LOS PRINCIPIOS RECTORES DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL Y SUS IMPLICACIONES EN EL PROCESO PENAL

The principles relating to processing of personal data and their implications for criminal proceedings

Por Juan Alejandro Montoro Sánchez[1]

Investigador Postdoctoral Margarita Salas. Universidad Pablo de Olavide de Sevilla. Instituto de Justicia y Litigación "Alonso Martínez" de la Universidad Carlos III de Madrid.
jamonsan@upo.es

Artículo recibido: 15/05/22 | Artículo aceptado: 19/07/22

RESUMEN

El presente trabajo aborda el estudio de los principios rectores del tratamiento de datos de carácter personal asociados al derecho fundamental a la protección de datos, desde la perspectiva del órgano judicial del orden penal, en tanto autoridad responsable del tratamiento de datos con fines de investigación y enjuiciamiento del delito. Se analizarán igualmente las principales implicaciones procesales que se derivan de su efectiva aplicación.

ABSTRACT

This paper analyses the fundamental right of data protection regarding its treatment by the criminal court, as the authority responsible for the processing of data for the purposes of investigation and prosecution of crimes. The main procedural implications deriving from its effective application will also be analyzed.

PALABRAS CLAVE

Derecho protección de datos, Principios rectores del tratamiento, Tratamiento de datos, Principio limitación de la finalidad, Proceso Penal.

KEYWORDS

Data Protection Right, Principles relating to processing of personal data, Processing of personal data, Purpose limitation principle, Criminal proceeding.

[1] Trabajo vinculado al Proyecto de Investigación de Excelencia del Ministerio de Economía y Competitividad "Límites a la utilización de datos, evidencias e información entre procesos y procedimientos diversos en España y la Unión Europea (LUDEI)".

Sumario: 1. Los principios rectores del tratamiento de datos de carácter personal. 2. Principios de licitud y lealtad. 2.1 Principio de licitud. 2.2 Principio de lealtad. 3. Principio de limitación de la finalidad del tratamiento. 4. Principio de minimización. 5. Principio de exactitud. 6. Principio limitación del plazo de conservación. 7. Principios de integridad y confidencialidad. 8. Principio de responsabilidad activa o proactividad. 9. Bibliografía.

1. Los principios rectores del tratamiento de datos de carácter personal

Bajo el paraguas del Capítulo II de la Directiva 2016/680/UE, que tiene como rúbrica "Principios" se proclaman y desarrollan toda una serie de reglas y fundamentos heterogéneos[2] sobre los que se articula básicamente todo el régimen jurídico protector del derecho fundamental a la protección de datos de carácter personal en el ámbito penal[3]. Estos principios vertebradores constituyen el núcleo básico de las obligaciones de toda autoridad responsable de un fichero, que deben ser observados minuciosa y diligentemente a lo largo de todas las fases del tratamiento[4], pues de su respeto y observancia depende, en gran medida, que se pueda garantizar adecuadamente a los interesados los poderes de

[2] APARICIO SALOM, J. La calidad de los datos. En TRONCOSO REIGADA, A. (dir.) *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. Madrid, Civitas, 2010, p. 324, alude a la heterogeneidad de los principios, si bien, todos ellos contribuyen a un fin común, garantizar los poderes de control y disposición que atribuye al interesado el derecho fundamental a la protección de datos sobre sus propios datos.

[3] Los primeros instrumentos jurídicos que fueron promulgados en la materia ya preveían una serie de principios básicos destinados a vertebrar los sistemas de protección de datos que configuraban. Las pioneras Resoluciones 22/73 y 29/74 del Consejo de Europa, referidas respectivamente a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos de los sectores privado y público proclamaron como principios informadores a la proporcionalidad, lealtad, licitud, finalidad, conservación y exactitud. De igual modo, el Convenio 108 dedicó sus arts. 4 a 7, comprendidos bajo su Título II sobre "Principios básicos para la protección de datos", a fijar sus fundamentos estructurantes. Por su parte, la Directiva 95/46/CE los reconoció en su art. 6 bajo la expresiva denominación de principios relativos a la calidad de los datos. Por ello, puede comprobarse como ha sido una constante la existencia de estos principios en los instrumentos convencionales y legales de la materia y su posición privilegiada, en tanto elementos rectores e inspiradores de los sistemas de protección de datos.

[4] Principios cuya observancia se debe procurar desde el mismo momento de la recogida de los datos hasta su supresión una vez concluya la finalidad para la que fueron recabados. Por lo tanto, el escrupuloso respeto de estos principios resulta esencial durante todas las fases o etapas del tratamiento y durante el desarrollo de cualquier actividad que se realice en la organización del responsable relacionada o vinculada al uso de los datos personales. TRONCOSO REIGADA, A. El principio de calidad de los datos. En TRONCOSO REIGADA, A. (dir.) *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. Madrid: Civitas, 2010, pp. 340-343.

control y disposición[5] sobre sus datos personales que atribuyen el derecho fundamental a la protección de datos reconocido tanto en el art. 18.4 CE[6] como en el art. 8 de la CDFUE y del CEDH.

Tradicionalmente denominados como principios relativos a la calidad[7] de los datos de carácter personal, consisten en una serie de directrices, prohibiciones y limitaciones estrechamente relacionadas y complementarias entre sí, que definen y condicionan la forma en la que los datos han de ser recabados y tratados con posterioridad por la autoridad responsable durante todo el ciclo de procesamiento[8]. Especialmente descriptiva de la función que están llamados a desempeñar es la definición recogida en la primigenia LORTAD[9], en la que se expresaba que éstos "…definen las pautas a las que debe atenerse la recogida de datos de carácter personal, pautas encaminadas a garantizar tanto la veracidad de la información contenida en los datos almacenados cuanto la congruencia y racionalidad de la utilización de los datos".

Son, por tanto, elementos de especial trascendencia para todos los operadores jurídicos implicados en el tratamiento[10], incluidas las autoridades de

[5] PUYOL MONTERO, J. Los principios del derecho a la protección de datos. En PIÑAR MAÑAS J. L. (dir.), *Reglamento general de protección de datos: hacia* un *nuevo modelo europeo de privacidad*. Madrid: Editorial Reus, 2016, p. 136.

[6] La STC 292/2000 de 30 de noviembre, concretó el contenido basilar del derecho fundamental a la protección de datos afirmando que "consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso".

[7] En el RGPD y en la Directiva 2016/680/UE se califican meramente como "principios", mientras la Directiva 95/46/CE siendo más expresiva de su cometido los denominó como "principios relativos a la calidad de los datos" tal y como se reflejaba en el título dado a la Sección 1ª del Capítulo II en los que se enmarcaban. Expresión que también fue trasladada a la derogada LOPD de 1999, pero que no se ha mantenido en su sucesora, la Ley Orgánica 3/2018, ni en la más reciente Ley Orgánica 7/2021.

[8] PALMA ORTIGOSA afirma que para garantizar el derecho a la protección de datos no basta con reconocer a los interesados el ejercicio de los derechos ARSOPOL, sino que es necesario imponer a los responsables una serie de obligaciones adicionales que hagan efectiva en toda su extensión la protección dispensaba por el derecho fundamental, lo cual se consigue a través del respeto debido a dichos principios vertebradores. Vid. PALMA ORTIGOSA, A. Principios relativos al tratamiento de datos personales. En MURGA FERNÁNDEZ, J. P., FERNÁNDEZ SCAGLIUSI M. A. y ESPEJO LERDO DE TEJADA, M. (dirs.), Protección de datos, responsabilidad activa técnicas de garantía. Madrid: Editorial Reus, 2018, pp. 39-40.

[9] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

[10] PUYOL MONTERO subraya la importancia de los principios vinculados a la calidad del siguiente modo: "porque los mismos han de servir de referencia a los operadores jurídicos que intervienen en la materia, a los efectos de que puedan cumplir de manera satisfactoria las

control que supervisan y controlan la adecuada aplicación de la normativa, pues se erigen en parámetros de referencia nuclear para la toma de decisiones en el seno de la organización y para garantizar una respuesta respetuosa con los derechos fundamentales a los interesados[11]. Incluso, es posible afirmar que actúan como auténticos principios informadores de la normativa, habida cuenta de que permiten extraer criterios con los que cubrir las lagunas normativas que puede surgir ante la ausencia de soluciones específicas que cubran supuestos de hechos controvertidos. Por su parte, para los interesados, estos principios actúan como variables de referencia permitiendo valorar la adecuación del tratamiento llevado a cabo por la autoridad, a las exigencias que dimanan del derecho a la protección de datos y su regulación.

Es el primero de los apartados del art. 4 de la Directiva 2016/680/UE, que tiene por título "Principios relativos al tratamiento de datos personales"[12], el precepto encargado de proclamar a los principios operantes en el sistema de protección de datos del ámbito penal. En particular, se reconocen como tales a los principios de licitud y lealtad; al principio de limitación de la finalidad del tratamiento; al principio de minimización de datos; al principio de exactitud; al principio de limitación del plazo de conservación; a los principios de integridad y confidencialidad y finalmente, al innovador principio de responsabilidad proactiva. Cabe mencionar que este precepto reproduce casi miméticamente los mismos principios enunciados en el Reglamento General de Protección de Datos, con la única excepción del principio de transparencia. Sin embargo, la falta de reconocimiento expreso en el articulado no empece que también resulte aplicable, habida cuenta de su reconocimiento explícito en el Considerando (26) de la Directiva[13], aunque ciertamente, la intensidad de su eficacia es de mucho menor calado que en el régimen general, dadas las particularidades que presentan las actividades públicas vinculadas al sistema de represión del delito que se enmarcan en este ámbito.

Dicho listado de principios rectores del tratamiento ha sido incorporado al ordenamiento nacional a través del art. 6.1 de la Ley Orgánica 7/2021, de 26 de

---

exigencias jurídicas y de responsabilidad social empresarial vinculadas a las nuevas exigencias y requerimientos derivados de la protección de datos de carácter personal". PUYOL MONTERO, J. Los principios del derecho a la protección de datos…. referencia 5 p. 136.

[11] APARICIO SALOM, J. La calidad de los datos... referencia 1 p. 335.

[12] Anteriormente en la LOPD y su reglamento de desarrollo sí se recogía expresamente la denominación de principios relativos a la calidad de los datos, en sus arts. 4 y 8 respectivamente.

[13] Puede comprobarse que el Considerando (26) de la Directiva exige que todo tratamiento de datos personales sometido al mismo, además de ser lícito y leal, debe de reputarse transparente en relación con las personas físicas afectadas. Fórmula idéntica a la utilizada en el Reglamento General de Protección de Datos, aunque en la Directiva dicho principio no se eleve a la categoría de vertebrador del tratamiento.

mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, norma interna con la que el legislador ha procedido a la transposición de la Directiva 2016/680/UE, con un retraso superior a los cuatro años.

Tras la lectura del elenco de principios, es posible advertir que el grueso de éstos se mantiene intacto respecto al repertorio previsto en el anterior régimen encabezado por la Ley Orgánica 15/1999[14], existiendo por tanto una vocación continuista respecto de los que podríamos tildar como principios arquetípicos del tratamiento de los datos de carácter personal. Sin embargo, es cierto que bien se ha previsto la incorporación de algún principio plenamente novedoso, como ha sucedido con el de responsabilidad proactiva, o bien se ha dado el caso de que elementos previamente vigentes en el orden anterior se han visto elevados expresamente al nivel de principios fundamentales de la materia, como sucede con los principios de integridad y confidencialidad.

A continuación, procede analizar individualmente a cada uno de estos principios al objeto de conocer su contenido, exigencias y alcance en lo que respecta al tratamiento de datos por parte de los órganos judiciales, en su condición de autoridades responsables del tratamiento, prestando especial atención a las implicaciones de índole procesal.

2. Principios de licitud y lealtad

Los primeros principios informadores del tratamiento de datos de carácter personal, se enuncian conjuntamente en el art. 4.1.a) de la Directiva 2016/680 y 6.1.a) de la Ley Orgánica 7/2021, al disponer este último que "Los datos personales serán tratados de manera lícita y leal"[15]. Nos hallamos ante dos principios consolidados y tradicionalmente incorporados en los textos

[14] La doctrina ha destacado el carácter continuista del legislador europeo respecto a los principios que se dispusieron en la Directiva 95/46/CE y consecuentemente, los reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vid. PUYOL MONTERO, J. Los principios del derecho a la protección de datos…. referencia 5, p. 137. Por su parte, PALMA ORTIGOSA, destaca, además, que, en el nuevo paquete normativo de 2016, el legislador europeo ha aclarado y sistematizado la regulación atinente a los principios rectores, añadiendo alguno de suma importancia como el de responsabilidad activa. Vid. PALMA ORTIGOSA, A. Principios relativos al tratamiento de datos personales… referencia 8 p. 40.

