2017 - 05 - 08

Revista Aranzadi Unión Europea
2017
Número 1 (2017)
Doctrina
2. La protección de datos en la UE: recapitulación de novedades (PUERTO SOLAR CALVO)

2 La protección de datos en la UE: recapitulación de novedades

PUERTO SOLAR CALVO

Jurista de II.PP. especialista en protección de datos. DEA Derechos Fundamentales. Experto Universitario en Derecho UE

ISSN 1579-0452

Revista Aranzadi Unión Europea 1
Enero 2017

Sumario:

RESUMEN:

RESUMEN: Los últimos pronunciamientos del Tribunal de Justicia Europeo (TJUE) en supuestos relativos a la protección de datos: la primera, en cuanto a la necesidad de consentimiento del interesado o habilitación legal para la cesión de datos entre administraciones públicas; la segunda, declarando la invalidez de la Decisión 2000/520 sobre el estatus de EE.UU. como puerto seguro, suponen por sí solos un importante revulsivo en la materia. Aspectos a los que se suma la nueva normativa –Reglamento y Directiva–, que por vez primera, aborda la regulación sobre ficheros policiales en el contexto comunitario. Todo ello reclama una reflexión pausada y profunda sobre lo que estos cambios individualmente implican y, más allá de los mismos, si tienen una razón de

ABSTRACT:

The latest sentences of the European Court about data protection: first, about the need of consent or legal prevision for data exchange between public administrations; second, about the Decision 2000/500 and the status of EE.UU. and its security dealing with treatment of personal data, are an important change in the state of the issue. In addition, we have a new Resolution and a new Directive that, for the first time in the EU, deals with police files. The situation justifies a deep study of the changes produced. Moreover, we will try to discover if there is a general idea under these changes and if we can understand the direction of the EU in this important policy.

ser de conjunto que permita conocer el hacía dónde de los avances en la materia.

PALABRAS CLAVE: Cesión de datos AA.PP. - EE.UU. puerto seguro - Reglamento - ficheros privados - Directiva - ficheros policiales

KEYWORDS: Data Exchange between Public Administrations - EE.UU. safe stop - Resolution - Private files - Directive - police files

I. SITUACIÓN ACTUAL EN MATERIA DE PROTECCIÓN DE DATOS

A pesar de la nueva Directiva y Reglamento, el Derecho a la Protección de Datos actual sigue respondiendo a la Directiva 95/46/CE, la LO 15/99, de 13 de diciembre, de Protección de Datos (LOPD)[1], cuyas previsiones viene a completar el Reglamento de desarrollo aprobado en RD 1720/2007, de 21 de diciembre (RDLOPD)[2].

En el contexto nacional, el derecho a la protección de datos ha sido regulado en tanto que parte nuclear y específica del Derecho a la Intimidad Personal (art. 18 CE). Tal y como define el TC, en Sentencia 290/2000 de 30 de noviembre (RTC 2000, 290) , se trata del derecho de todo ciudadano a disponer de sus datos personales y conocer el tratamiento de los mismos que realicen otras personas. Esto es, se trata de proteger y garantizar el control de todo sujeto de derecho de los datos de los que sea titular. En este sentido, y en el contexto tecnológico en el que nos desenvolvemos, ha sido definido por la Doctrina como un derecho de consecución utópica, pero necesario e ideológicamente exigible[3]. Con esta finalidad, de acuerdo con la mencionada Directiva, la LOPD establece una exhaustiva regulación para la protección de los datos personales basada en los siguientes pilares: principios de protección de datos, derechos de los titulares de los datos personales, medidas de seguridad para su tratamiento y requisitos formales para la legalidad del mismo.

En relación con los principios que aplican al tratamiento de datos personales y siguiendo el orden que establece la norma, son los siguientes: principio de calidad, principios de información y consentimiento, y principios de seguridad y secreto (arts. 4 a 10LOPD). El principio de calidad regulado en el art. 4LOPD[4] tiene dos consecuencias principales. De un lado, los datos personales sólo pueden recogerse en tanto que necesarios para finalidad legítima que se proponen, valorado todo ello bajo el prisma del principio de proporcionalidad y sin que sea posible destinarlos a finalidad distinta de la específica para la que fueron recabados. De otro, el tratamiento de los datos, su uso, únicamente es posible durante el tiempo en el que esa finalidad para la que ha sido recabado lo exija, debiendo ser cancelados en cuanto dejen de ser necesarios a la misma. Dada la dificultad que puede suponer determinar el momento en que decae esa utilidad, es práctica habitual distinguir dos tipos de cancelación: la cancelación en sentido estricto frente al bloqueo previo de los datos. La primera, de contenido e interpretación más legalista, supone la destrucción definitiva de los datos. Por su parte, el bloqueo de los datos, limita el acceso a los mismos, permitiéndolo únicamente en supuestos tasados previamente por el responsable del tratamiento del dato. Es decir, el bloqueo se justifica cuando el dato ha dejado de ser útil a la finalidad que pretendía, excepto en determinados casos concretos[5].

Por su parte, el Derecho a la Información en la recogida de datos regulado en el art. 5LOPD[6] implica el cumplimiento del siguiente, el de consentimiento, regulado en el art. 6 de la Ley[7]. Es decir, una buena información deriva en un adecuado consentimiento del titular del dato.

Por último, íntimamente relacionados entre sí y con las medidas de seguridad que tratamos posteriormente, concurren los principios de seguridad y de secreto (arts. 9 y 10LOPD respectivamente). Así, el principio de seguridad implica que su tratamiento se va a realizar de acuerdo con la norma que analizamos, aplicando las medidas de seguridad previstas para cada tipo de dato y en cumplimiento, además de con los principios anteriores, muy especialmente, con el de secreto. Todo ello con la finalidad de evitar que datos personales resulten indebidamente difundidos o que personal no autorizado conozca, use o ceda datos personales excediendo la habilitación que normativamente le hubiera sido concedida.

