Capítulo 3

La Directiva 2016/680/UE: un nuevo paradigma para el tratamiento de datos de carácter personal con fines penales

Juan Alejandro Montoro Sánchez[1]

Investigador Postdoctoral Margarita Salas[2]
Universidad Pablo de Olavide de Sevilla-Instituto de Justicia y Litigación "Alonso Martínez" de la Universidad Carlos III de Madrid

I. LA ERA DIGITAL: EL NUEVO ESCENARIO GLOBAL REGIDO POR LA TECNOLOGÍA Y EL TRATAMIENTO DE LA INFORMACIÓN

En las cuatro últimas décadas, aunque con más intensidad desde inicios del siglo XXI, estamos siendo testigos de la radical transformación, sin paragón en toda la historia de la humanidad, que está sufriendo la sociedad a nivel global. El incesante desarrollo y la alta penetración que presentan las cada vez más avanzadas e innovadoras Tecnologías de la Información y Comunicación (en adelante TICs) en prácticamente todas las esferas de nuestras vidas, pueden señalarse como dos de las principales causantes y motores de este este nuevo contexto mundial.

La expansión de las TICs ha llegado a tal punto, que es posible afirmar, sin miedo a equivocación, que resultan imprescindibles para realizar

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)".
2. Esta publicación ha sido financiada por la Unión Europea "NextGenerationEU", por el Plan de Recuperación, Transformación y Resiliencia 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.

la práctica totalidad de las tareas y actividades que llevamos a cabo en nuestro día a día. De hecho, es difícil pensar en algún reducto en que estas tecnologías no hayan encontrado alguna utilidad y conseguido implementarse de alguna manera. Así, las utilizamos como herramientas indispensables de nuestros puestos de trabajo, hacemos uso de ellas para comunicarnos y relacionarnos con nuestros familiares y amigos, para adquirir los bienes y servicios más tradicionales o los más punteros que se ofrecen el mercado o incluso para relacionarnos y hacer trámites con las Administraciones Públicas.

Podría decirse que es inconcebible que hoy día, una persona, incluidos los adolescentes menores de edad y nuestros mayores, no disponga de un teléfono inteligente[3] o que un hogar no cuente, al menos, con acceso a internet a través de fibra óptica[4]. Y es que hemos pasado en las últimas cuatro décadas, de vivir en una sociedad analógica, a estar inmersos en una sociedad plenamente digital ante la denominada revolución industrial 4.0[5]. Ha sido tal el nivel de la transformación, que difícilmente encajan en la sociedad actual o cuanto menos ven impedido el desarrollo de su vida cotidiana, aquellas minorías que rechazan la dependencia forzosa de estas tecnologías o aquellas otras que meramente no dominan su uso por razones de edad o por la dificultad de acceso a las mismas[6].

Ahora bien, si algo caracteriza a estas tecnologías disruptivas y a la multitud de servicios que han surgido en torno a ellas, es que su

3. De acuerdo con las últimas estadísticas publicadas por la CNMC sobre el sector de las telecomunicaciones, en agosto de 2022, existían en España, en activo, un total de 56896715 de líneas móviles, de las cuales 49.435.554 contaban además con servicio de acceso a internet de banda ancha. Es decir, existen más líneas en activo que población al existir una tasa de penetración –líneas/100 habitantes– de 107,5. Consultado en http://data.cnmc.es/datagraph/jsp/inf_anual.jsp (Último acceso, 20 de agosto de 2022).
4. En este caso, los datos de la CNMC arrojan un total de 16.710.090 líneas de banda ancha fija, lo que representa una tasa de penetración de 35,3. Consultado en http://data.cnmc.es/datagraph/jsp/inf_anual.jsp (Último acceso, 20 de agosto de 2022).
5. Se recomienda la lectura del excelente trabajo de BARONA VILAR, S., *Algoritmización del derecho y de la justicia: de la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, Valencia, 2021, pp. 42-76. En el mismo se hace un completo estudio de no sólo de las notas que caracterizan a la Revolución Industrial 4.0 en la que nos encontramos inmersos, si no que efectúa un completo recorrido histórico de las anteriores fases que se han sucedido hasta llegar al presente.
6. Especialmente preocupante es la situación de las personas mayores ante los usos impuestos de las TICS por parte de empresas y Administraciones Públicas, situación que ha contribuido a crear una importante brecha digital que incluso puede desembocar en situaciones de vulnerabilidad. *Vid*. CÍVICO ARIZA, A., "Vulnerabilidad de las personas mayores ante la brecha digital: análisis bibliométrico", en TORRES FERNÁNDEZ, C. (Coord.) *Avances y prospectiva en la protección jurídico-social de las personas en situación de vulnerabilidad*, Tirant lo Blanch, Valencia, 2022, pp. 223-239.