[15] Aunque la derogada LOPD no hacía mención a los mismos, el art. 8 del Reglamento LOPD fue la norma nacional encargada de proclamarlos. En concreto la disposición reglamentaria aún vigente, aunque inoperativa, establece que "Los datos de carácter personal deberán ser tratados de forma leal y lícita. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos". Ello en plena sintonía con lo preceptuado en la Directiva 95/46/CE, que en su art. 6.1 obligaba a los Estados miembros a disponer que los datos personales fueran tratados de manera leal y lícita.

convencionales más vetustos e importantes sobre la materia. No en vano, el Convenio 108, ya hacía referencia a los mismos al preceptuar que los datos personales "Se obtendrán y tratarán leal y legítimamente", mientras el art. 8 del CDFUE, determina que los datos "…se tratarán de modo leal (…) y sobre la base del consentimiento (…) o de otro fundamento legítimo previsto por la ley". Procede analizarlos de forma individualizada.

2.1 Principio de licitud

En el ámbito de aplicación del RGPD, el principio de licitud exige, en primer lugar, que cualquier tratamiento de datos que se efectúe por un responsable del tratamiento se ampare en una base legal habilitante de las enumeradas en su art. 6 y, en segunda instancia, que además dicho tratamiento se circunscriba en todo momento a las previsiones y obligaciones derivadas de la normativa reguladora del derecho a la protección de datos que resulte de aplicación.

Sin embargo, en el ámbito de la Directiva 2016/680/UE este principio presenta una serie de exigencias y connotaciones específicas que impiden equipararlos plenamente. Y ello se debe en gran medida, al hecho de que no nos situamos ante una norma que establezca un régimen jurídico garantista de vocación general que deba comprender cualquier actividad dirigida al tratamiento de datos, tal y como sucede con el RGPD, sino ante un régimen excepcional referido exclusivamente al tratamiento asociado a las actividades estatales vinculadas al sistema de represión penal, como acertadamente afirma GALÁN MUÑOZ[16].

En concreto, es el art. 8 de la Directiva 2016/680/UE el que conceptúa y configura a este principio rector. Y lo hace, obligando a los Estados miembros a

[16] GALÁN MUÑOZ habla de una doble vía europea de protección de los datos personales, distinguiendo entre "la vía garantista general, en orden a preservar ante la libre circulación de datos personales, los derechos de información, acceso, rectificación, cancelación y oposición; y, la vía excepcional o especial, la relacionada con la represión, la investigación y el enjuiciamiento del delito, que requiere un tratamiento especial en cuanto se trata de medios de investigación y obtención de fuentes probatorias preconstituidas y, en definitiva, de prueba de cargo en orden a la imposición de consecuencias jurídicas sancionadoras de naturaleza penal". Vid. GALÁN MUÑOZ, A. La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea. En COLOMER HERNÁNDEZ, I. (dir.) *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*. Cizur Menor: Aranzadi, 2015, pp. 43-44. En idéntico sentido, GONZÁLEZ CANO, M. I., Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680. En *Revista Brasileira de Direito Processual Penal*, vol. 5, núm. 3, 2019, Brasil, p. 1363 y SOLAR CALVO, P. La doble vía europea en protección de datos. En *Diario La Ley*, núm. 7832, 2012, España, p. 3.

que dispongan en su ordenamiento interno, que únicamente sea lícito "el tratamiento en la medida en que sea necesario para la ejecución de una tarea realizada por una autoridad competente, para los fines establecidos en el artículo 1, apartado 1[17], y esté basado en el Derecho de la Unión o del Estado miembro". Mandato que conecta y debe interpretarse a su vez con las directrices dispuestas en su Considerando (11), que disponen que "Para que sea lícito, el tratamiento de datos personales en virtud de la presente Directiva debe ser necesario para el desempeño de una función de interés público llevada a cabo por una autoridad competente en virtud del Derecho de la Unión o de un Estado miembro con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública"[18].

Así las cosas, la licitud del tratamiento de datos personales en el ámbito penal va a depender de la verificación conjunta de tres factores imprescindibles: 1) la contribución del tratamiento a alguno de los fines de la Directiva, como elemento teleológico; 2) la naturaleza del responsable, como factor subjetivo y; 3) la habilitación legal de la autoridad para el tratamiento, como factor legitimador. Dicho, en otros términos, el tratamiento de datos será lícito, en tanto se circunscriba a alguno de los fines referidos al ámbito de aplicación de la Directiva y se acometa por una autoridad competente habilitada legalmente para el tratamiento de datos a tales efectos[19].

De este modo, la finalidad del tratamiento debe coincidir necesariamente con alguna de las señaladas en el primero de los preceptos de la Directiva, y que se relacionan con el ámbito penal y la seguridad pública, recordemos nuevamente: la prevención, investigación, detección o enjuiciamiento de

[17] Tales fines son, de acuerdo con dicho precepto, la "prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública".

[18] Puede rechazarse de plano que el consentimiento, en los términos exigidos en el RGPD, pueda constituir un fundamento para el tratamiento por las autoridades competentes, pues como reza el Considerando (35) de la Directiva: "En este caso, el consentimiento del interesado [según se define en el Reglamento (UE) 2016/679] no constituye un fundamento jurídico para el tratamiento de los datos personales por las autoridades competentes. El ejercicio de las funciones de prevención, investigación, detección o enjuiciamiento de infracciones penales que la legislación atribuye institucionalmente a las autoridades competentes permite a estas exigir u ordenar a las personas físicas que atiendan a las solicitudes que se les dirijan. Cuando se exige al interesado que cumpla una obligación jurídica, este no goza de verdadera libertad de elección, por lo que no puede considerarse que su respuesta constituya una manifestación libre de su voluntad".

[19] Véase que el mandato establecido en el art. 8 de la Directiva 2016/680/UE se ha materializado en el art. 11 de la Ley Orgánica 7/2021, disponiéndose que "El tratamiento sólo será lícito en la medida en que sea necesario para los fines señalados en el artículo 1 y se realice por una autoridad competente en ejercicio de sus funciones".

infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Por tanto, se exige del tratamiento que sea necesario o coadyuve a la consecución de alguno de esto fines, o dicho de otro modo, que se lleve a cabo en el marco de alguna de dichas actividades públicas, puesto que únicamente en tal medida, puede colmarse la primera de las exigencias del principio de licitud.

Por otro lado, no puede obviarse, que todas y cada una de las actividades que integran el ámbito de la Directiva, constituyen por sí mismas el ejercicio de una función de interés público general, tal y como exige el precitado Considerando (11) Directiva 2016/680/UE. Y ello porque contribuyen a la consecución de intereses colectivos o supraindividuales[20] como la aplicación del *ius puniendi* por el Estado y el mantenimiento de la libertad y seguridad públicas[21].

El segundo de los requisitos de licitud lo constituye la identificación del responsable con la de una autoridad competente, únicos sujetos legitimados para tratar datos de carácter personal con alguno de los fines penales que abarca la Directiva. De acuerdo con las definiciones dispuestas en el apartado 7º de su art. 3, tienen dicha consideración: las autoridades públicas competentes para alguno de los fines del art. 1, así como cualquier otro órgano o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas con alguno de los fines de la norma[22]. Vista la primera

[20] La jurisprudencia del TJUE ha declarado que la lucha contra el terrorismo y frente a otros delitos especialmente graves para el mantenimiento de la paz y la seguridad son objetivo de interés general de la Unión. En este sentido, las sentencias Tribunal de Justicia de la Unión Europea, caso Kadi y Al Barakaat International Foundation/Consejo y Comisión (C-402/05 P y C-415/05 P), 3 de septiembre de 2008, apartado 363, y caso Al-Aqsa/Consejo (C-539/10 P y C-550/10 P), 15 de noviembre de 2012, apartado 130.

[21] MORENO CATENA, V. y CORTÉS DOMÍNGUEZ, V. *Derecho Procesal Penal.* Valencia: Tirant Lo Blanch, 2021, p. 13, consideran al "proceso penal como el instrumento último de la política pública de seguridad y además como medio de reparación de las víctimas". En idéntico sentido, RÍO LABARTHE, G. El proceso penal. Funciones. En ASENSIO MELLADO, J. M. (dir.) *Derecho procesal penal.* Valencia: Tirant Lo Blanch, 2020, p. 27. El TC sitúa a la persecución y castigo del delito como bienes constitucionalmente protegibles y de interés público pues a través de ellos "…se defienden otros como la paz social y la seguridad ciudadana. Bienes que igualmente reconocidos en los arts. 10.1 y 104.1 CE. Al respecto las SSTC 292/2000 de 30 de noviembre FJ 6º; 166/1999, de 27 de septiembre, FJ 2º; y 127/2000, de 16 de mayo, FJ 3º. El TJUE también ha declarado que la lucha contra la delincuencia grave es esencial para garantizar la seguridad pública y libertad garantizada en el art. 6 de la CDFUE. Véase la sentencia, caso Tsakouridis (C-145/09), de 23 de noviembre de 2010, apartados 46 y 47.

[22] El art. 4 de la Ley Orgánica 7/2021 reputa como autoridades competentes a las Fuerzas y Cuerpos de Seguridad; las Administraciones Penitenciarias; la Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria; al Servicio Ejecutivo de la

definición y habida cuenta de su competencia para la investigación de los hechos criminales en la fase de instrucción[23] y posterior enjuiciamiento y ejecución de penas, es indiscutible que los órganos judiciales del orden penal pueden reputarse como autoridades competentes a efectos de la Directiva. En cualquier caso, tal catalogación se confirma expresamente, despejando cualquier duda que pudiera suscitarse, en el segundo de los apartados del art. 4 de la Ley Orgánica 7/2021[24].

En último lugar, cabe examinar al último de los presupuestos que son exigidos por la Directiva 2016/680/UE para determinar la licitud y que se concreta en la reserva de ley habilitante para el tratamiento de datos. Es decir, la exigencia de que la autoridad esté expresamente habilitada en el ordenamiento interno para tratar datos de carácter personal con alguno de los fines amparados por la Directiva. Requisito que viene motivado por la necesaria adecuación de una medida restrictiva de derechos fundamentales a los cánones y parámetros de proporcionalidad y necesariedad establecidos en la CDFUE y la jurisprudencia del TEDH[25]. Y es que no debe obviarse, que toda recogida y/o posterior tratamiento de datos por una autoridad competente supone una injerencia en el derecho a la vida privada de las personas y a la protección de sus datos de carácter personal tal y como ha reiterado el TJUE en su jurisprudencia[26].

Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y a la Comisión de Vigilancia de Actividades de Financiación del Terrorismo.

[23] Véase al respecto los apartados 1º y 2º del art. 303.1 LECrim, que encomiendan la formación del sumario, a los jueces de instrucción. Tales preceptos deben ponerse en correspondencia con las reglas de atribución de competencia establecidas en la LOPJ, especialmente sus arts. 57, 61, 73.3, 87 y 87 *ter*. Únicamente en el ámbito del derecho penal del menor, dicha labor corresponde al Ministerio Fiscal según lo previsto en la Ley Orgánica 5/2000.

[24] Este reza que "También tendrán consideración de autoridades competentes las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal".

[25] FRÍAS MARTÍNEZ, E. Obtención de datos personales en procesos penales y administrativos. En *Diario La Ley*, núm. 9404, 2019, España, explica que se trata de una consecuencia de la exigencia plasmada en el art. 8.2 CEDH y que, en su virtud, "solamente podrá haber recogida y tratamiento de datos en aquellos supuestos en los que exista una ley habilitante, que se hagan para una investigación o con finalidad concreta y no prospectiva y sean proporcionados a la misma".