En cuanto al análisis del segundo pilar en la protección de datos personales, se trata de los derechos de los titulares. Estos suponen la manifestación directa de los principios antes expuestos. En concreto, se trata de los derechos conocidos como derechos ARCO: Acceso, Rectificación, Cancelación y Oposición. Si el significado de los

tres primeros es claro, el Derecho de Oposición merece mayor explicación. En concreto, actúa en aquellos supuestos en que no es necesario consentimiento para el tratamiento de datos personales (art.6LOPD), constituyendo este derecho a oponerse una especie de garantía subsidiaria para los titulares de los datos tratados. Los arts. 13 a 19LOPD regulan el contenido específico de todos ellos. Por su parte, el RDLOPD en su Título III desarrolla los trámites específicos previstos para su ejercicio y denegación. En concreto, para el caso del derecho de acceso, el Responsable del Tratamiento ha de responder en el plazo de un mes desde su ejercicio, pudiendo denegar el acceso en caso de que el mismo ya se hubiese ejercido en el plazo de los doce meses anteriores, excepto que concurra interés legítimo del titular del dato. En relación con los restantes derechos, el plazo para resolver es de diez días.

En relación al tercero de los pilares de protección mencionados, las medidas de seguridad antes anunciadas, se regulan al competo en el Título VIII del Reglamento de desarrollo de la LOPD. Se organizan normativamente en tres niveles de clasificación, paralelos a la sensibilidad o importancia de los datos personales que protegen [8)]. De manera que, las exigencias que las medidas de seguridad conllevan son correlativas a la importancia y sensibilidad de los diferentes niveles expuestos. Y, aunque las medidas de seguridad en sí coinciden entre los diferentes niveles, implican mayores requisitos a medida que se asciende en nivel de clasificación.

En concreto, los ficheros de nivel bajo requieren desde el punto de vista personal, que quienes traten los datos estén informados de sus obligaciones, en especial el deber de secreto. A su vez, los usuarios habrán de estar incluidos en diferentes niveles de uso y acceso a los datos, dependiendo de las necesidades derivadas de las funciones que desarrollan con los mismos. Por su parte, a nivel procedimental, se exige que se realice una copia de respaldo semanal que evite la pérdida de los datos. Ello en el contexto más general de un proceso de resolución de incidentes que también habrá de estar previsto (arts. 89-94 RDLOPD).

Si ascendemos al nivel medio de clasificación, a los anteriores requisitos se suman otros nuevos. En primer lugar, este tipo de ficheros han de ser auditados cada dos años de modo completo a fin de observar que su tratamiento se adecua a la legalidad. A su vez, es necesario que por cada uno de estos ficheros se nombre un , que bajo la tutela del Responsable de Tratamiento, verdadero titular del fichero, reportará ante el mismo y será el responsable de que las medidas de seguridad del fichero se cumplimentan por todo el personal implicado (arts. 95-100 RDLOPD)[9)]. En cuanto al resto de medidas aplicables a los ficheros pertenecientes a este nivel, no suponen más que un aumento de las exigencias de las medidas ya previstas para los ficheros de nivel bajo. De esta manera, las medidas de seguridad para el acceso al fichero incluyen una política de identificación más estricta, que limita los errores en intentos de acceso. Con la misma lógica, no sólo se controla el acceso al dato en sí, sino también al lugar físico en que los mismos están ubicados.

Por último, en cuanto a los ficheros que se corresponden al nivel máximo de protección y sensibilidad, se aplican las medidas previstas para los ficheros anteriores pero como venimos diciendo, con mayores exigencias. En este sentido y en cuanto a los accesos, se requiere además, que los mismos queden grabados. Del lado procedimental, y como parte del procedimiento de resolución de incidentes, se exige que las copias de respaldo estén ubicadas en un lugar diferente al del original cuya conservación garantizan (arts. 101-104 RDLOPD).

Lo anterior de acuerdo con el siguiente esquema normativo.

NIVEL BAJO	NIVEL MEDIO	NIVEL ALTO
Recursos Humanos +		
Procedimiento de Incidencias +		
Control de Acceso	Responsable de Seguridad	
Inventario de Soportes	Auditorías	
Identificación y Autenticación +		
Copias de respaldo y Recuperación +		
Ficheros no automatizados		
(medidas especiales)		

Como pilar último de la protección general que la norma otorga a los datos personales, destaca la necesidad de que se cumplan determinados formalismos que amparen la legalidad de la recogida y tramitación del dato. Para el caso de ficheros de titularidad privada, es decir, aquellos en los que el Responsable de Tratamiento es un sujeto privado, empresa o particular, basta con la inscripción del fichero en el Registro de la AEPD (art. 25LOPD). Para el caso de ficheros bajo titularidad pública, y por la mayor afectación de bienes jurídicos que estos conllevan, se requiere su publicación en Orden General, de acuerdo con lo que establece el art. 20LOPD (art. 54 RDLOPD)[10].

Vistos los cuatro pilares básicos, establecidos con carácter general para la protección de los datos personales, corresponde considerar las especialidades existentes relativas a determinados ficheros de titularidad pública. En primer lugar, en cuanto a los ficheros totalmente excluidos de la normativa que exponemos, los del art. 2.2 c) LOPD. Así:

«El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.»

En segundo lugar, estando bajo aplicación la norma pero con especialidades a tener en cuenta en tres de los cuatro bloques de protección general antes expuestos, los ficheros policiales del art. 22.2LOPD.

Así, en cuanto a su definición:

«2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.»

En cuanto a sus especialidades, el art. 23LOPD establece que:

«1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.»