funcionamiento se sustenta fundamentalmente en una actividad primordial: el procesamiento de información. Y muy particularmente en el de la información que tiene carácter personal. Es decir, aquella que directa o indirectamente concierne a una concreta persona física identificada o que alternativamente puede identificarse por el prestador, sin un esfuerzo desproporcionado. Baste decir que sin la captación y el posterior tratamiento de datos personales, los proveedores se verían impedidos, sino de la prestación de los servicios digitales más extendidos y exitosos, de muchas de sus funcionalidades más relevantes y apreciadas por los consumidores.

Por ello, la carga de facilitar los datos recae, por lo general, en los propios usuarios, hasta el punto de que se ven obligados a entregarlos si desean hacer un uso plenamente funcional de tales herramientas. Así sucede, por ejemplo, con la información que se incorpora a los perfiles de las redes sociales[7] o con la información que se proporciona a los cada vez más usuales dispositivos y electrodomésticos del Internet de las Cosas (IoT)[8]. Otros datos, en cambio, se generan automáticamente durante el funcionamiento de los propios servicio o incluso se extraen deliberadamente por el proveedor a través del análisis inteligente del conjunto de datos de los usuarios, como ocurre respectivamente, con los datos de tráfico que resultan del uso de cualquier servicio de comunicaciones electrónicas y con de los perfiles de consumo y hábitos elaborados por los proveedores mediante herramientas de BigData o Inteligencia Artificial[9].

La paradoja de este panorama es que en la mayoría de los supuestos, tales datos se facilitan o generan incluso sin que los propios titulares sean plenamente conscientes de ello y del verdadero alcance de la cesión y de su destino. Prácticamente, ningún usuario se lee las extensas y complejísimas condiciones contractuales impuestas que regulan las prestaciones de dichos servicios[10]. Y es que no debe obviarse que tales datos se erigen

7. MARTÍNEZ MARTÍNEZ, R., "Protección de datos personales y redes sociales: un cambio de paradigma" en RALLO LOMBARTE, A. (Coord.) *Derecho y redes sociales*, Civitas, Cizur Menor, 2010, pp. 83-116.

8. ARELLANO TOLEDO, W., Privacidad e Internet de las Cosas: (Internet of Things, IoT) en *Revista de privacidad y derecho digital*, núm. 6, 2017, pp. 25-56.

9. CHAVES VALDIVIA, A. K., "Entre los perfiles a la carta y la protección de datos personales: el producto eres tú", en BUENO DE MATA, F. (Dir.) *Hacia una Justicia 2.0: actas del XX Congreso Iberoamericano de Derecho e Informática*, Ratio Legis, Salamanca, 2016, pp. 67-79.

10. En el estudio realizado por el Consejo Noruego del Consumidor en 2020 se estimó que la lectura detenida de las condiciones de uso de las aplicaciones y redes sociales más utilizadas puede llevar incluso más de una hora, superando el tiempo que habría que dedicar a obras literarias como Macbeth.. https://magnet.xataka.com/preguntas-no-tan-frecuentes/tiempo-que-tardarias-leer-terminos-condiciones-uso-tus-apps-grafico. (Última consulta, 20 de agosto de 2022).

además en moneda de cambio, puesto que constituyen la auténtica contraprestación para el proveedor por el acceso a las aplicaciones, habida cuenta de su carácter gratuito o del precio simbólico de la mayoría de estas. Es decir, el modelo de negocio arquetípico funciona del siguiente modo: los servicios se prestan gratuitamente a condición de que los datos que se capten de los usuarios y terceras personas puedan ser reutilizados y explotados empresarialmente por los operadores para otras finalidades comerciales distintas, que son las que les proporcionan el verdadero y principal beneficio económico.