[26] Las sentencias del Tribunal de Justicia de la Unión Europea, caso Schwarz (C-291/12), de 17 de octubre de 2013, apartado 25, y caso Digital Rights Ireland y otros (C-293/12 y C-594/12), de 8 de abril de 2014, apartado 36, recogen la doctrina jurisprudencial por la que se considera que se produce una injerencia los derechos a la protección de datos de carácter personal por el mero hecho de que un responsable trate datos personales, y ello con independencia de la operación en que consista éste, al expresar que "Dichas operaciones [comunicación, acceso, etc.] son asimismo constitutivas de una injerencia en el derecho fundamental a la protección de datos de carácter personal garantizado por el artículo 8 de la Carta, puesto que constituyen tratamientos de datos de carácter personal". Dicha doctrina se confirma de modo específico, en lo que respecta a las autoridades competentes del orden penal en la sentencia del Tribunal de Justicia de la Unión

En el ámbito nacional, el fundamento legal primario que habilita a los órganos judiciales para el tratamiento de datos de carácter personal se encuentra implícito en el art. 117.3 CE[27], precepto que atribuye en exclusiva a los jueces y magistrados el ejercicio de la potestad jurisdiccional, siendo el procesamiento de datos una actividad inherente e inescindible de dicha función. No obstante, la habilitación específica para el tratamiento de datos en el desarrollo de estas funciones, y particularmente en lo que respecta al orden jurisdiccional penal, se halla en los apartados 2º y 3º del art. 236 ter LOPJ. Preceptos que genéricamente autorizan a los órganos judiciales del orden penal a tratar datos personales para el ejercicio de las funciones y potestades encuadrables en dicho orden jurisdiccional. No obstante, de modo adicional es posible localizar en la legislación procesal, o incluso en otras leyes especiales del ordenamiento jurídico, habilitaciones específicas para la utilización de ciertas categorías de datos, principalmente, con motivo de la regulación de determinadas actuaciones judiciales o medidas de investigación, que llevan aparejadas la aprehensión o recogida de datos. Piénsese en todas aquellas medidas de investigación limitativas de derechos fundamentales, especialmente las de índole tecnológica introducidas por en la LECrim por la Ley Orgánica 14/2015, que fueron incorporadas en sus arts. 588 bis a 588 octies, como son el registro de dispositivos de almacenamiento masivo, la utilización de dispositivos de geolocalización para el seguimiento o la cesión de datos de tráfico por los operadores de comunicaciones electrónicas, medida cuya regulación se complementa con las disposiciones establecidas en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

En cualquier caso, debemos tener presente, que las habilitaciones genéricas establecidas en favor de los órganos judiciales que legitiman la obtención y uso de datos con fines penales, no amparan el procesamiento de cualquier modalidad de dato de carácter personal. Al contrario, hay ciertas

---

Europea, caso Ministerio Fiscal (C-207/16), 2 de octubre de 2018, en cuyo parágrafo 51 se expresa que "En cuanto a la existencia de una injerencia en los derechos fundamentales, procede recordar que (…) el acceso de las autoridades públicas a estos datos constituye una injerencia en el derecho fundamental al respeto de la vida privada, consagrado en el artículo 7 de la Carta, incluso a falta de circunstancias que permitan calificar esta injerencia de «grave» y sin que sea relevante que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia. Tal acceso también constituye una injerencia en el derecho fundamental a la protección de los datos personales garantizado por el artículo 8 de la Carta, puesto que constituye un tratamiento de datos personales [véase, en este sentido, el Dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 124 y 126 y jurisprudencia citada]".

[27] DELGADO MARTÍN, J. Reflexiones sobre la protección de datos personales en la Administración de Justicia. En *Diario La Ley*, núm. 9363, 2019, España, p. 4.

categorías de datos, que por su naturaleza y la especial capacidad que presentan para revelar aspectos nucleares sobre la vida privada de las personas, requieren que la autoridad competente, cuente con una base legal específica legitimadora del tratamiento. Nos referimos a los denominados tradicionalmente como datos sensibles o pertenecientes a categorías especiales, tal y como se denominan en la más reciente legislación europea. Bajo esta denominación se encuadran, por ejemplo, los datos que revelen el origen étnico o racial del interesado; sus opiniones políticas, convicciones religiosas o filosóficas o la afiliación sindical; y los datos genéticos y biométricos, y los relativos a la salud o a la vida sexual. La utilización de estas modalidades de datos que gozan de una protección privilegiada requiere ineludiblemente que la autoridad responsable cuente con una autorización legal específica en el derecho interno para el uso específico de tales datos, tal y como se menciona en el art. 10 de la Directiva 2016/680/UE y en el art. 13.1 de la Ley Orgánica 13/2021[28]. Por ello, la licitud del tratamiento de datos de tal naturaleza por un órgano judicial, dependerá de que cuente con una base con rango de ley que lo autorice expresamente a su tratamiento, de lo contrario únicamente, podrá reputarse lícito cuando resulte necesario para proteger los intereses vitales de una persona o cuando los datos se hubieran hecho manifiestamente públicos por el interesado, como prevén los preceptos previamente citados.

2.2 Principio de lealtad

Además de ser lícito, todo tratamiento de datos debe ser leal, esto es, ser respetuoso con el principio de lealtad. Este presupuesto implica, en términos generales, que el tratamiento debe efectuarse por el órgano judicial en consonancia con las exigencias derivadas del principio general de la buena fe, al que se encuentra íntimamente ligado.

Tales condicionantes repercutirán al tratamiento de datos personales desde una doble perspectiva. En primera instancia, desde una posición subjetiva que se traducirá en la necesaria confianza en la apariencia y en la ausencia de dolo que deben resultar de la autoridad mientras se prolongue el tratamiento. Ello implica que el interesado cuyos datos vayan a ser tratados debe esperar del órgano judicial que toda su actuación se encamine a garantizar los principios, derechos y garantías que la ley le reconoce[29]. Ello se compadece con la función de

[28] Ejemplos de dichas habilitaciones específicas las encontramos en el art. 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica para el acceso al historial clínico o en el art. 95.1 de la Ley General Tributaria, respecto a los datos con trascendencia fiscal que conservan las Administraciones.

[29] Muy expresiva de esta dimensión es el art. 6.1 de la Propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad , en relación con el

garante de los derechos fundamentales que cumplen los jueces y magistrados, especialmente durante la fase de instrucción.

En segundo lugar, el principio de la lealtad se manifiesta desde una perspectiva objetiva en la observancia de unas reglas de conducta social que imponen a la autoridad responsable un determinado comportamiento ético en su relación jurídica con el interesado, en la que deberán destacar especialmente la honradez y rectitud[30]. Se trata, en definitiva, de evitar que la autoridad responsable pueda ejecutar operaciones de tratamiento de datos personales a espaldas del interesado, ya fuere de forma engañosa, prospectiva, clandestina, subrepticia o encubierta. Al contrario, el principio de lealtad persigue que el interesado deba tener constancia fehaciente, clara e inequívoca de que sus datos van a ser tratados, para qué concretos fines y bajo qué condiciones[31], debiendo la autoridad contribuir activamente a la consecución de este objetivo, primordialmente a través del cumplimiento del deber de prestar información[32]

---

tratamiento de datos de carácter personal, acogida favorablemente por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009 en Madrid, que en referencia a al principio de lealtad estableció que "Los tratamientos de datos de carácter personal se deberán realizar de manera leal, respetando la legislación nacional aplicable y los derechos y libertades de las personas, de conformidad con lo previsto en el presente documento y con los fines y principios de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos".

[30] Este aspecto objetivo de la buena fe se traduce en una exigencia de rectitud, lealtad y honradez en el trato, que la ética social aprueba y considera como razonablemente exigibles. Por tanto, la lealtad "debe presidir con carácter general la actuación individual del responsable del fichero, siendo un parámetro objetivo que debe ser tenido en cuenta a la hora de valorar su conducta respecto al cumplimiento de sus obligaciones". Vid. ATAZ LÓPEZ, J. La buena fe contractual. En Bercovitz RODRÍGUEZ-CANO, R., MORALEJO IMBERNÓN, N. y QUICIOS MOLINA, M. S. (coord.) *Tratado de los Contratos*. Valencia, Tirant Lo Blanch 2009, p. 167. En el mismo sentido PALMA ORTIGOSA, A. Principios relativos al tratamiento de datos personales referencia 8, p. 49.

[31] Esta dimensión informativa del principio de lealtad ha sido reconocida tanto por la AEPD como por la jurisprudencia. Por ejemplo, en las resoluciones recaídas en los procedimientos E/01490/2016, PS-00275-2016 y AAPP-00044-2015 la autoridad de control declaró que el principio de lealtad "se encuentra en el prestar una información adecuada al afectado o interesado, de forma que conozca el alcance real del consentimiento que presta". Por su parte, la sentencia de la Audiencia Nacional de 13 septiembre 2002, destacó que "(...) el tratamiento de datos no debe ser solamente legal, sino también leal, e implícito en dicho deber de lealtad se encuentra el de prestar una información adecuada al afectado o interesado, de forma que conozca el alcance real del consentimiento que presta".

[32] Es patente que el principio de lealtad se encuentra inexorablemente vinculado al derecho/deber de información, puesto que este es el medio principal por el que el interesado adquiere constancia, no solo de la inminencia o preexistencia de un tratamiento de sus datos, sino de sus características, fines, de las circunstancias del responsable y de los medios de impugnación. Por ello, el Considerando (42) de la Directiva 2016/680/UE preceptúa que, a fin de garantizar un tratamiento leal "Debe informarse al interesado, como mínimo, de lo siguiente: la

completa y veraz en los términos planteados en el art. 13 de la Directiva 2016/680/UE y 21 Ley Orgánica 7/2021. Todo ello sin perjuicio de los supuestos legalmente establecidos en que el órgano judicial pueda retrasar o limitar el cumplimiento de dicho deber en aras de no perjudicar la investigación en curso.

Por lo expuesto, la lealtad se erige en un estándar jurídico de obligada observancia a toda la actividad vinculada al tratamiento de datos llevada a cabo por la autoridad judicial, implicando de manera genérica, que su propia actuación tenderá a garantizar las exigencias derivadas del derecho a la protección de datos en favor de los interesados[33], absteniéndose de efectuar cualquiera de las actividades comprendidas en el tratamiento de datos personales mediante prácticas engañosas, fraudulentas o ilícitas[34] o que puedan generar un efecto negativo o injustificado[35].

3. Principio de limitación de la finalidad del tratamiento

El siguiente de los principios informadores vinculados al derecho a la protección de datos es el denominado como principio de limitación de la finalidad del tratamiento. Se trata de un principio esencial que podría calificarse como la clave de bóveda del sistema protector del derecho a la protección de datos. Se reconoce en el art. 4.1.b) de la Directiva 2016/680/UE y en el ámbito interno ha sido transpuesto a través del art. 6.1.b) Ley Orgánica 7/2021 bajo la fórmula: "Los datos personales serán recogidos con fines determinados,

identidad del responsable del tratamiento, la existencia de la operación de tratamiento, los fines del tratamiento, el derecho a presentar una reclamación y el derecho a solicitar al responsable del tratamiento el acceso a los datos personales, su rectificación o supresión, o la limitación de su tratamiento (…) Además, en determinados casos y con el fin de permitir que ejerza sus derechos, debe informarse al interesado de la base jurídica en la que se fundamenta el tratamiento y del período durante el que se conservarán los datos, siempre que dicha información adicional resulte necesaria y habida cuenta de las circunstancias concretas en que se produce el tratamiento de los datos…".

[33] En sentido similar se pronuncia el art. 15.2 de los Estándares de Protección de Datos para los Estados Iberoamericanos, al establecer que "el responsable tratará los datos personales en su posesión privilegiando la protección de los intereses del titular y absteniéndose de tratar éstos a través de medios engañosos o fraudulentos". Asimismo, la LOPD y el RLOPD, prohibían expresamente "la recogida de datos por medios fraudulentos, desleales o ilícitos" ex art. 4.7 y 8.1 respectivamente.

[34] En sentido contrario, una actuación desleal, podría considerarse aquella seguida en el tratamiento de datos personales que den lugar a una discriminación injusta o arbitraria contra los titulares, como señala el criterio interpretativo incluido en el art. 15.1 de los Estándares de Protección de Datos para los Estados Iberoamericanos.

[35] PALMA ORTIGOSA, A. Principios relativos al tratamiento de datos personales… referencia 8, p. 49, colige que de este precepto debe derivarse una actitud honesta y abierta del responsable respecto a los datos que tratando de no causar efectos negativos en los interesados.

explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines".

Debe partirse de que la recogida de cualquier dato personal - ya sea directamente del propio interesado o de otra fuente alternativa- y su posterior tratamiento deben obedecer, necesariamente, a la consecución de uno o varios fines perfectamente definidos. Es decir, el procesamiento de datos por la autoridad judicial es viable cuando se constituya como condición indispensable –ya sea principal o accesoria- para la obtención de un propósito circunscrito necesariamente al ámbito de aplicación de la Ley Orgánica 7/2021. Por tal motivo, se excluye la posibilidad de llevar a cabo la utilización de datos que no contribuyan o coadyuven a la consecución de unos propósitos concretos, como pudiera ser la mera acumulación gratuita o prospectiva de datos, actuaciones vedadas igualmente por el principio de especialidad proclamado en el art. 588 bis a) LECrim.