A la misma, se suma lo expuesto anteriormente al tratar los diferentes niveles de clasificación de los datos. Así, según el art. 81 RDLOPD, los ficheros del art. 22.2LOPD (ficheros policiales recabados sin consentimiento) son todos de nivel alto de protección y seguridad.

En tercer lugar, el art. 24LOPD prevé, con carácter más general respecto de ficheros bajo titularidad pública y no referido exclusivamente al grupo de ficheros del art. 22.2LOPD, lo siguiente:

«1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.

2. Lo dispuesto en el artículo 15 y en el apartado 1 del artículo 16 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.»

Por tanto, como vemos, existen tres supuestos diferentes de ficheros de titularidad pública con posibilidad de excepción parcial o total del régimen de protección general que la norma establece. De un lado, los ficheros con datos para la investigación de terrorismo y formas graves de delincuencia organizada, completamente exentos de la aplicación de los cuatro bloques de protección de datos antes descritos. De otro, los ficheros bajo titularidad de Fuerzas y Cuerpos de Seguridad con datos destinados específicamente a la investigación policial. Respecto de estos aplica el régimen general excepto en lo relativo a algunos de los bloques expuestos y siempre que concurran determinadas circunstancias: exención del principio de información y consentimiento, por propia definición de los ficheros (art. 22.2LOPD); y denegación de ejercicio de derechos ARCO en los casos del art. 23LOPD, valoradas las circunstancias que enumera precepto una vez aplicadas al caso concreto. Por último, el régimen del art. 24LOPD, con exención del principio de información y consentimiento (art. 5LOPD), y la denegación del ejercicio de los derechos ARCO, aplicable respecto de datos contenidos en ficheros públicos, siempre que concurran determinados riesgos valorados también caso a caso. Respecto de estos últimos, y aunque en muchos casos se trate de supuestos coincidente con las excepciones propias de los ficheros policiales, la norma concede cierta habilitación para la aplicación de estas excepciones con carácter más general, no sólo circunscrita a los mismos.

Desde un punto de vista valorativo, se trata de una normativa híper garantista respecto de los derechos de los ciudadanos. De hecho, las excepciones que la norma prevé respecto del régimen de protección que establece, son del todo comprensibles. La administración pública quedaría imposibilitada para llevar a cabo las funciones que le son propias, especialmente las relativas a la persecución y represión de los delitos, de tener que respetar en todo caso y sin excepción, el alto régimen de protección de la privacidad que la norme impone. Sin embargo, justamente por ese híper garantismo y la burocracia que se le asocia, y las necesarias excepciones que hay que establecer respeto al mismo, la norma resulta excesiva en algunos de sus puntos y escueta en otros. La realidad práctica de la protección de datos y la relación de este derecho con el vertiginoso avance de las tecnologías dan idea de ello. De ahí la nueva normativa que la UE ha elaborado y las nuevas resoluciones del TSJE que pasamos a comentar.

II. SENTENCIA DEL TJUE SOBRE CESIÓN DE DATOS ENTRE ADMINISTRACIONES

A modo de contextualización para comprender la importancia de la Sentencia del Tribunal de Justicia Europeo de 1 de octubre de 2015 es necesario conocer el modo en que dicha cesión se regula de manera general. De acuerdo con el art. 11LOPD:

«1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas.

Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.»

Como vemos, para que la cesión de datos entre administraciones públicas sea legítima, bien se ha de contar con el consentimiento del titular del dato, bien han de concurrir determinados supuestos que específicamente legitimen esa cesión [11)]. Prescindiendo de la cesión a autoridades judiciales o casos extremos de interés vital del interesado, estos son: existencia de una ley que habilite la cesión; utilización de los datos personales por la administración receptora para fines estadísticos, científicos o históricos, lo que en la práctica equivale a su disociación; recogida de los datos con destino a la administración cedente o cesión a otra con competencias idénticas a la cesionaria, tal y como especifica el RDLOPD [12)].

Teniendo en cuenta lo anterior, y para el caso de habilitación legal, la Sentencia del TJUE declara que la Directiva 95/46/CE y las normas nacionales que la implementan «deben interpretarse en el sentido de que se oponen a medidas nacionales, como las que son objeto del procedimiento principal, que permiten a una administración pública de un Estado miembro transmitir datos personales a otra administración pública y el subsiguiente tratamiento de estos datos, **sin que los interesados hayan sido informados de esa transmisión ni de ese tratamiento ».** Según el TJUE, es lícito transmitir esos datos de relevancia para el interés general sin autorización o comunicación al interesado, pero siempre que se cumplan requisitos muy estrictos. En concreto: es indispensable que la ley nacional defina específicamente y de manera detallada los datos que pueden transmitirse. A tales efectos, el TJUE reprocha a la ley rumana objeto de la cuestión prejudicial, que regule la transmisión sólo « **como principio».**

En resumen, el TJUE no sólo exige que haya una habilitación legal para que la cesión de datos entre AA.PP. sea legítima, sino que, conforme al principio de calidad, la norma ha de ser lo suficientemente específica respecto de los datos a transmitir y su finalidad. A pesar de que quedan pendientes de delimitación ciertos aspectos –« falta delimitar a qué se refiere la transmisión de datos que se ha de notificar, si es solo cuando una administración pide los datos a otra o si se ha de realizar siempre que se transmitan datos personales aunque sea en una petición más amplia»– [13)], una simple lectura inicial de la resolución plantea ya importantes consecuencias que obligan a replantear el modo en que la AP procede en nuestro país.

