el comportamiento de una máquina y, por tanto, la del usuario que se encuentra detrás. Así pues, se unen las diferentes piezas que componen la personalidad del individuo con el fin de atribuirle determinadas decisiones. Sin ni siquiera solicitar el nombre y la dirección de la persona es posible incluirla en una categoría, sobre la base de criterios socioeconómicos, psicológicos, filosóficos o de otro tipo, y atribuirle determinadas decisiones puesto que el punto de contacto del individuo (un ordenador) hace innecesario conocer su identidad en sentido estricto. En otras palabras, la posibilidad de identificar a una persona ya no equivale necesariamente a la capacidad de poder llegar a conocer su nombre y apellidos"[108].

---

[103] COM(2012)0011.

[104] Según el Parlamento: "«datos personales»: toda información relativa a una persona física identificada o identificable («el interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador único o uno o varios elementos específicos, característicos de la identidad física, fisiológica, genética, psíquica, económica, cultural, social o de género de dicha persona". En su enmienda el Parlamento incluía el género como ejemplo de identificador (P7_TC1-COD(2012)0011, disponible en http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//ES ,(visitado por última vez el 17 de octubre de 2018)

[105] Art. 4.1 del nuevo Reglamento.

[106] ARIAS POU, M., "VIII. Definiciones a efectos del Reglamento General de Protección de datos" en PIÑAR MAÑAS, J. L. (dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Editorial Reus, 2016, pp. 117-118.

[107] Al inicio de sus conclusiones para el asunto *Nowak*, la Abogada General KOKOTT señalaba que "si bien la Directiva de protección de datos sería sustituida próximamente por el Reglamento general de protección de datos, "la definición de datos personales no resulta afectada". No obstante, creemos que la Abogada General quería decir que el concepto contenido en la Directiva ya había sido previamente actualizado por el TJUE y que las novedades introducidas por el Reglamento al respecto no iban a provocar un cambio jurisprudencial.

[108] Dictamen 4/2007 del Grupo de trabajo del artículo 29 sobre el concepto de datos personales, adoptado el 20 de junio de 2007, disponible en

El Considerando 26 del Reglamento completa la definición del artículo 4.1, señalando que la protección debe aplicarse también a aquellos datos seudonimizados que mediante la utilización de información adicional cabria atribuir a una persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, el Considerando 26 señala que deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.

En consecuencia, la protección de datos no se aplicará a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo.

Tal como señala la Comisión,

> "los datos personales son cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal. Los datos personales que hayan sido anonimizados, cifrados o presentados con un seudónimo, pero que puedan utilizarse para volver a identificar a una persona, siguen siendo datos personales y se inscriben en el ámbito de aplicación del RGPD"[109]

Por otro lado, el Reglamento protege los datos personales independientemente de la tecnología utilizada para su tratamiento, esto es, el Reglamento es "tecnológicamente neutro":

> "se aplica tanto al tratamiento automatizado como manual, siempre que los datos se organicen con arreglo a criterios predeterminados (como el orden alfabético). Asimismo, no importa cómo se conservan los datos; ya sea en un sistema informático, a través de videovigilancia o sobre papel; en todos estos casos, los datos personales están sujetos a los requisitos de protección establecidos en el RGPD"[110].

Con todo, hay que criticar que la definición de dato personal, decisivo para concretar el ámbito de aplicación material del Reglamento, se encuentre fragmentada entre el art. 4. 1) y el Considerando 26[111], pues dificulta la comprensión integral del concepto.

---

http://www.redipd.es/actividades/encuentros/VI/common/wp136_es.pdf (visitado por última vez el 18 de octubre de 2018). El Grupo de Trabajo se creó de conformidad con el art. 29 de la Directiva 95/46/CE, de ahí su nombre. Se trataba de un órgano consultivo independiente de la UE en materia de protección de datos e intimidad. Sus funciones se describían en el art. 30 de la Directiva 95/46/CE.