El concepto teleológico de fines o finalidad que se contempla en la Directiva 2016/680/UE – e igualmente en la Ley Orgánica 7/2021- adquiere en este ámbito mayores connotaciones que el incorporado en el RGPD. Concretamente, dicho concepto opera con dos sentidos distintos que resulta imprescindible distinguir a efectos de dilucidar el alcance y efectos del principio rector. Por un lado, podemos distinguir a los fines en sentido amplio, con los que se alude de forma genérica a los fines de interés general y actividades propias de las autoridades competentes que determinan el ámbito de aplicación de la Directiva. Esto es, a los fines que son propios de las autoridades competentes en virtud de las competencias genéricas que le son atribuidas *ope legis* y que sirven de fundamento legal a la licitud del tratamiento, a saber: fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

Y de otro lado, los fines entendidos de forma específica o concreta. Es decir, al particular cometido que desarrolla la autoridad responsable al que se dirige el tratamiento de datos. Por ello, estos fines coincidirán con un concreto delito o riesgo para la seguridad pública que se pretende prevenir, atajar, investigar o enjuiciar. Pues bien, consideramos que es ésta última concepción del término "fines" a la que se refiere necesariamente el principio de limitación de la finalidad del tratamiento, pues es la única interpretación que resulta coherente de un análisis sistemático de la Directiva y especialmente de sus objetivos[36].

[36] Esta diferenciación se deduce especialmente de los Considerando (26) y (29) en relación con el art. 4.2 Directiva 2016/680/UE. Pues se observa como utiliza fines en sentido genérico y fines específicos con distinto sentido. Uno para referirse a los fines previstos en ley y otra para los fines específicos a los que obedezca el tratamiento por lo que deben determinarse con carácter

Estando analizando en este trabajo, de modo específico el tratamiento de datos por los órganos judiciales pertenecientes al orden penal, es posible concretar que: cuando éstos procesen datos personales, lo harán exclusivamente y en la medida en que sea necesario para la consecución de unos fines específicos, que se enmarquen, a su vez, dentro de unos fines generales. Por ejemplo, un Juzgado de Instrucción recopila y procesa datos para investigar (fines generales) un delito de robo cometido por A.A.A. frente a B.B.B (fines concretos). O un Juzgado de lo Penal recibe del Juzgado de Instrucción el anterior expediente del delito de robo (fines concretos), para ser enjuiciado (fines genéricos).

Si bien la atribución de la competencia a las autoridades para la realización de los fines genéricos en los que se enmarca el tratamiento de datos se prefijan a través de la ley, los fines concretos, se definen por la propia autoridad competente, generalmente, con carácter previo a la hora de obtenerse los datos. En el caso de los órganos judiciales mediante el dictado de la oportuna resolución que bien incoa la fase de instrucción o bien mediante la resolución de apertura del juicio oral. Fijados estos fines específicos, el tratamiento de los datos debe someterse con exclusividad a los mismos, hasta el punto de erigirse en un límite, *a priori,* infranqueable durante todo el ciclo de vida de los datos[37]. Por consiguiente, es imprescindible que el órgano judicial delimite de antemano y con suficiente precisión, los fines a los que se destinaran los datos personales que se requieran obtener durante la instrucción, hasta el punto de que dicha determinación se erige en una suerte de autovinculación que impide, salvo bajo determinadas circunstancias extraordinarias, alterar o extender el ámbito finalista del tratamiento. Entre dichas causas, podemos señalar, por ejemplo, el descubrimiento de delitos conexos a los inicialmente investigados o de hallazgos casuales, pero al margen de estos supuestos, la mutación del destino de los datos queda proscrita en virtud de dicho principio.

De lo anterior, se deriva la necesidad de que los fines a los que responda el tratamiento sean explícitos, esto es que se expresen de una manera clara, transparente, determinante, unívoca y que sean puestos en conocimiento del interesado a través de los cauces informativos previstos –tanto en la legislación procesal como en la sectorial de protección de datos-, sin que proceda la persecución de otros fines encubiertos, solapados o ambiguos[38]. Igualmente, y

previo a su recopilación. Debiendo ser adecuados y no excesivos, lo que exige una valoración respecto a los fines específicos, no es posible *ex ante*, al menos en el plano penal, la delimitación de los datos que pueden servir para la tramitación de un proceso penal, sino que dependerá en exclusiva de las circunstancias y particularidades que resulten del asunto.

[37] TRONCOSO REIGADA, A. El principio de calidad de los datos… referencia 4, p. 344.

[38] Lo determinante es que al interesado no le queden dudas de la concreta y exacta finalidad para la que se destinarán sus datos personales y que dará lugar al tratamiento, pues esta

como regla complementaria y delimitadora de las anteriores, se exige que los fines perseguidos por la autoridad judicial responsable respondan al principio de legitimidad. Esto implica en primer lugar que los fines para los cuales se recaban los datos personales deben ser lícitos, esto es, que la finalidad a la que se destinan los datos debe estar amparada por la ley[39]; y en segunda instancia, que la autoridad debe estar legitimada para la realización de la misma[40]. Por tanto, todo tratamiento de datos cuya finalidad sea contraria a las normas o para la que no esté amparada la autoridad será ilegítima y vulnerará el presente principio, incluso, cuando los datos pudieran resultar adecuados a la finalidad.

Sin perjuicio lo anterior, lo cierto es que, el principio de limitación de la finalidad habilita de forma directa y automática y sin requisito adicional a una autoridad responsable a tratar datos para nuevos fines, cuando éstos no resulten incompatibles con los previos. Véase como el precepto que proclama este principio, prevé *in fine* que "[los datos] no serán tratados de forma incompatible con esos fines", máxima que, interpretada a *sensu contrario*, infiere su destino a usos compatibles.

Bajo nuestro parecer, la compatibilidad resultará cuando la nueva finalidad se utilice como complemento necesario a la finalidad originaria específica. Dicho en otros términos, se reputa compatible el destino de los datos a las sucesivas fases que integran el proceso penal, entendido éste en sentido lato. De este modo, siempre que los datos se dediquen a nuevos fines de los generales plasmados en el art. 1 de la Directiva 2016/680/UE, más vinculados, derivados y accesorios o complementarios a los fines específicos existirá compatibilidad de usos. Por

claridad permite el ejercicio de las facultades de control y disposición con plenitud. PALMA ORTIGOSA, A. Principios relativos al tratamiento de datos personales… referencia 8, p. 44. Por tal motivo TRONCOSO REIGADA considera que es contraria a este principio la determinación de finalidades vagas, inconcretas o excesivamente generales, aunque ésta fueran legítimas. TRONCOSO REIGADA, A. El principio de calidad de los datos… referencia 4, p. 345. APARICIO SALOM, clarifica esta concepción amplia de la finalidad, distinguiendo a la finalidad de las actuaciones concretas que se desarrollen en ejecución de la actividad. APARICIO SALOM, J. La calidad de los datos… referencia 1, p. 329.

[39] El término ley deberá de ser interpretado en sentido amplio, como cualquier disposición del ordenamiento jurídico que faculte, permita o ampare una concreta actividad para la que se desarrolle el tratamiento de datos. Vid. PALMA ORTIGOSA, A. Principios relativos al tratamiento de datos personales… referencia 8, p. 44. TRONCOSO REIGADA añade que para que una finalidad sea legítima, debe de ajustarse en primer lugar a la Constitución y posteriormente a la ley. VID. TRONCOSO REIGADA, A. El principio de calidad de los datos… referencia 4, p. 345

[40] Legitimidad por tanto referida al sujeto respecto a los fines. TRONCOSO considera que este requisito se cumpliría para personas jurídicas privadas si las finalidades de tratamiento de datos se encuadran el objeto social o la actividad que desarrolla habitualmente, mientras que, en el supuesto de los entes públicos, es imprescindible que la finalidad responda a una competencia previamente otorgada por el ordenamiento, identificándose el principio de finalidad con los principios de competencia y de reserva.

ejemplo, cuando los datos sean recopilados por una autoridad policial para la investigación preprocesal, podrán ser cedidos al órgano judicial de instrucción para el desarrollo de la instrucción y, a su vez, éstos podrán ser cedidos al juzgado de lo Penal o Audiencia Provincial para el enjuiciamiento, para finalmente ser comunicados al juzgado de Vigilancia Penitenciaria para la ejecución de la pena. Puede verse como, a pesar de sucederse varias comunicaciones de datos entre diferentes responsables y destinarse a varios fines genéricos – investigación policial, investigación judicial, enjuiciamiento y ejecución- todos ellos guardan relación con los fines específicos que dieron lugar al tratamiento inicial en el ámbito de la Directiva. Sin embargo, cuando unos datos fueron obtenidos inicialmente para la investigación o enjuiciamiento de unos hechos específicos y, posteriormente se ceden por el órgano judicial a fin de investigar o enjuiciar otros delitos ni siquiera conexos, se estaría produciendo un tratamiento incompatible, no amparado por el principio de limitación de la finalidad.

Ahora bien, la Ley Orgánica 7/2021 también establece excepciones de carácter relativo a este límite, a fin de permitir a una autoridad competente o incluso a una tercera, previa cesión, el tratamiento de los datos personales a otros fines específicos. Es decir, datos personales que son procesados por una autoridad competente para alguno de los fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública respecto a unos hechos delictivos específicos, podrán ser destinados por esta a cualquiera de estos fines respecto a otros delitos o incluso ser comunicados a una tercera autoridad para que actúe en tal sentido. Posibilidad que también se contempla actualmente en los arts. 579 bis y 588 bis i) LECrim para los datos obtenidos por órganos judiciales. Aquí pues, sí que nos situamos ante una auténtica excepción al principio de finalidad, puesto que los fines que motivan el tratamiento se expanden y mutan necesariamente en su concepción específica, pudiendo afectar en el mismo sentido a su dimensión genérica.

Ahora bien, a pesar del contenido de este último precepto, las autoridades competentes no se encuentran legitimadas para ampliar o transmutar los fines del tratamiento en cualquier caso en que consideren que puede resultar útil para el ejercicio de las competencias que legalmente le sean atribuidas. La Directiva se encarga expresamente de limitar estas actuaciones, imponiendo requisitos que únicamente posibiliten la expansión del tratamiento cuando ello obedezca a situaciones de necesidad justificadas y sometidas a criterios de proporcionalidad. Por tanto, los señalados preceptos de la LECrim deben interpretarse conforme a las reglas establecidas en la Directiva y Ley Orgánica 7/2021, al menos, cuando

los medios de investigación o de prueba que se pretenden ceder, consistan en datos de carácter personal.

Es el art. 4.2 de la Directiva – y 6.3 de la Ley Orgánica 7/2021- el que establece la regla excepcional al principio de limitación de la finalidad que permite a las autoridades competentes que puedan destinar los datos, por sí mismas o a una tercera, previa cesión, para su utilización en unos fines penales distintos y desconectados de los que motivaron su uso. Es decir, lo que la normativa legitima, es ni más ni menos, el empleo de datos que se recogieron a efectos de ser utilizados con relación a un delito, con respecto a otro delito distinto. En cualquier caso, para que esta cesión de datos se repute legítima, habida cuenta de la pérdida de ineficacia que se deriva para el principio de limitación, se requiere que concurran acumuladamente los siguientes requisitos.

En primer lugar, que la autoridad que dedique los datos a una nueva finalidad esté legitimada, mediante ley, para desarrollar la actividad a la cual se destinan los datos. Es decir, la legislación del Estado miembro debe atribuir el ejercicio de competencias penales a la autoridad para el desarrollo de los fines genéricos a los que se destinan y de la que se derive la necesidad de tratamiento de datos[41]. Por ejemplo, cuando con motivo de un hallazgo casual, un Juzgado de Instrucción comunica los datos a otro órgano judicial de idéntica naturaleza, a efectos de que se despliegue la investigación, es imprescindible, que el cesionario de los datos esté legitimado por ley para la investigación del delito y, además, ostente competencia. Tal exigencia deriva de la garantía de reserva de ley de aquellas actividades que supongan una merma o limitación de aspectos esenciales de un derecho fundamental, como sucede en este caso con el derecho a la protección de datos.

En segundo lugar, el nuevo tratamiento pretendido debe ser necesario y proporcionado con relación a los nuevos fines. Es decir, no basta entonces con que la legislación atribuya a una autoridad la competencia genérica para ejercer ciertas funciones vinculadas a alguno de los fines del art. 1.1 de la Directiva y que exija, a su vez, el tratamiento de datos personales. Sino que atribuida *ex lege* la competencia, el ejercicio puntual de ésta que abarque nuevos usos o cesiones para finalidades distintas que se pretendan llevar a cabo, deberá superar individualmente el estricto filtro de un juicio de proporcionalidad. Es decir, en el ámbito que nos ocupa, cada cesión de datos para un nuevo uso, deberá ser sometida *ex ante* por la autoridad cedente a un examen de adecuación a los criterios de necesidad, proporcionalidad y aquellos otros condicionantes adicionales que la legislación procesal pueda plantear.

4. Principio de minimización

[41] Considerando (29) Directiva 2016/680/UE.