En primer lugar, afecta a la cesión de datos personales que se realiza al amparo de la Ley 58/2003 General Tributaria (LGT), poco detallista, como vamos a ver, en cuanto al contenido, requisitos y finalidad de la cesión. Conforme al art. 94 de la LGT, sobre las Autoridades sometidas al deber de informar y colaborar:

«1. Las autoridades, cualquiera que sea su naturaleza, los titulares de los órganos del Estado, de las comunidades autónomas y de las entidades locales; los organismos autónomos y las entidades públicas empresariales; las cámaras y corporaciones, colegios y asociaciones profesionales; las mutualidades de

previsión social; las demás entidades públicas, incluidas las gestoras de la Seguridad Social y quienes, en general, ejerzan funciones públicas, estarán obligados a suministrar a la Administración tributaria cuantos datos, informes y antecedentes con trascendencia tributaria recabe ésta mediante disposiciones de carácter general o a través de requerimientos concretos, y a prestarle, a ella y a sus agentes, apoyo, concurso, auxilio y protección para el ejercicio de sus funciones.

Asimismo, participarán en la gestión o exacción de los tributos mediante las advertencias, repercusiones y retenciones, documentales o pecuniarias, de acuerdo con lo previsto en las leyes o disposiciones reglamentarias vigentes.

2. A las mismas obligaciones quedarán sujetos los partidos políticos, sindicatos y asociaciones empresariales.

3. Los juzgados y tribunales deberán facilitar a la Administración tributaria, de oficio o a requerimiento de la misma, cuantos datos con trascendencia tributaria se desprendan de las actuaciones judiciales de las que conozcan, respetando, en su caso, el secreto de las diligencias sumariales.

4. El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y la Comisión de Vigilancia de Actividades de Financiación del Terrorismo, así como la Secretaría de ambas comisiones, facilitarán a la Administración tributaria cuantos datos con trascendencia tributaria obtengan en el ejercicio de sus funciones, de oficio, con carácter general o mediante requerimiento individualizado en los términos que reglamentariamente se establezcan.

Los órganos de la Administración tributaria podrán utilizar la información suministrada para la regularización de la situación tributaria de los obligados en el curso del procedimiento de comprobación o de inspección, sin que sea necesario efectuar el requerimiento al que se refiere el apartado 3 del artículo anterior.

5. La cesión de datos de carácter personal que se deba efectuar a la Administración tributaria conforme a lo dispuesto en el artículo anterior, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito no será de aplicación lo dispuesto en el apartado 1 del artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.»

Se observa cómo la norma, en contra del criterio que defiende el TJUE, establece un principio general de comunicación-cesión de datos, sin concretar aspectos adicionales ahora necesarios.

Pero más grave aún, y más allá de lo anterior, la sentencia supone la piedra de toque definitiva para que determinadas administraciones dejen de realizar las cesiones de datos personales que habitualmente acostumbran aún careciendo de una mínima habilitación legal para ello. Es lo que sucede en el caso de la Administración Penitenciaria abordado con ocasión de anteriores estudios [14)]. En concreto, la protección de los datos de los internos se regula en los arts. 6-9 del Reglamento Penitenciario regulado por RD 190/1996, de 9 de febrero (RP) [15)]. Si bien el RP de 1996 coincide en parte con lo que contempla la LOPD de 1999, lo cierto es que requiere, ante la falta de su adecuada adaptación, una interpretación en clave legal. Por tanto, no nos sirven aquellas excepciones que el RP establece por sí sólo y no coinciden con las de la norma específica. En especial, la del apartado 2 del art. 7RP:

«Tampoco será preciso el consentimiento del recluso afectado para ceder a otras administraciones públicas, en el ámbito de sus respectivas competencias, los datos de carácter personal contenidos en los ficheros informáticos penitenciarios que resulten necesarios para que éstas puedan ejercer sus funciones respecto de los internos en materia de reclutamiento para la prestación del servicio militar, servicios sociales, Seguridad Social, custodia de menores u otras análogas.»

Sin embargo, en la práctica, por desconocimiento o comodidad administrativa, se entiende que este precepto sigue vigente y se ceden datos sin consentimiento del interesado interno y sin habilitación legal alguna para ello. Hecho que, por pura inercia, se extiende también a los datos especialmente protegidos –como los contenidos en informes psicológicos– a pesar de para estos el RP sí prevé la necesidad de que en todo caso se preste consentimiento expreso [16)]. Todo ello con importantes consecuencias para la vida de los internos que ven cómo se propagan datos que deberían quedar en el intramuros de lo penitenciario [17)].

En definitiva, a pesar de las críticas a las que la nueva Sentencia del TJUE ha sido sometida, en especial por las dificultades tributarias que implica y sus aspectos favorables para los defraudadores [18)], lo cierto es que nos parece del todo necesaria. Y es que no nos está diciendo que los datos personales necesarios para el buen funcionamiento de las AA.PP. no se cedan, sino que se cedan con determinadas garantías: bien una norma legal suficientemente específica, bien bajo consentimiento del interesado [19)].

III. EE.UU. NO ES LO QUE PARECE: SENTENCIA DEL TJUE SOBRE PUERTO SEGURO

Con fecha 6 de octubre de 2015, el TJUE ha declarado inválida la Decisión de la Comisión 2000/520/CE que establece el nivel adecuado de protección de las garantías internacionales de datos a Estados Unidos ofrecidas por el acuerdo de puerto seguro, prohíbe transferir datos de carácter personal y datos de especial protección a países que no sean puerto seguro. Y como puerto seguro, de momento, solo se entiende el ámbito de la UE. En concreto, de acuerdo con la propia sentencia:

«El artículo 25, apartado 6, de la de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en su versión modificada por el Reglamento (CE) nº 882/2003 del Parlamento Europeo y del Consejo, de 29 de septiembre de 2003, entendido a la luz de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que una Decisión adoptada en virtud de la referida disposición, como la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, por la que la Comisión Europea constata que un tercer país garantiza un nivel de protección adecuado, no impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, en su versión modificada, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado.

La Decisión 2000/520 es inválida.»