[109] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es (visitado por última vez el 17 de octubre de 2018). En sus Orientaciones sobre la aplicación del Reglamento general de protección de datos (COM(2018) 43 final), la Comisión ya había señalado que aunque el éxito del Reglamento dependía de la adecuada sensibilización de todos aquellos a quienes concernían las nuevas normas, todavía no existía entre los ciudadanos un nivel de sensibilización suficientemente generalizado sobre los cambios y las mejoras en los derechos que las nuevas normas de protección de datos traerán consigo. Para facilitar su entrada en vigor, la Comisión anunciaba que elaboraría una serie de materiales dirigidos a todos los agentes implicados en la protección de datos. Una vez que el Reglamento ha entrado en vigor, la Comisión ha elaborado unos documentos explicativos para acercar el nuevo Reglamento a la ciudadanía. Entre los materiales prácticos, la Comisión ha incluido una serie de preguntas y respuestas, seleccionadas en función de los comentarios recibidos por las partes interesadas, con ejemplos prácticos y enlaces a distintas fuentes de información. Entre ellos la Comisión ha incluido un apartado destinado a aclarar el concepto de datos personales. Asimismo, la institución comunitaria ha incluido un listado con ejemplos de datos personales y otro con ejemplos de lo que no son datos personales. En concreto la Comisión señala que el concepto de dato personal incluiría el nombre y apellidos, el domicilio, la dirección de correo electrónico, del tipo nombre.apellido@empresa.com, el número de documento nacional de identidad, los datos de localización (como la función de los datos de localización de un teléfono móvil), la dirección de protocolo de internet (IP), el identificador de una cookie, el identificador de la publicidad del teléfono o los datos en poder de un hospital o médico, que podrían ser un símbolo que identificara de forma única a una persona. Por el contrario, la Comisión señala que el número de registro mercantil, la dirección de correo electrónico, del tipo info@empresa.com o los datos anonimizados, no estarían incluidos en el concepto del art. 4.1 del Reglamento. Los diferentes materiales están disponibles en https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_es (visitado por última vez el 17 de octubre de 2018).

[110] *Ibid.*

[111] En su análisis de la Propuesta de Reglamento General de Protección de Datos, TRONCOSO REIGADA calificaba con razón a este enfoque como "mala técnica normativa" (TRONCOSO REIGADA, A., *op. cit.*, p. 75).

IV. CONCLUSIONES: REFORZANDO LA PROTECCIÓN FRENTE AL *BIG DATA*

En un mundo cada vez más globalizado en el que la magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa, alcanzando niveles desorbitantes, es indispensable que los ciudadanos podamos disponer de nuestra propia identidad, poniendo límites a la dispersión de nuestros datos personales y pudiendo acceder en todo momento a la información que nos concierna.

De manera acertada, en los últimos años, el TJUE ha ponderado el derecho a la protección de datos frente a otros derechos fundamentales, demostrando una especial sensibilidad en relación a la autodeterminación informativa.

Por otro lado, la rápida evolución tecnológica ha planteado nuevos retos para la protección de los datos personales. La tecnología ha transformado tanto la economía como la vida social, y ha facilitado aún más la libre circulación de datos personales dentro de la Unión y la transferencia incluso a terceros países. Con todo, la interpretación extensiva del concepto de dato personal, realizada por el TJUE, ha permitido adaptar la tutela del derecho a la protección de datos a las nuevas realidades tecnológicas. De este modo, el concepto de dato personal no solo atañe a las referencias estrictamente personales sino que abarca todo género de información, tanto objetiva como subjetiva, en forma de opiniones o apreciaciones, relativa a una persona identificable.

A pesar de su tardío reconocimiento, el derecho a la protección de datos cuenta desde el mes de mayo de 2018 de un único conjunto de normas aplicable en todo el territorio de la UE. De este modo, la adopción del nuevo Reglamento general de protección de datos supone, entre otras cosas, la adaptación del Derecho material a la ya existente realidad jurisprudencial.

Empero, el legislador ha adolecido de poca concreción a la hora de acotar el concepto de dato personal. Al segregar la noción de dato personal entre su articulado y sus considerandos, el nuevo Reglamento sufre de cierta dispersión conceptual, lo que puede resultar negativo a la hora de determinar su ámbito de aplicación.

Solo el transcurso del tiempo nos permitirá saber si el nuevo cuerpo normativo alcanza su objetivo primordial: garantizar un nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de sus datos equivalente en todos los Estados miembros. El próximo año ya tendremos ocasión de evaluar los primeros progresos en la protección unificada del derecho a la protección los datos personales porque al finalizar el primer semestre de 2019 la Comisión organizará un acto para hacer balance de las experiencias de las distintas partes interesadas por lo que respecta a la aplicación del Reglamento. Este balance se incorporará también al informe que la Comisión debe preparar para mayo de 2020 sobre la evaluación y revisión del Reglamento[112]. Sin duda, el TJUE tendrá también ocasiones para seguir contribuyendo a precisar los perfiles de un concepto en permanente expansión.

[112]Así lo indica la Comisión en sus Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018, de 24 de enero de 2018, COM(2018) 43 final, punto 4, apdo. g).