El principio de minimización[42] de los datos, se establece de forma idéntica en los arts. 4.1c) Directiva 2016/680/UE y 6.1.c) de la Ley Orgánica. En su virtud, los datos personales que se traten por una autoridad penal deben de ser "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados[43]". Como puede comprobarse, mediante este principio se persigue minimizar, en la medida de lo posible, el número de datos personales que se tratan con relación a una concreta finalidad. Por ello, la autoridad debe de ceñirse, de modo estricto, a la recopilación y utilización de aquellos datos imprescindibles que posibiliten lograr la finalidad perseguida. De esta manera, se consigue reducir el riesgo de afección sobre aquella parcela de dato personales superfluos que se evitan ser tratados[44]. Se trata, por tanto, de una limitación que afecta a la actividad que desarrolla la autoridad responsable, tanto a nivel cuantitativo como cualitativo[45].

La primera regla que deben cumplir los datos personales que se utilicen para un tratamiento de datos por mor de este principio básico del derecho a la autodeterminación informativa son las de adecuación[46] y pertinencia[47]. Elementos que implican en primer lugar que los datos deben ser apropiados para el tratamiento y además tener cierta relevancia[48] para el alcance del fin perseguido respectivamente.

---

42 TRONCOSO REIGADA, A. El principio de calidad de los datos… referencia 4, p. 344 y PUYOL MONTERO, J. Los principios del derecho a la protección de datos… referencia 5, p. 138, denominan a este principio como de adecuación.

43 Dicha regla puede considerarse análoga a la de proporcionalidad prevista en la derogada LOPD. Esta obligaba al responsable a que los datos fueran adecuados, pertinentes y no excesivos en relación con la finalidad perseguida y el ámbito en el que se recabaron. En cambio, la LORTAD aludía al principio de congruencia y racionalidad en su Exposición de Motivos, el cual garantizaba que los datos solo pudieran ser usados cuando lo justificara la finalidad para la que fueron recabados. Su observancia resultaba capital para evitar la difusión incontrolada de la información y garantizar el poder de control de los interesados sobre sus datos.

44 Señala TRONCOSO REIGADA que mediante este principio se consigue frenar el conocimiento excesivo sobre el interesado que es posible conseguir mediante el tratamiento de sus datos, ya sea directamente o bien a través de técnicas avanzadas. Vid. TRONCOSO REIGADA, A. El principio de calidad de los datos… referencia 4, p. 345.

45 En virtud del Considerando (26) Directiva 2016/680/UE, la limitación a lo necesario debe ser evaluada tanto desde un punto de vista cuantitativo -volumen de datos-, como cualitativo -categoría de datos-.

46 El concepto de adecuación se refiere a la eficacia del dato para conseguir la finalidad fijada del tratamiento, es decir, un dato será adecuado, cuando sea estrictamente necesario. Vid. PUYOL MONTERO, J. Los principios del derecho a la protección de datos… referencia 5, p. 138.

47 Los datos serán pertinentes, cuando su recolección se encuentre plenamente justificada, en función de la naturaleza y la finalidad que se persigue por el tratamiento,

48 TRONCOSO REIGADA, A. El principio de calidad de los datos… referencia 4, pp. 343-344 pone de relieve el debate doctrinal acerca del significado de estos subprincipios respecto al principio de calidad. Así mientras LUCAS MURILLO mantiene que ambos son términos

En segundo lugar, este principio conculca que los datos personales que se traten deben de limitarse a aquellos estrictamente necesarios en relación a los fines para los que son tratados. Vemos como por razón de la aplicación de estas máximas, los datos personales a tratar resultan restringidos fundamentalmente por la estricta necesidad que marquen los fines perseguidos[49] por el responsable del tratamiento, sin que sea posible exigir datos innecesarios o prescindibles, que no aporten ninguna utilidad para alcanzar los fines del tratamiento o que puedan ser sustituidos por otros menos invasivos. Por tanto, de no ser necesarios todo o parte de los datos personales, debe evitarse su tratamiento, tal y como reseña el Considerando 26 de la Directiva 2016/680/UE[50].

Así las cosas, en este momento histórico en el que el conocimiento, la acumulación de información y la ágil accesibilidad a los datos personales de la gran mayoría de los ciudadanos por el Estado constituye una realidad, limitar la recolección de los datos a aquellos que vienen justificados por la necesidad y pertinencia de la investigación o enjuiciamiento del delito, justifica que única y exclusivamente se recopilen aquellos datos que sean imprescindibles para la finalidad pretendida[51].

---

sinónimos con pequeños matices que aluden a la idoneidad de los datos para la finalidad del tratamiento, mientras SÁNCHEZ BRAVO y HERRÁN ORTIZ, diferencian ambos elementos, considerando que su enunciación conjunta no responde a un interés de reforzar una idea, sino que a la necesidad de delimitar y definir realidades diferentes en relación con los datos personales, indicando que la adecuación hace referencia a la conexión del dato con la finalidad, mientras que la pertinencia con la exigencia de no solicitar más datos que los necesarios para cumplir el objetivo, criterio éste último con el que nos identificamos, en analogía a los requisitos de la prueba civil previstos en la Ley de Enjuiciamiento Civil. MURILLO DE LA CUEVA, P. *Informática y protección de datos personales*. Madrid: CEC, 1993, p. 65; HERRÁN ORTIZ, A.I., *La violación de la intimidad en la protección de datos personales*. Madrid: Dykinson, 1999, p. 243 y SÁNCHEZ BRAVO, A. *La protección del derecho a la libertad informática en la Unión Europea*. Sevilla: Universidad de Sevilla, 1998, p. 85.

[49] Por tanto, es la finalidad del tratamiento la que posibilita saber si los datos a recabar se ajustan a su logro desde el punto de vista de la causalidad, motivo por el que se convierte en el elemento clave para determinar la pertinencia o no de los datos. Vid. TRONCOSO REIGADA, A. El principio de calidad de los datos… referencia 4, p. 346.

[50] Esta indica que "Los datos personales solo deberían ser objeto de tratamiento si la finalidad del tratamiento no puede lograrse razonablemente por otros medios".

[51] Se establece, asimismo, junto a la adecuación y funcionalidad de los datos, una prohibición de exceso de los datos personales. Ello implica que debe reducirse el número de datos a tratar hasta el mínimo posible que permita seguir alcanzando la finalidad pretendida. Igualmente, de entre todos los datos personales que sirvan al cumplimiento de una misma finalidad, debe de optarse por el menos invasivo para la privacidad del interesado. Habida cuenta del desarrollo de técnicas especialmente intrusivas para los ciudadanos, es por lo que se exige en estos casos someter las opciones disponibles a un juicio de proporcionalidad de conformidad con las asentadas reglas establecidas por nuestro Tribunal Constitucional en su STC 207/1996, de 16 de diciembre.

En el ámbito del proceso penal, y principalmente en su fase de instrucción, dada su función recopiladora de medidas de investigación y fuentes de prueba para la preparación del juicio, el cumplimiento de este principio va a exigir, que en la medida de lo posible, el órgano judicial que pretenda obtener datos personales necesarios, delimite y acote cuantitativa y cualitativamente, en la medida de lo posible, siquiera relativamente o en base a ciertos criterios, la información cuya obtención se requiere. Esta concreción deberá de definirse necesariamente en la resolución judicial que acuerde la medida de investigación consistente en la aprehensión o recogida de datos.

Más complejo resulta el cumplimiento de dicho principio en los supuestos en los que se lleva a cabo una medida limitativa de derechos sobre soportes y dispositivos que almacenen o conserven importantes cantidades de información y datos de carácter personal, que impidan filtrar y discriminar, durante el propio registro inicial, los que presentan relevancia para el proceso. En estos supuestos, sería imprescindible articular en la Ley de Enjuiciamiento Criminal un procedimiento posterior al registro, con intervención de las partes implicadas, dirigida a determinar la información que debe ser objeto de expurgo por no resultar pertinente ni útil para la investigación. De este modo se conseguiría un mayor respeto al principio de adecuación y se evitaría, la acumulación gratuita de datos en manos de las autoridades con la tentación de utilización para otros fines distintos[52].

5. Principio de exactitud

Los arts. 4.1.d) Directiva 2016/680/UE y 6.1.d) Ley Orgánica 7/2021 proclaman el principio de exactitud[53], como regla cuya observancia coadyuva a

[52] "La conservación de datos personales con una determinada finalidad despierta el deseo de hacer uso de dichos datos con otros fines". Con esta reveladora sentencia dio inicio el escrito de conclusiones de la Abogada General del TJUE de fecha 18 de julio de 2007 relativas a la cuestión prejudicial planteada por el Juzgado Mercantil núm.5 de Madrid en el caso Promusicae contra Telefónica de España S.A.U. (C-275/06), y en la que se pone de relieve los riesgos que se crean de la mera acumulación de datos de interesados.

[53] Principio que ya se dispuso en el Convenio 108 del Consejo de Europa, al proclamar en su art. 5.d) que los datos "serán exactos y si fuera necesario puestos al día". La LORTAD, en su art. 4.3 recogía el principio tal que así "Dichos datos serán exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado", aunque sin precisar el momento al que debía de referirse dicha situación. Por su parte, la Directiva 95/46/CE en términos similares a los del RGPD y la Directiva 2016/680/UE, establecía en su art. 6.1.c) la obligación de los Estados de disponer la obligación de que los datos personales fueren "exactos y, cuando sea necesario, actualizados; 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". Y también la LOPD en los apartados 3º y 4º de su art. 4 proclamaba a este principio bajo los siguientes términos: "Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del

garantizar la calidad del dato[54]. Ambos preceptos disponen que los datos personales tratados deberán ser "exactos y, si fuera necesario, actualizados; se habrán de adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que son tratados".

Esta regla, de la que se derivan varias implicaciones para la autoridad judicial, acarrea en primer término, la necesidad de que los datos que recoja y conserve en sus ficheros, con fines penales, sean en todo momento correctos[55] y/o que respondan fidedignamente a la realidad del interesado. En segundo término y como consecuencia de la anterior, que aquellos datos que por su propia naturaleza o características sean susceptibles de modificación o variación, deban de ser correctamente actualizados[56], si durante el curso del tratamiento son objeto de cambio, para reflejar en todo momento la veracidad, especialmente, si de los mismos se puede derivar alguna consecuencia jurídica.

De este modo, en caso de que los datos albergados en los ficheros no sean exactos, bien por no reflejar la realidad o bien por haber variado el valor del dato, la autoridad queda obligada a adoptar, sin dilaciones indebidas, todas las medidas razonables que sean necesarias para suprimir o actualizar los datos. Recaen, por tanto, en la autoridad judicial, las referidas tareas de control, supervisión, supresión y actualización de los datos personales de los afectados,

---

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". Siendo posteriormente desarrollado en el RLOPD, a través del apartado 5º de su art. 8 estableciendo que "Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste. Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello (…)".

[54] SANZ CALVO, L. Calidad de los datos. En LESMES SERRANO, C. (coord.) La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia. Valladolid: Lex Nova, 2008, p. 142.

[55] El RGPD alude al término exacto, lo que hace referencia a lo puntual, fiel y cabal, en relación con la realidad que el dato pretenda reflejar. Así, el dato es exacto cuando refleja lo que el titular del mismo quiere reflejar y es reconocido por en idénticos términos por el responsable. Vid. ABERASTURI GORRIÑO, U. *Los principios de la protección de datos aplicados en la sanidad (tesis doctoral)*. Bilbao: Universidad del País Vasco, 2011, p. 236.

[56] El término actualizado, hace referencia a la correspondencia con el tiempo presente, por lo que deben aludir a la realidad del tiempo en que se tratan. ABERASTURI GORRIÑO, U. *Los principios de la protección de datos aplicados en la sanidad (tesis doctoral)…* referencia 55, p. 236.

so pena de incumplimiento del principio de exactitud. Así las cosas, el responsable deberá en su caso, corregir el dato inexacto si existe una contradicción entre el registro conservado y realidad; actualizar el dato a su valor actual si el mismo ha sufrido una variación o, en su caso suprimir radicalmente el dato si no responde a la realidad y además no nos encontramos en ninguno de los anteriores supuestos.

Ahora bien, en este punto, hay que hacer varias precisiones. En primer lugar, se requiere diferenciar entre los datos obtenidos directamente del afectado de los datos que se obtienen de terceros, fuentes accesibles al público y otras autoridades. En el primero de los casos, dado que los datos a tratar son entregados libre y directamente por el interesado a la autoridad, los mismos pueden presumirse correctos y exactos, de forma análoga a la prevista en la Ley Orgánica 3/2018 para el régimen general. En estos supuestos, la autoridad judicial, no está obligada a llevar una verificación de los mismos, al menos cuando se soporten mediante algún medio idóneo para sustentarlos. Tan solo cuando se ponga de manifiesto por el propio interesado o a través de otro medio, la inexactitud del fichero deberá proceder su actualización. Todo ello, sin perjuicio de las facultades de control de la fiabilidad del dato que para este ámbito se atribuyen a la autoridad en el art. 7 de la Directiva 2016/680/UE y 10 de la Ley Orgánica 7/2021. De hecho, el primero de los apartados de este último precepto, obliga a las autoridades, a distinguir, en la medida de lo posible, entre los datos personales basados en hechos y los basados en apreciaciones personales. Sin embargo, para los supuestos en que los datos se obtienen de otras fuentes distintas del interesado, la autoridad deberá mostrar una especial diligencia a la hora de realizar el precitado análisis de calidad, procurando confirmar la realidad del dato y su fiabilidad objetiva.