La resolución, además de disipar las dudas sobre la competencia de la autoridad de control, elimina a EE.UU. como contraparte garante pues refiere haber constatado intromisiones ilegítimas de las autoridades gubernativas en los datos personales de sus ciudadanos.

Las consecuencias de la sentencia son numerosas y casi inabarcables, pues son numerosas las ocasiones en que en el tráfico jurídico se utilizan servidores americanos y se transfieren datos a través de los mismos. Por ejemplo, el fisco español utiliza esos servidores para conceder la firma digital, por lo que en una cantidad importante de transferencias de datos –cuando se hace referencia a datos personales–, se estaría vulnerando la ley comunitaria.

IV. EL NUEVO PAQUETE EUROPEO PARA LA PROTECCIÓN DE DATOS PERSONALES: CONTENIDO E INCIDENCIA NACIONAL

En la era de la digitalización y el avance tecnológico parecía inevitable una actualización de la Directiva 95/46 sobre protección de datos, elaborada en una época en que el uso de internet y las nuevas tecnologías era comparativamente incipiente. En este sentido, la nueva normativa pretende facilitar el Mercado Digital Único y responder a sus necesidades. Igualmente, se trata de hacer frente a los retos que plantea la Agenda de Seguridad Europea. Para ello, son dos normas las que componen el nuevo paquete normativo. De un lado, el Reglamento (EU) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46. De otro lado, la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales; ejecución de sanciones penales, y a la libre

circulación de dichos datos, por la que se deroga la Decisión Marco 2008/977/JAI del Consejo [20]. Veamos su contenido más en concreto y los avances que el mismo supone.

1. EL REGLAMENTO PARA LA PROTECCIÓN DE DATOS DE FICHEROS PRIVADOS

Se trata de una norma muy extensa, que consta de 173 considerandos previos y 99 artículos, agrupados en once capítulos, con la siguiente estructura: Capítulo I. Disposiciones generales; Capítulo II. Principios; Capítulo III. Derechos del interesado; Capítulo IV. Responsable del tratamiento y encargado del tratamiento; Capítulo V. Transferencias de datos personales a terceros países u organizaciones internacionales; Capítulo VI. Autoridades de control independientes; Capítulo VII. Cooperación y coherencia; Capítulo VIII. Recursos, responsabilidad y sanciones; Capítulo IX. Disposiciones relativas a situaciones específicas de tratamiento; Capítulo X. Actos delegados y actos de ejecución; Capítulo XI. Disposiciones finales.

La finalidad de la norma, según su art. 1, lo constituyen: «1. Las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales. 2. Las normas relativas a la libre circulación de tales datos». Como ámbito de aplicación material, el art. 2 determina: «el tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero», quedando excluidas principalmente: «actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión; la actividad de las autoridades con fines de prevención o investigación de delitos o de protección de la seguridad pública; el tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.» En cuanto a su aplicación territorial, es importante resaltar que, conforme a su art. 3: «El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.» Y, muy especialmente, según el número 2 del mismo artículo, el Reglamento se aplica también al tratamiento de datos personales de residentes en la Unión «por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.» Es decir, se aplica también al también al tratamiento de datos fuera de la Unión, lo que amplía notablemente su ámbito de aplicación.

En cuanto a los principios aplicables al tratamiento de datos, se amplían y precisan los mismos. Así, destacan los principios de: limitación de la finalidad –principio de recogida con fines determinados, explícitos y legítimos–; minimización de los datos –limitados a lo necesario en relación con los fines para los que son tratados–; exactitud –datos exactos y, si fuera necesario, actualizados–; limitación del plazo de conservación –datos mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales–; integridad y confidencialidad –tratados de tal manera que se garantice una seguridad adecuada de los datos personales–; responsabilidad proactiva –el responsable del tratamiento será responsable del cumplimiento de la norma y capaz de demostrarlo– y principio de portabilidad que materializa un mayor carácter de disposición del titular de los datos sobre el uso y tratamiento que se dé a los mismos.

A su vez, la nueva norma acaba con los conocidos y antes referidos derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). El Reglamento, en desarrollo de los principios señalados, desglosa y amplía los derechos actualmente vigentes, refiriendo los derechos de Transparencia (art. 12), Información (arts. 13 a 14), Acceso (art. 15), Rectificación (Art. 16), Supresión o derecho al olvido (art. 17), Limitación del tratamiento (art. 18), Portabilidad de datos (art. 20) y Oposición (art. 21).

Además de lo anterior, destacan como principales novedades a tener en cuenta: un continente, una norma –la nueva normativa establece un único conjunto de normas aplicable en el conjunto de la Unión Europea–; ventanilla única –los empresarios solo tendrán que relacionarse con un único supervisor en Europa, lo que se estima representará un ahorro de 2.300 millones de euros al año–; consideración de los riesgos específicos –las nuevas normas evitarán pesadas obligaciones genéricas sobre el tratamiento de datos, adaptándolas apropiadamente a los factores de riesgo de cada empresa–; privacidad desde el diseño –las nueva regulación garantizará que la salvaguarda de la protección de datos se incorpora a los productos y servicios desde sus

primeros estadios de desarrollo (*Data protection by design*). Esto implica, por ejemplo, que en materia de redes sociales, los perfiles de privacidad de los usuarios estarán por defecto cerrados a otros usuarios, debiendo ser el usuario quien los abra a otros–; la importancia del consentimiento –el consentimiento para el tratamiento de los datos deberá ser «libre, específico, informada e inequívoco» y el responsable del tratamiento de los datos deberá poder probar que el titular «consintió el tratamiento de sus datos»–; regulación específica del conocido como Derecho al olvido – *the right to be forgotten* – o, más propiamente, derecho de supresión; notificación a los interesados de las violaciones de seguridad; consulta previa a la autoridad de control en caso de identificarse riesgos en el tratamiento; introducción de la figura del Delegado de protección de datos [21)].

En general, El Reglamento Europeo de Protección de Datos unifica y moderniza la normativa europea sobre protección de datos, permitiendo a los ciudadanos un mejor control de sus datos personales y a las empresas aprovechar al máximo las oportunidades de un mercado único digital, reduciendo la burocracia y beneficiándose de una mayor confianza de los consumidores.

Sin embargo, el alcance tan amplio explica el tiempo que ha tardado en aprobarse y que sea un texto muy extenso y detallado, lleno de letra pequeña [22)]. A la vez, se trata de una norma que recurre a abundantes conceptos jurídicos indeterminados, que lo hacen difícil de interpretar en muchas ocasiones [23)]. Por ello, se pone también en duda que pueda ser considerado un reglamento homogéneo para todos los países. En España, como hemos visto antes, la legislación sobre esta materia ya ha sido muy exigente pero cabe preguntarse si en el resto de países se aplicará con el mismo rigor. En el mismo sentido, existen en el Reglamento una serie de materias en las que los Estados van a contar con un cierto margen de maniobra –como el tratamiento de datos por los poderes públicos y las situaciones específicas de tratamiento o el Derecho laboral, de las que el Reglamento parece huir–. Aspectos todos ellos que, unidos a lo estricto del régimen de garantías, hacen bastantes recomendable la autorregulación empresarial que evite dudas interpretativas y posteriores denuncias.

Igualmente, el sector destaca que el Reglamento no contempla específicamente cuestiones como el Big Data, el Cloud Computing, el Internet de las cosas o BiTech. Parece que se ha perdido una ocasión para adaptar completamente la norma al entorno digital para permitirla envejecer bien. Finalmente, se critica el hecho de que el pequeño empresario, que es el mayoritario dentro y fuera de nuestro país, es el gran olvidado de esta norma, para cuyo cumplimiento, a pesar de la eliminación de ciertas trabas burocráticas y la adaptación al riesgo específico que su actividad presente, estará obligado a solicitar continuo asesoramiento.

2. LA DIRECTIVA EUROPEA PARA LA PROTECCIÓN DE LOS FICHEROS POLICIALES

La Directiva Europea de Protección de Datos, por su parte, está destinada a los ámbitos policiales y de la Justicia. Pretende asegurar que los datos de las víctimas, testigos y sospechosos de la comisión de delitos se encuentren debidamente protegidos en el ámbito de una investigación criminal o de aplicación de la ley. Su intención es proteger a las personas implicadas en investigaciones policiales o procesos judiciales, sea como víctimas, acusados o testigos, mediante la clarificación de sus derechos y el establecimiento de límites en la transmisión de datos para prevención, investigación, detección y enjuiciamiento de delitos o la imposición de penas. La norma incluye salvaguardas para evitar riesgos para la seguridad pública, al tiempo que se facilita una cooperación más rápida y efectiva entre las autoridades policiales y judiciales [24)].

A la vez, una vez armonizadas, las nuevas normas nacionales facilitarán la cooperación transfronteriza de la policía y los fiscales para combatir más eficazmente el crimen y el terrorismo en toda Europa. Según la ponente de la Directiva, Marju Lauristin: «El principal problema ante los ataques terroristas y otros crímenes trasnacionales es que los cuerpos judiciales y de seguridad son reacios a compartir información valiosa. Al fijar estándares europeos para el intercambio de información, esta norma se convertirá en una herramienta útil para ayudar a las autoridades a trasladar datos personales de manera sencilla y efectiva, asegurando el respeto al derecho fundamental a la privacidad» [25)]. En este punto es relevante tener en cuenta que a diferencia de la Decisión a la que sustituye, se aplicará a los intercambios domésticos y transfronterizos y supone una adaptación a las últimas normas sobre recogida de datos de pasajeros aéreos.

3. ¿EN QUÉ SENTIDO SE HAN DE MODIFICAR LAS NORMAS NACIONALES?

El reto al que se enfrentan los países de la EU en materia de protección de datos es ingente y múltiple. Primero, en relación al Reglamento, a pesar de que su art. 99 determina que entrará en vigor 20 días después de su publicación en el Diario oficial de la UE, la compleja preparación que requiere por parte de los Estados miembros –como tal Reglamento de la Unión será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro–, justifica una *vacatio legis* mayor. En concreto, sus disposiciones serán de aplicación directa en todos los Estados miembros dos años después, a partir del 25 de mayo de 2018. Segundo, para la Directiva, los países tendrán un plazo de dos años para implementar sus cambios en la legislación nacional. En el caso de Reino Unido e Irlanda, la directiva sobre intercambio de datos para fines policiales y judiciales sólo se aplicará de manera limitada.

Para el contexto español, la entrada en vigor de este paquete normativo plantea la duda de cómo va a convivir con la LOPD. En cuanto al Reglamento, parece que la ley española podrá seguir siendo aplicable en lo que esté fuera del Derecho de la UE, dado que el mismo hace numerosas remisiones a la legislación nacional de los Estados miembros. Sin embargo, ello no resuelve las numerosas dudas que se suscitan. Así, para el registro de ficheros se desconoce si habrá que seguir realizándolo en nuestro país por efecto de la LOPD o cabe entender una derogación tácita de sus disposiciones en este sentido. Igualmente, ante la creación de una única autoridad supervisora europea, cabe preguntarse en qué papel quedará al AEPD y qué valor tendrán sus circulares en el nuevo contexto. En relación a la Directiva, sin duda requerirá una labor de revisión, actualización y adaptación de las previsiones de la LOPD a su contenido armonizador.