Asimismo, como consecuencia de este principio, el art. 10 de la Ley Orgánica 7/2021, también ordena que las autoridades competentes deben adoptar cuantas medidas organizativas y técnicas razonables sean necesarias para garantizar que aquellos datos que no reúnan las cualidades vinculadas a la exactitud, esto es, que sean inexactos, incompletos o desactualizados, no sean comunicados ni puestos a disposición de terceros. De hecho, se les exige que si una vez consumada la transmisión de unos datos, se comprobara que los mismos no eran correctos, por adolecer de alguno de los defectos señalados con anterioridad, deberán de ponerlo en conocimiento inmediato del cesionario, con el objeto de que, según proceda, se rectifiquen, se supriman o se limite su tratamiento.

La anterior restricción de transmisión de datos no empece que aquellos no sustentados en hechos objetivos, sino en valoraciones subjetivas, puedan cederse a terceras autoridades. Para ello, además de cumplir con los requisitos ordinarios que se exigen para la cesión de datos entre autoridades, se deberá de incorporar

una valoración sobre la calidad, exactitud y estado de actualización de estos. Y ello con el fin de que la autoridad cesionaria pueda advertir el nivel de calidad y fiabilidad de los datos que recibe. A tal fin, la autoridad cedente tendrá la obligación, cuando ello sea factible, de controlar ex ante tales cualidades. No obstante, bajo nuestro punto de vista, dicha valoración debería ser objeto de transmisión, incluso en aquellas cesiones que tengan por objeto la cesión de datos objetivos que sean susceptibles de alteración por cualquier razón y no presenten un carácter puramente estático.

En conclusión, nos encontramos ante un principio esencial del derecho a la protección de datos, que aunque no ha sido abordado muy extensamente por la doctrina, es de especial relevancia, como ha destacado en algún pronunciamiento la jurisprudencia de la Audiencia Nacional[57], por contribuir con su cumplimiento la protección enérgica de los derechos del interesado, toda vez que su falta de verificación puede afectar negativamente al interesado, acarreándole perjuicios o inconvenientes de suma importancia, especialmente en determinados ámbitos[58].

6. Principio limitación del plazo de conservación

El principio de limitación del plazo de conservación[59] aparece regulado en el art. 4.1.e) de la Directiva 2016/680/UE y 6.1.e) de la Ley Orgánica 7/2021. En el primero de los preceptos, aparece formulado bajo la siguiente máxima: "Los datos personales serán: mantenidos de forma que se permita la identificación de

[57] España. Sentencia Audiencia Nacional de 28 de junio 2002, FJ 3º.

[58] TRONCOSO REIGADA, A. El principio de calidad de los datos… referencia 4, p. 358.

[59] Principio que también se previó por el Consejo de Europa en el Convenio 108 bajo su art. 5.e) al precisar que los datos personales "se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario". La LORTAD, por su parte, lo introdujo en el ordenamiento español expresando que los datos "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". Posteriormente, la Directiva 95/46/CE lo configuró determinando que los *datos* "deberían ser conservados de forma que no permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente", por lo que amplió la posibilidad de conservación más allá de la conclusión del tratamiento inicial a otros tratamientos que eventualmente pudieran desarrollarse con posterioridad. Asimismo, contempló la posibilidad de que dicho plazo se extendiera siempre que se tomaran las medidas adecuadas de seguridad y el tratamiento a realizar tuviera finalidad histórica, estadística o científica. La LOPD, siguiendo la senda de la norma a la que sucedió, proclamó el principio en su art. 4.5 mediante una regla similar, estableciendo que "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".

los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales"[60].

En virtud de dicho principio, la autoridad judicial responsable del tratamiento debe de limitar de manera general el plazo de conservación de los datos personales mantenidos en los ficheros por el plazo imprescindible para el cumplimiento de la finalidad para la que fueron recogidos. Para conseguir tal objetivo, se exige que la autoridad competente establezca de antemano los plazos previstos o previsibles para su supresión, de acuerdo a los criterios adecuados para ello. Esta delimitación temporal, a pesar de que consta como elemento del derecho de información y debe ser comunicada al interesado cuando los datos son recogidos, no exige en todo caso una concreción *ab initio* exacta y perfecta del plazo por el que los datos van a ser tratados. Por ejemplo, el art. 8 de la Ley Orgánica 7/2021, sin prever plazos concretos o máximos de conservación, dispone la obligación de las autoridades de conservar los datos únicamente durante el tiempo necesario para cumplir los fines penales que estén desarrollando. Y es que, en el ámbito del proceso penal, no resulta controvertido que no es posible prefijar los plazos de supresión de forma general con relación a cifras temporales cuantitativas, habida cuenta de la contingencia e incertidumbre en la duración y alcance del desarrollo de éstos. Y es que, aunque el art. 324 LECrim establezca un plazo máximo de instrucción, ésta puede ser objeto de prórroga, no existen plazos para la celebración del juicio oral y los posibles medios de impugnación existentes al alcance de las partes impiden determinar plazos temporales concretos.

Por ello, únicamente en el caso de que se pueda prever con certeza el mismo con anterioridad a acometer el tratamiento será necesaria su determinación precisa. Lo habitual, siendo regla igualmente válida a los efectos de cumplimiento de este principio, es que el responsable en cambio sí pueda determinar este periodo relativamente atendiendo a alguna circunstancia o exigencia legal. Así, en el ámbito de la Directiva 2016/680/UE, dichos plazos coinciden con el tiempo establecido en la legislación que obligue a conservar determinada información durante un concreto periodo[61] o el plazo de

[60] En la Ley Orgánica 7/2021, se recoge bajo una redacción distinta, aunque con idéntico alcance: "Los datos personales serán conservados de forma que permitan identificar al interesado durante un período no superior al necesario para los fines para los que son tratados".

[61] Piénsese por ejemplo en las exigencias de conservación de los datos de tráfico y localización de las comunicaciones electrónicas a las que se someten los operadores de telecomunicaciones en virtud de lo dispuesto en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, las previstas en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica referidas a la historia clínica o las derivadas de la normativa fiscal y de prevención del blanqueo de capitales.

prescripción o caducidad[62] de las eventuales acciones que contemple el ordenamiento para la relación de la que subyace al tratamiento.

No obstante, lo anterior, sin perjuicio de que pueda extenderse la conservación de los datos personales en previsión del cumplimiento de aspectos secundarios o accesorios de los fines principales, por aplicación de este principio, los datos que sucesivamente vayan dejando de ser adecuados y pertinentes para la conclusión de aquellos que permanecen, no deberán seguir siendo conservados, lo que implica la obligación de la autoridad de proceder a su borrado definitivo. En caso contrario, es decir en todos aquellos supuestos en los que sea viable, siquiera relativamente mediante la aplicación de algún criterio predefinido, establecer dichos plazos de antemano por cualquier razón que impida determinar precisamente el periodo en que se prolongará el tratamiento, se hace necesaria que el responsable del tratamiento efectúe revisiones periódicas de los datos almacenados, con el objetivo de que aquellos datos que se compruebe que han devenido innecesarios para la finalidad dejen de ser conservados de forma que permitan la identificación de su titular.

En el ámbito aplicativo de la Directiva 2016/680/UE, dicha obligación se ha incorporado en el art. 8.2 de la Ley Orgánica 7/2021 disponiendo la necesariedad de revisar, cada tres años, a lo sumo, y si fuere posible mediante tratamientos automatizados, la necesidad de conservar, limitar o suprimir el conjunto de los datos personales contenidos en cada una de las actividades de tratamiento que ejecutan. Para lo cual deben atender a factores como la edad del afectado, el carácter de los datos y a la conclusión de una investigación o procedimiento penal.

La aplicación de este principio se complementa con una exigencia lógica y consecuente, que no puede ser otra que la obligación de la autoridad responsable del tratamiento de suprimir los datos personales una vez que han cumplido su función. Ciertamente, al contrario de lo que hiciera la derogada LOPD en su art. 4.5 al disponer que "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", ni la Directiva 2016/680/UE ni la Ley

---

Troncoso precisa que el señalamiento de plazos es habitual en el ámbito del derecho administrativo, echando en falta la existencia de una norma que establezca plazos de conservación general de la información que fije los criterios de archivo y los procedimientos de expurgo. TRONCOSO REIGADA, A. El principio de calidad de los datos… referencia 4, p. 385.

[62] PUYOL MONTERO expresa que la conservación de los datos siempre ha sido un tema polémico en función de la discrepancia existente entre los plazos que cubren las responsabilidades derivadas del propio tratamiento de los mismos, de aquellos que se vinculan a la prescripción de las acciones derivadas del negocio jurídico subyacente, sobre la base del cual se han recolectado dichos datos. PUYOL MONTERO, J. Los principios del derecho a la protección de datos… referencia 5, p. 139.

Orgánica 7/2021 prevén una regla análoga. En todo caso, la misma es posible deducirla de la lectura de los diferentes supuestos enumerados en 16.2 de la Directiva 2016/680/UE –23.2 de la Ley Orgánica 7/2021-, coincidentes con los casos en los que encaja la aplicación del derecho de supresión, en los que se encuentra implícita.

No obstante, lo anterior, debemos señalar que en la LECrim es posible encontrar ciertos plazos de naturaleza relativa que condicionan la limitación de la conservación de los datos. En particular, es el art. 588 bis k) LECrim el destinado a reglamentar la destrucción de registros, si bien, su aplicación se circunscribe *prima facie*, a los datos e información obtenidos a través de diligencias de investigación tecnológica. Sin perjuicio de que su aplicación pueda extenderse a la totalidad de los datos obrantes en un expediente, sería imprescindible, en aras de garantizar la seguridad jurídica y una aplicación efectiva de dicho principio, la introducción de una regulación específica de alcance general a cualquier dato, con independencia de la fuente de origen.

Este precepto, establece que una vez que se ponga término al procedimiento mediante resolución firme, se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida, que habitualmente coincidirán con los de la Policía Judicial. Y ello sin perjuicio de que se conserve una copia bajo la custodia del Letrado de la Administración de Justicia. Dichas copias, serán igualmente destruidas, cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación a juicio del Tribunal.

En cualquier caso, para los casos en que dicha supresión no se lleve a cabo en los plazos estipulados o se prorrogue su cancelación, el art. 8.3 de la Ley Orgánica 7/2021 establece un plazo máximo absoluto y terminante de veinte años, que, en principio, no debe sobrepasarse. No obstante, éste pierde su carácter de plazo propio, al preverse ciertas causas que permiten la extensión del mismo, como, por ejemplo, que se incorporen en una causa abierta o se vinculen a un delito no prescrito o cuya ejecutoria no ha concluido. En cualquier caso, lo cierto es que acudir a dichos plazos máximos, debe ser en todo caso la excepción, al menos en el ámbito penal, debiendo entrar en juego rotundamente la regla general de operatividad del principio de limitación de la conservación, por el cual deben ser suprimidos los datos en los plazos marcados por la LECrim.

7. Principios de integridad y confidencialidad

La consagración de la integridad y confidencialidad – o seguridad[63]- de los datos como auténticos principios informadores[64] del derecho a la protección de datos ha venido de la mano del nuevo paquete legislativo de protección de datos aprobado por la Unión Europea en 2016. Tanto la Directiva 2016/680/UE, como la Ley Orgánica 7/2021 como ley de transposición, preceptúan que los datos personales deben ser "tratados de tal manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas"[65].

De sendos principios dimana la obligación de la autoridad competente de dotar a los ficheros y a los sistemas – manuales o automatizados- utilizados en la organización para el desarrollo y ejecución de las actividades vinculadas al tratamiento, de una protección suficientemente adecuada para garantizar la seguridad de los datos personales que se conservan en sus ficheros[66]. No es

[63] Como era denominado dicho principio en la Directiva 95/46/CE y la LOPD.

[64] La seguridad –tal y como se denominaba a la integridad y confidencialidad- se configuraba en la antigua Directiva 95/46/CE no directamente como principio, sino como un elemento condicionante de las actividades y sistemas vinculados al tratamiento de los datos del responsable. En cambio, la LOPD sí reconocía a ambos elementos como auténticos principios, al encuadrarlos bajo su Título II dedicado a la regulación de éstos. Muestra de ello es el pronunciamiento de la Audiencia Nacional, en su sentencia de fecha 09/05/2008, cuyo Fundamento de Derecho 2º comienza diciendo: "El art. 10 de la LOPD regula de forma individualizada el deber de secreto de quienes tratan datos personales, dentro del título dedicado a los principios de protección de datos, lo que refleja la gran importancia que el legislador atribuye al mismo".