V. MENSAJE GLOBAL DE CAMBIOS QUE COINCIDEN

Vivimos en un mundo en el que almacenar y tratar datos personales es base de negocios y ganancias excepcionales. Nuestra intimidad supone un importante filón para publicistas, marcadores de tendencias, estudiosos de los mercados, analistas varios. Y no sólo eso. Los datos personales que nos definen y pertenecen son básicos para el devenir de toda actividad pública y privada que implique a varias personas. Siendo éste el contexto, la dirección que han adoptado las normas en protección de datos es la del híper garantismo. Ante las infinitas posibilidades de uso de nuestra intimidad, se aboga por tender a procurar el control absoluto sobre la misma. Siendo esto loable, la realidad que hemos analizado nos dice hasta qué punto resulta imposible.

En primer lugar, hemos visto que la norma ha sucumbido a la realidad estableciendo excepciones al régimen tan exigente que la define. Motivos de seguridad pública, investigación policial, etc. permiten rebajas a las exigencias generales que la protección de datos impone. Excepciones necesarias, pero que, por el propio dinamismo de la realidad que abordan, dan lugar a nuevos huecos de desprotección en los que la intimidad se ve inevitablemente lesionada. Reconducir estos huecos, estos espacios de indefensión, es el objetivo de las sentencias que hemos abordado. Objetivo que, si bien creemos que puede cumplirse con proporcionalidad –especialmente en lo relativo a la cesión de datos entre administraciones públicas–, puede llevar de nuevo a ese híper garantismo paralizador de la actividad a la que el tratamiento de datos sirve.

En segundo lugar, la tecnología avanza a un ritmo vertiginoso e inasumible para el Legislador comunitario. Sus dos normas estrella en lo que a la materia que abordamos se refiere dan idea de ello. La homogeneización y armonización que Reglamento y Directiva pretenden van muy por detrás de los objetivos que las inspiran. El primero por no haber abordado nuevos cambios tecnológicos que lo hacen obsoleto. La segunda al pretender atajar determinados tipos de delincuencia años luz de distancia de las normas que tratan de atajarla. El ratón que juega con un gato que, casi por definición, aparece siempre despistado.

---

notas al pie de pÁgina

---

[1] BOE núm. 298, de 14 de diciembre de 1999.

---

[2] BOE núm. 17, de 19 de enero de 2008.

[3]

Destacan entre otros, Lesmas Serrano, C., *La Ley de Protección de datos: Análisis y Comentario de su Jurisprudencia,* Lex Nova, Valladolid, 2007; Serrera Cobos, P., *Buenas prácticas en Protección de Datos* , Dintes Fundación, Madrid, 2007; Zabía de la Mata, J., *Protección de datos. Comentario al Reglamento* , Lex Nova, Valladolid, 2008.

[4]

«1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. 2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos. 3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. 4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16. 5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos. 6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados. 7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.»

[5]

Supuesto típico de bloqueo es el que tiene lugar el de ficheros bajo titularidad de Fuerzas y Cuerpos del Estado, cuyos datos se tratan con específica finalidad policial. En estos supuestos es fundamental conservar ciertos datos en ese estado de semicancelación que supone el bloqueo, en espera de futuras reaperturas del caso o de reclamaciones judiciales de determinados datos del mismo.

[6]

«1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento. 2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior. 3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. 4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo. 5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos.»

[7]

«1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco el afectado, salvo que la ley disponga otra cosa. 2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado. 3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. 4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.»

8

En concreto, el art. 81 RDLOPD distingue: «1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico. 2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal: a) Los relativos a la comisión de infracciones administrativas o penales. b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre (servicios de información sobre el crédito). c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias. d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros. e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social. f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos. 3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal: a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual. b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas. c) Aquéllos que contengan datos derivados de actos de violencia de género.»

9

Los Arts. 3LOPD y 5 RDLOPD establecen algunas definiciones relevantes en la comprensión global del conjunto normativo que presentamos. Entre ellas, destaca la del Responsable del Fichero o Tratamiento. La letra q) de la norma reglamentaria aporta la definición más completa al respecto. Así, Responsable del fichero o del tratamiento es la «Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.» Se distingue por tanto, el Responsable de Fichero o Tratamiento del mero Usuario tramitador de los datos. A la vez que, las medidas de seguridad introducen como hemos visto, una nueva figura independiente, la del Responsable de Seguridad.

10

Al respecto: «1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente. 2. Las disposiciones de creación o de modificación de ficheros deberán indicar: a) La finalidad del fichero y los usos previstos para el mismo. b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos. c) El procedimiento de recogida de los datos de carácter personal. d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo. e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros. f) Los órganos de las Administraciones responsables del fichero. g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición. h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible. 3. En las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.»

11

El art. 21LOPD añadía un supuesto adicional para cesión de datos entre Administraciones Públicas. De acuerdo con el mismo: «1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. 2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra. 3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa. 4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.» Sin embargo, el inciso innovador que permitía la cesión sin consentimiento cuando «hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso» fue declarado inconstitucional en STC 292/2000, de 30 de noviembre (RTC 2000, 292).

12

Por su parte, el art. 10 del RDLOPD, refiere en términos parecidos aunque más específicos: «1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello. 2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando: a) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes: El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre. El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas. b) Los datos objeto de tratamiento o de cesión figuren en fuentes accesibles al público y el responsable del fichero, o el tercero a quien se comuniquen los datos, tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado. No obstante, las Administraciones públicas sólo podrán comunicar al amparo de este apartado los datos recogidos de fuentes accesibles al público a responsables de ficheros de titularidad privada cuando se encuentren autorizadas para ello por una norma con rango de ley. 3. Los datos de

carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando: a) Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario. b) Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento. c) El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre. 4. Será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando: a) La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique. b) La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente. c) La cesión entre Administraciones públicas cuando concurra uno de los siguientes supuestos: Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos; Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra; La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias. 5. Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre. En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.»