[65] Puede apreciarse la incidencia del Convenio 108 en la redacción de este principio, toda vez que en su art. 7, se reconocía a la seguridad de los datos como principio básico, estableciéndose al efecto que "Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados".

[66] El concepto de seguridad aplicado a un sistema de información, tal y como puede entenderse un fichero a efectos de la normativa de protección de datos, se describe en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, como "la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles". Concepto que a su vez se conforma de cuatro dimensiones diferenciadas: la disponibilidad, propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren; la integridad, propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada; la confidencialidad, propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados y la autenticidad, propiedad o característica

posible obviar que de la existencia de brechas y fisuras de seguridad en la organización y en los sistemas de tratamiento de datos deriva en un riesgo para los derechos y libertades de las personas físicas cuya gravedad y probabilidad dependerá de la naturaleza, el alcance, el contexto y los fines del tratamiento de datos.

Por tal razón, a todo el sistema de protección de datos se le deben de aplicar las medidas de naturaleza técnica y organizativa apropiadas[67] que permitan garantizar en todo momento[68] la integridad[69] y la confidencialidad de los datos[70], debiendo evitarse específicamente supuestos tales como el

consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

[67] Obligación que se recoge en el art. 29 Directiva 2016/680/UE para autoridades competentes, cuando precisa que "… teniendo en cuenta el estado de la técnica y los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como el riesgo de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, apliquen medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, sobre todo en lo que se refiere al tratamiento de las categorías especiales de datos personales previstas en el artículo 10". En mismo sentido se pronunciaba el art. 17 de la Directiva 95/46/CE, cuando requería la "aplicación de las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la perdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales". La LOPD también preceptuaba en su art. 9.1 que "El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".

[68] La legislación europea persigue que la seguridad se garantice incluso con carácter previo al comienzo del tratamiento, por tal motivo, establece como una de sus prioridades en cuanto a las medidas de seguridad, el cumplimiento *ab initio* de los principios de protección de datos desde el diseño y por defecto que se plasman en el art. 20 Directiva 2016/680/UE, que colaboran en la minimización de uso de datos y de los riesgos.

[69] Por integridad de un dato se debe entender el atributo o cualidad que permite considerar a la información como exacta, completa, homogénea, sólida y coherente, con la intención de los creadores del fichero. Esto es, los datos serán íntegros cuando mantenga las características de completitud y corrección. Esta cualidad, que va ligada al propio dato y no al lugar donde se almacena, se obtiene cuando se impide eficazmente que el contenido de un fichero se vea accidental o intencionalmente modificado, en base a su propio contenido o con ayuda de la inserción de nuevo o destruido total o parcialmente. Vid. MAGERIT versión 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas, octubre 2012.

[70] Por confidencialidad, se debe entender la situación que permite acceder a un determinado dato de un fichero exclusivamente a la o las personas autorizadas para ello en función del cargo o puesto que desempeñan. La confidencialidad se rompe al acceder un tercero sin legitimación ni autorización por razón del cargo que desempeña, sea de manera voluntaria

tratamiento de datos no autorizado o ilícito, la pérdida accidental y el daño o destrucción de éstos.

Hasta la entrada en vigor del paquete legislativo de protección de datos, las concretas medidas técnicas y organizativas que debían de implantarse por el responsable del tratamiento en su organización se determinaban por vía reglamentaria en el RLOPD[71], estableciéndose al efecto tres niveles diferenciados de protección, a aplicar, según el grado de sensibilidad que presentaran los datos personales objeto de tratamiento. No obstante, esta situación se ha visto alterada en el régimen vigente a raíz de la introducción del principio de responsabilidad activa o proactividad que será analizado en el epígrafe siguiente. Actualmente, de acuerdo con lo estipulado en los arts. 29 Directiva 2016/680/UE – art. 37 de la Ley Orgánica 7/2021 -, se obliga a los responsables y encargados del tratamiento, previa evaluación de los riesgos inherentes al tratamiento, especialmente para los derechos y libertades fundamentales, a adoptar aquellas medidas técnicas y organizativas necesarias para garantizar la integridad y confidencialidad de los datos, si bien facultándolos para que ellos mismos puedan seleccionar las que consideren oportunas, con la única condición de que sea apropiadas, adecuadas y suficientes para tales fines y se muestren respetuosas con los demás principios y obligaciones de la normativa y, muy especialmente, con los derechos y libertades de los interesados. Y es por este giro en la delegación de la capacidad de decidir del responsable sobre las concretas medidas de seguridad a adoptar,

por haber vulnerado las medidas de seguridad establecidas al efecto o involuntaria por no haberse establecido aquellas. Vid. MAGERIT versión 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas, octubre 2012.

[71] El régimen de las medidas de seguridad aplicables a los sistemas de tratamiento de datos se establecía anteriormente en el Título VIII del RLOPD, desarrollándose en sus arts. 79 a 114. Este marco clasificaba en tres niveles – bajo, medio y alto – las medidas de seguridad exigidas a los ficheros, enumerando las diferentes reglas que serían de aplicación a cada nivel diferenciando a su vez entre los ficheros manuales y los automatizados, y cuya aplicación era acumulativa, según se iba ascendiendo de categoría. De modo que a los ficheros que exigían una protección más elevada, se le aplicaban conjuntamente las medidas de los niveles alto, medio y bajo, mientas a los que merecían una protección más leve, tan solo se les deberían aplicar las de nivel bajo, ex art. 81 RLOPD. Aunque actualmente el marco dispuesto en el RLOPD no es directamente aplicable, constituye un elemento esencial para la guía y orientación de responsables en cuanto a la adopción de medidas en la organización. Vid. RIBAGORDA GARNACHO, A. Las medidas de seguridad en el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal: Título II. Principios de la Protección de Datos. Artículo 9. en TRONCOSO REIGADA, A. (dir.) *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.* Madrid: Civitas, 2010, pp. 735-761 y MARTÍNEZ MARTÍNEZ, R. Las medidas de seguridad. En MARTÍNEZ MARTÍNEZ, R. (coord.), *Protección de datos: comentarios a la LOPD y su reglamento de desarrollo*. Valencia: Tirant lo Blanch, 2009, pp. 89-119.

por lo que recae en éste la carga de demostrar su adecuación a la salvaguarda de seguridad del tratamiento de los datos personales.

No obstante, en el ámbito de aplicación de la Directiva 2016/680/UE, habida cuenta del desarrollo de una función eminentemente pública, como es la jurisdiccional, la libertad de maniobra de los órganos judiciales, en tanto responsables, no es tal, sino que viene establecida reglamentariamente por el Esquema Nacional de Seguridad y particularmente por el Esquema judicial de interoperabilidad y seguridad. En estas normas técnicas, se compaginan toda una serie de objetivos o medidas de obligada consecución o implantación que se relacionan en los preceptos mencionados. Dicha distinción con el ámbito general obedece, sin duda alguna, al reforzamiento de las garantías que requieren la naturaleza de los datos y la propia actividad a la que se vincula el tratamiento, en la que la cadena de custodia, la trazabilidad de las operaciones y la seguridad se erigen elementos esenciales, incluso para garantizar la validez de las fuentes de prueba que se pretendan practicar. Para este ámbito, en particular, la Ley Orgánica 7/2021, exige en su art. 37 que las autoridades competentes garanticen la implantación, cuanto menos, de las siguientes medidas orientadas a la seguridad:

> a) Control de acceso a los equipamientos, a fin de denegar el acceso a personas no autorizadas a los equipamientos utilizados para el tratamiento.
>
> b) Control de los soportes de datos, a fin de impedir que estos puedan ser leídos, copiados, modificados o cancelados por personas no autorizadas.
>
> c) Control del almacenamiento, a fin de impedir que se introduzcan sin autorización datos personales, o que estos puedan inspeccionarse, modificarse o suprimirse sin autorización.
>
> d) Control de los usuarios, a fin impedir que los sistemas de tratamiento automatizado puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos.
>
> e) Control del acceso a los datos, con el objeto de garantizar que las personas autorizadas a utilizar un sistema de tratamiento automatizado, sólo puedan tener acceso a los datos personales para los que han sido autorizados.
>
> f) Control de la transmisión, en aras de garantizar que sea posible verificar y establecer a qué organismos se han transmitido o pueden transmitirse, o a cuya disposición pueden ponerse los datos personales mediante equipamientos de comunicación de datos.
>
> g) Control de la introducción, para garantizar que pueda verificarse y constatarse, a posteriori, qué datos personales se han introducido en los

sistemas de tratamiento automatizado, en qué momento y quién los ha introducido.

h) Control del transporte, con miras a impedir que durante las transferencias de datos personales o durante el transporte de soportes de datos, los datos personales puedan ser leídos, copiados, modificados o suprimidos sin autorización.

i) Control de restablecimiento, al objeto de garantizar que los sistemas instalados puedan restablecerse en caso de interrupción.

j) Control de fiabilidad e integridad, con la finalidad de garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados y que los datos personales almacenados no se degraden por fallos de funcionamiento del sistema.

Como puede comprobarse, la aplicación de las medidas de seguridad y control que se establecen en pos de asegurar la integridad y confidencialidad de los datos obrantes en los ficheros jurisdiccionales no se circunscriben únicamente a los elementos materiales que conforman los sistemas de tratamiento, sino que se extienden igualmente a las personas que tienen acceso o que intervienen activamente de cualquier modo en actividades que conlleven aparejado inexorablemente un tratamiento de datos personales. Por tal motivo, la normativa exige igualmente al responsable que extienda la adopción de medidas de seguridad que tiendan a garantizar que de entre los sujetos que se hallen bajo su autoridad, únicamente puedan tratar datos personales aquellos que se señalen y exclusivamente de acuerdo a las instrucciones y directrices que imparta[72].

En todo caso, con relación a este principio es imprescindible recordar que la provisión de medios materiales y personales, y por tanto de los medios tecnológicos adecuados para el tratamiento de los datos personales, no depende de los propios órganos judiciales, ni de sus titulares, a pesar de tener la condición de autoridades competentes. Al contrario, éstos son suministrados por las denominadas Administraciones prestacionales[73]. Por tanto, son éstas, como encargadas del tratamiento, las que deben asegurar el cumplimiento de las obligaciones en materia de tratamiento y protección de datos personales, especialmente, en lo que se refiere al tratamiento que se lleva a cabo por medios y sistemas electrónicos, totalmente automatizado. Ello sin perjuicio de, tal y como prevé el art. 236 *sexies* LOPJ en su apartado 3º, que el Ministerio de Justicia,

[72] Con esta exigencia se trata, en definitiva, de conseguir la acomodación de la forma en que los funcionarios integrados en los Juzgados realizan sus funciones acorde exigencias que resultan de las medidas técnicas y organizativas implantadas, para asegurar el mantenimiento de la confidencialidad y seguridad de los datos personales.

[73] Arts. 236 sexies 1º y 2º LOPJ.

previo informe del Consejo General del Poder Judicial, elabore códigos de conducta destinados a contribuir a la correcta aplicación de la normativa de protección de datos personales en la oficina judicial, adecuando los principios de la normativa general a los propios de la regulación procesal y organización que resultan aplicables a los órganos judiciales.

8. Principio de responsabilidad activa o proactividad

Como colofón a los principios rectores vinculados al tratamiento de datos, el legislador europeo ha introducido *ex novo* al principio responsabilidad activa o proactividad[74], que se recoge en los arts. 4.4[75] Directiva 2016/680/UE y art. 6.5 Ley Orgánica 7/2021. Dicho principio puede, además, considerarse como una de las grandes novedades en la materia, por provocar un giro copernicano en cuanto al sistema de responsabilidad al que se sujetan las autoridades intervinientes en el tratamiento[76]. Éste se proclama bajo la siguiente consigna: "El responsable del

[74] Los términos de responsabilidad activa o proactividad -tal y como ha sido señalado mayoritariamente por la doctrina- han sido los vocablos utilizados para la trasposición al castellano del término anglosajón *accountability*, que es el concepto al que alude el legislador europeo para definir a tal principio. Véase ALBERTO GONZÁLEZ, P., *Responsabilidad proactiva en los tratamientos masivos de datos*. En *Dilemata*, núm. 24, 2017, España, p. 120 y MARTÍNEZ MARTÍNEZ, R. *Diligencia y responsabilidad en protección de datos: la llamada accountability* [en línea]. El Derecho, 2019. Éste último autor considera que los vocablos por los que se ha trasladado el término accountability al castellano no acaban de reflejar la riqueza material de este concepto anglosajón.

[75] Aunque el principio de responsabilidad proactiva se incorpora por primera vez en el ordenamiento jurídico como modelo preceptivo y orientador del marco de protección de datos a través del paquete legislativo impulsado por la Unión Europea en 2016, lo cierto es que la Organización para la Cooperación y el Desarrollo Económico ya optó por la adopción de este principio en sus Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales de 23 de septiembre de 1980. Asimismo, el GTA29 en su Dictamen 3/2010 sobre el principio de responsabilidad sugería la introducción de este modelo de responsabilidad mediante el otorgamiento de margen de actuación a los responsables del tratamiento para la modulación progresiva de la aplicación de medidas concretas en función del riesgo del tratamiento y la naturaleza de los datos a tratar.

[76] En los regímenes previos al RGPD se contemplaba un sistema de responsabilidad esencialmente basado en la responsabilidad reactiva – en contraposición al sistema proactivo o de responsabilidad activa- del responsable del fichero, pues los arts. 23 y 24 de la Directiva 95/46/CE conminaba a los Estados miembros a sancionar a los responsables que incumplieren las obligaciones que se dispusieran en las legislaciones nacionales que la transpusieran. Principio reactivo que en el ordenamiento interno se plasmó en el art. 43.1 LOPD al indicar que *"Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley"*. Es decir, el responsable del tratamiento estaba obligado a adoptar las concretas medidas de seguridad que se enumeraban con carácter general en la normativa de protección de datos para todos los responsables, con independencia de las particulares circunstancias existentes en la organización y la efectividad real de las medidas, respondiendo ante un eventual incumplimiento de estas obligaciones so pena de incurrir en la comisión de una

tratamiento deberá garantizar y estar en condiciones de demostrar el cumplimiento de lo establecido en este artículo".

El principio de responsabilidad proactiva determina que la responsabilidad del cumplimiento de las distintas obligaciones y garantías establecidas en el marco jurídico vigente del derecho a la protección de datos, con especial atención de los principios vertebradores del sistema, recae en último término en la autoridad competente[77]. Por tanto, los órganos judiciales, en tanto autoridad, deben no solamente cumplir diligentemente con los principios y obligaciones dispuestos en la normativa, sino que, además, deben de ser capaces de demostrarlo a la autoridad de control e incluso al propio interesado. O, dicho en otros términos, la autoridad competente, en tanto organiza y gestiona el sistema de protección de datos se encuentra sujeto a la condición inexcusable de cumplir férrea y escrupulosamente todos los principios y obligaciones esenciales de la materia con el fin de respetar los derechos y libertades del interesado, debiendo estar en disposición de poder acreditar fehacientemente tal cumplimiento[78].

En términos prácticos, este modelo requiere la realización de un análisis previo, exhaustivo y *ad casum* de los riesgos que entraña el tratamiento, atendiendo a los datos tratados, las finalidades a las que se destinan los mismos y las modalidades de operaciones de tratamiento seguidas. De acuerdo con los

infracción administrativa. Mientras la implantación de un sistema alternativo de responsabilidad activa supone un auténtico cambio de paradigma en la concepción del modelo de responsabilidad, pues los actores implicados adquieren un papel activo en la implantación y seguimiento de los procesos de cumplimiento de la normativa de protección de datos, debiendo afrontar tareas encaminadas una previa valoración de los riesgos que pudieran generarse con el tratamiento y a partir de los resultados obtenidos, proceder a la adopción de las medidas adecuadas para garantizar los principios y garantías de la materia, dotándose asimismo de mecanismos internos y externos para evaluar su fiabilidad y demostrar su efectividad cuando se solicite por las autoridades de control.

[77] BAJO ALBARRACÍN, J. C. Consideraciones sobre el principio de responsabilidad proactiva y diligencia (accountability). Experiencias desde el Compliance. En LÓPEZ CALVO, J. (coord.) *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*. Las Rozas de Madrid: Wolters Kluwer, 2019, p. 975.

[78] El Considerando (50) Directiva 2016/680/UE describe a la perfección las implicaciones esenciales de este principio para el responsable, tal que así "Se debe establecer la responsabilidad del responsable del tratamiento en relación con cualquier tratamiento de datos personales realizado por él mismo o en su nombre. En particular, el responsable del tratamiento debe estar obligado a poner en marcha medidas oportunas y eficaces y a poder demostrar la conformidad de las actividades de tratamiento con la presente Directiva. Estas medidas deben tener en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, así como el riesgo que representan para los derechos y las libertades de las personas físicas. Las medidas adoptadas por el responsable del tratamiento deben incluir la formulación y puesta en marcha de salvaguardias específicas en relación con el tratamiento de los datos personales de personas físicas vulnerables, en particular los niños".

resultados obtenidos, la autoridad deberá de determinar explícitamente los medios y formas de aplicar las medidas de seguridad y principios rectores del tratamiento, cerciorándose de que son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión. Obligaciones que adquieren especial significación a la hora de adoptar medidas de investigación para la obtención de fuentes de prueba consistentes en datos de carácter personal.

Asimismo, dichas obligaciones deben entenderse de modo dinámico, pues exigen del responsable una labor continua de revisión, actualización y mejora, especialmente ante los cambios que puedan acontecer en alguno de los elementos que participen en las actividades de tratamiento[79]. En síntesis, este principio exige principalmente del responsable del tratamiento por estar a la cabeza, aunque también de todos los demás participantes[80], una actitud consciente, diligente, preventiva y proactiva[81] frente a las operaciones de tratamiento de datos, con el claro objetivo de asegurar el respeto a los derechos y libertades del interesado.

9. Bibliografía

ABERASTURI GORRIÑO, U. *Los principios de la protección de datos aplicados en la sanidad (tesis doctoral)*. Bilbao: Universidad del País Vasco, 2011.

ALBERTO GONZÁLEZ, P., *Responsabilidad proactiva en los tratamientos masivos de datos*. En *Dilemata*, núm. 24, 2017, España, pp. 115-129. [consulta: 14 junio 2022] ISSN: 1989-7022. Disponible en: https://dialnet.unirioja.es/descarga/articulo/6066825.pdf

APARICIO SALOM, J. La calidad de los datos. En TRONCOSO REIGADA, A. (dir.) *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. Madrid, Civitas, 2010, pp. 324-339.

ATAZ LÓPEZ, J. La buena fe contractual. En Bercovitz RODRÍGUEZ-CANO, R., MORALEJO IMBERNÓN, N. y QUICIOS MOLINA, M. S. (coord.) *Tratado de los Contratos*. Valencia, Tirant Lo Blanch 2009, pp. 167-170. ISBN 9788498765045.

[79] MARTÍNEZ MARTÍNEZ, R. *Diligencia y responsabilidad en protección de datos: la llamada accountability*… referencia 74.

[80] PALMA ORTIGOSA, A. Principios relativos al tratamiento de datos personales… referencia 8, p. 48, considera que con este principio se pretende instaurar una filosofía y cultura de respeto al derecho a la protección de datos en el seno de la organización.

[81] PALMA ORTIGOSA, A., Principios relativos al tratamiento de datos personales… referencia 8, p. 48 y LORENZO CABRERA, S., PALMA ORTIGOSA, A., y TRUJILLO CABRERA, C., «Responsabilidad proactiva» en MURGA FERNÁNDEZ, J. P., FERNÁNDEZ SCAGLIUSI M. A. y ESPEJO LERDO DE TEJADA, M. (dir.), *Protección de datos, responsabilidad activa técnicas de garantía*, Reus, Madrid, 2018, pág. 154.

BAJO ALBARRACÍN, J. C. Consideraciones sobre el principio de responsabilidad proactiva y diligencia (accountability). Experiencias desde el Compliance. En LÓPEZ CALVO, J. (coord.) *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*. Las Rozas de Madrid: Wolters Kluwer, 2019, pp. 973-981. ISBN 9788490903452.

DELGADO MARTÍN, J. Reflexiones sobre la protección de datos personales en la Administración de Justicia. En *Diario La Ley*, núm. 9363, 2019, España. [consulta: 18 junio 2022] ISSN: 1989-6913. Disponible en: https://diariolaley.laleynext.es/

FRÍAS MARTÍNEZ, E. Obtención de datos personales en procesos penales y administrativos. En *Diario La Ley*, núm. 9404, 2019, España. [consulta: 18 junio 2022] ISSN: 1989-6913. Disponible en: https://diariolaley.laleynext.es/

GALÁN MUÑOZ, A. La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea. En COLOMER HERNÁNDEZ, I. (dir.) *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*. Cizur Menor: Aranzadi, 2015, pp. 37-70. ISBN 9788490599174.

GONZÁLEZ CANO, M. I., Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680. En *Revista Brasileira de Direito Processual Penal*, vol. 5, núm. 3, 2019, Brasil, pp. 1331-1384. [consulta: 16 junio 2022] ISSN: 2525-510X. Disponible en: https://revista.ibraspp.com.br/RBDPP/article/view/279/188

HERRÁN ORTIZ, A.I., *La violación de la intimidad en la protección de datos personales*. Madrid: Dykinson, 1999. ISBN 9788481554090.

LORENZO CABRERA, S., PALMA ORTIGOSA, A., y TRUJILLO CABRERA, C. Responsabilidad proactiva. En MURGA FERNÁNDEZ, J. P., FERNÁNDEZ SCAGLIUSI M. A. y ESPEJO LERDO DE TEJADA, M. (dir.), *Protección de datos, responsabilidad activa técnicas de garantía*. Madrid: Editorial Reus, 2018, pp. 143-172. ISBN 9788429020939.

MARTÍNEZ MARTÍNEZ, R. Las medidas de seguridad. En MARTÍNEZ MARTÍNEZ, R. (coord.), *Protección de datos: comentarios a la LOPD y su reglamento de desarrollo*. Valencia: Tirant lo Blanch, 2009, pp. 89-119. ISBN 9788498763560.

MARTÍNEZ MARTÍNEZ, R. *Diligencia y responsabilidad en protección de datos: la llamada accountability* [en línea]. El Derecho, 2019. [consulta: 16 junio 2022]. Disponible en: https://elderecho.com/diligencia-y-responsabilidad-en-proteccion-de-datos-la-llamada-accountabily

MORENO CATENA, V. y CORTÉS DOMÍNGUEZ, V. *Derecho Procesal Penal.* Valencia: Tirant Lo Blanch, 2021. ISBN 9788411130479.

MURILLO DE LA CUEVA, P. *Informática y protección de datos personales*. Madrid: CEC, 1993.

PALMA ORTIGOSA, A. Principios relativos al tratamiento de datos personales. En MURGA FERNÁNDEZ, J. P., FERNÁNDEZ SCAGLIUSI M. A. y ESPEJO LERDO DE TEJADA, M. (dirs.), Protección de datos, responsabilidad activa técnicas de garantía. Madrid: Editorial Reus, 2018, pp. 39-49. ISBN 9788429020939.

PUYOL MONTERO, J. Los principios del derecho a la protección de datos. En PIÑAR MAÑAS J. L. (dir.), *Reglamento general de protección de datos: hacia* un *nuevo modelo europeo de privacidad*. Madrid: Editorial Reus, 2016, pp. 135-150. ISBN 9788429019360.

RIBAGORDA GARNACHO, A. Las medidas de seguridad en el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal: Título II. Principios de la Protección de Datos. Artículo 9. en TRONCOSO REIGADA, A. (dir.) *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.* Madrid: Civitas, 2010, pp. 735-761. ISBN 9788447034239.

RÍO LABARTHE, G. El proceso penal. Funciones. En ASENSIO MELLADO, J. M. (dir.) *Derecho procesal penal.* Valencia: Tirant Lo Blanch, 2020, pp. 25-36. ISBN 9788413559544.

SÁNCHEZ BRAVO, A. *La protección del derecho a la libertad informática en la Unión Europea*. Sevilla: Universidad de Sevilla, 1998. ISBN 8447204936.

SANZ CALVO, L. Calidad de los datos. En LESMES SERRANO, C. (coord.) La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia. Valladolid: Lex Nova, 2008, pp. 138-162.

SOLAR CALVO, P. La doble vía europea en protección de datos. En Diario La Ley, núm. 7832, 2012, España. [consulta: 18 junio 2022] ISSN: 1989-6913. Disponible en: https://diariolaley.laleynext.es/

TRONCOSO REIGADA, A. El principio de calidad de los datos. En TRONCOSO REIGADA, A. (dir.) *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. Madrid: Civitas, 2010, pp. 340-396. ISBN 9788447034239.

Conflicto de intereses

El autor declara no tener ningún conflicto de intereses.

Financiación

Esta publicación ha sido financiada por la Unión Europea "NextGenerationEU", por el Plan de Recuperación, Transformación y Resilencia y por el Ministerio de Universidades, en el marco de las ayudas Margarita Salas, para la Recualificación del sistema universitario español 2021-2023 convocadas por la Universidad Pablo de Olavide, de Sevilla.