---

[13]

Eulalio Ávila Cano, presidente del Colegio Oficial de Secretarios, Interventores y Tesoreros de la Administración Local (Cosital) en http://www.elconfidencial.com/espana/2016-03-29/una-sentencia-europea-pone-los-embargos-de-hacienda-al-borde-de-la-legalidad_1175169/

---

[14]

Lacal Cuenca, P.; Solar Calvo, P., «Cesión de datos entre Administraciones: el caso de la Administración Penitenciaria», *Diario la Ley* , 21.09.15, pp. 66-11.

---

[15]

BOE de 15 de febrero de 1996.

---

[16]

Así, según el art. 7.3LOPD: «Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente» y, conforme al mismo, el art. 8RP: «1. No obstante lo dispuesto en el artículo anterior, los datos de carácter personal de los reclusos relativos a opiniones políticas, a convicciones religiosas o filosóficas, al origen racial y étnico, a la salud o a la vida sexual, que hayan sido recabados para formular los modelos individualizados de ejecución o los programas de tratamiento penitenciarios, sólo podrán ser cedidos o difundidos a otras personas con el consentimiento expreso y por escrito del recluso afectado o cuando por razones de interés general así lo disponga una Ley. 2. Cuando se soliciten de la Administración Penitenciaria este tipo de datos especialmente protegidos por medio de representante del recluso, deberá exigirse, en todo caso, poder especial y bastante otorgado por el mismo en el que conste expresamente su consentimiento para que su representante pueda tener acceso a dichos datos personales del recluso.»

---

[17]

Lacal Cuenca, P., en Lacal Cuenca, P.; Solar Calvo, P., «Cesión de datos entre Administraciones: el caso de la Administración Penitenciaria», *Diario la Ley* , ob. cit., p. 10, apunta un problema adicional, más allá de la disminución de garantías que supone para los derechos de los internos, para el caso concreto de ceder datos contenidos en informes psicológicos: «No debemos olvidar en este punto que los informes del medio penitenciario tienen una finalidad concreta y que, aún de contar con el consentimiento del interno, la valoración de los mismos debiera realizarse con todas las precauciones. Esto porque la finalidad de los mismos es específica y destinada a su tratamiento penitenciario pero no a valorar aptitud alguna que pueda influir en el cuidado y custodia de sus hijos. Sin embargo, a pesar de los inconvenientes constitucionales y legales aducidos, y por el propio sentido distinto de las actividades administrativas que pueden concurrir, es mucho más cómodo solicitar informes estrictamente penitenciarios que completen o, lo que es peor, sustituyan una actividad valorativa que debiera ser exclusiva y propia. Todo ello con los riesgos descritos no sólo desde el punto de vista normativo, sino por la confusión de criterios valorativos que sin duda perjudicará el fundamento y acierto de la decisión que finalmente se adopte.».

---

[18]

Bornstein F., «Un defensor inesperado de los tramposos: el candor fiscal del Tribunal Europeo», *El Confidencial* , disponible en:

http://www.cuartopoder.es/luzdecruce/2016/04/10/defensor-inesperado-los-morosos-la-ingenuidad-fiscal-del-tribunal-europeo/8997

---

[19]

Para las complicaciones burocráticas que pudieran surgir al respecto, el secretario de Alzira propone «que se firme una especie de protocolo o

autorización una sola vez, por el que el ciudadano da su permiso para la transmisión de datos. Él ya es consciente de los datos que tenemos las administraciones, y lo que se haría sería simplificar los trámites. Esa autorización se podría validar incluso telemáticamente. Es la manera más sencilla que veo para que no se produzca un colapso de las administraciones, porque no tiene sentido que tengamos que enviar una notificación cada vez que pedimos o enviamos un dato personal». http://www.elconfidencial.com/espana/2016-03-29/una-sentencia-europea-pone-los-embargos-de-hacienda-al-borde-de-la-legalidad_1175169/

[20]

Sobre su elaboración, Solar Calvo, P., «La doble vía europea en protección de datos», *Diario La Ley* , n.º 7832, Sección Doctrina, 4 de abril 2012; «La Protección de datos en la UE: Análisis y perspectivas de futuro», *Revista Aranzadi Unión Europea* (RUE), n.º 2, febrero, 2012.

[21]

Se trata de una importante oportunidad respecto de la que el sector de la privacidad discute intensamente si habrá necesidad de titulación.

http://noticias.juridicas.com/actualidad/noticias/11047-el-nuevo-reglamento-europeo-de-proteccion-de-datos:-un-texto-complejo-que-abre-nuevas-perspectivas-profesionales-a-la-abogacia/

[22]

Según el catedrático de Derecho Administrativo y ex director de la AEPD José Luis Piñar Mañas. Entrevista disponible en página arriba citada.

[23]

Como señalaron José López Calvo (ex subdirector general de Inspección de Datos), Javier Puyol (Socio de Ecix) y Borja Adsuara (Profesor y abogado).

Entrevista disponible en página arriba citada.

[24]

Describe el régimen actual de protección de datos personales incluidos en ficheros policiales en nuestro país, Solar Calvo, P., «Los datos personales en la investigación criminal», *Revista de la Guardia Civil* , n.º 817, Sección Formación, Mayo 2012; «Una perspectiva práctica de la Protección de Datos. La adaptación del Ministerio del Interior», *Diario la Ley* , n.º 7719, 20 de octubre de 2011.

[25]

Disponible en:

http://www.europarl.europa.eu/news/es/news-room/20160407IPR21776/reforma-de-la-protecci%C3%B3n-de-datos-%E2%80%93-nuevas-reglas-adaptadas-a-la-era-digital

© 2017 Revista Aranzadi de Unión Europea