Dada la extrema utilidad y el consecuente inmenso valor que han alcanzado los datos personales, no es de extrañar que a la actual época se la denomine la Era de la Información, o que a los datos personales se les califique como el petróleo del siglo XXI. Para confirmarlo no hay más que comprobar como las empresas con mayor capitalización bursátil a nivel mundial basan su modelo de negocio, directa o indirectamente, en el tratamiento y análisis de la información personal que recopilan masivamente a través de las aplicaciones y servicios que ofrecen al público, habiendo conseguido desplazar muchos puestos atrás a las compañías y corporaciones multinacionales cuyo negocio se ha centrado en la venta de bienes y servicios tradicionales y que hasta hace recientes fechas ocupaban dichos puestos[11].

II. LA DIRECTIVA 2016/680/UE: UN INSTRUMENTO PARA GARANTIZAR LA PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES DE LOS CIUDADANOS EN EL ÁMBITO PENAL

La utilidad de muchas de las categorías de datos personales que se procesan a través de las variadas tecnologías y herramientas digitales que están al alcance de la población, no se reduce a los fines meramente comerciales o técnicos previamente mencionados. Debido a la extraordinaria y variada información que albergan y a la que son susceptibles de revelar, ya sea por sí mismos o analizados en su conjunto, los datos de carácter personal son en la actualidad elementos esenciales del sistema de justicia penal[12], puesto que permiten a las autoridades implicadas el

11. A cierre del ejercicio 2021, siete de las diez primeras empresas con mayor valor a nivel global, son tecnológicas y utilizan los datos personales como fuente directa o indirecta de ingresos. Únicamente la petrolera saudí Aramco, se cuela entre las cinco primeras. https://cincodias.elpais.com/cincodias/2021/12/30/companias/1640886339_354215.html. (Última consulta, 20 de agosto de 2022).
12. ORTIZ PRADILLO, J. C., "Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos fundamentales en el proceso penal", *Diario La Ley*, núm.

desarrollo de las labores de investigación penal, el esclarecimiento de multitud de hechos de naturaleza criminal así como a la determinación de sus autores y partícipes. Máxime, en este momento en que gran parte de la delincuencia cuenta con, al menos, algún componente electrónico o digital en los medios o fines comisivos, lo que implica que necesariamente existan huellas digitales –datos personales en muchos supuestos– susceptibles de ser aprehendidas y utilizadas[13]. Dicho con otras palabras, los datos personales pueden convertirse en trascendentes evidencias y fuentes de prueba que pueden ser utilizados en las actividades llevadas a cabo por las autoridades policiales y judiciales de detección, investigación y enjuiciamiento de delitos. Y ello, hasta el punto de haberse erigido en elementos imprescindibles e inherentes a todo proceso penal, puesto que no es posible su normal desarrollo sin que exista un tratamiento, siquiera meramente identificativo de las partes y demás intervinientes, de datos personales. La localización de un terminal móvil en los alrededores de la escena del crimen, las muestras de fluidos corporales o las grabaciones de un sistema de videovigilancia son buena muestra de datos personales que sirven a tal capital función.

Por otro lado, debemos tener en cuenta que los datos y la información en formato electrónico cuentan con la gran ventaja de ser fácilmente conservables durante largos periodos de tiempo y dejar una huella digital, prácticamente indeleble, que permite asegurar, no solo su trazabilidad e integridad, sino incluso su fiabilidad[14]. Siendo consciente del gran potencial de los datos en el ámbito penal –e incluso en el sancionador administrativo– y de su alta disponibilidad, no sólo las autoridades recurren con más frecuencia a obtenerlos de proveedores y terceros como fuentes de prueba o incluso como cuerpo o efecto del delito en su sentido más amplio, sino que el propio legislador ha promovido la aprobación de normas encaminadas a la creación de diversas bases de datos tanto públicas como privadas con miras a conservar masiva y preventivamente, diversas categorías de datos personales vinculados a distintos ámbitos, por si algún momento resultaren necesarios para una concreta investigación penal. Es el caso de las bases de datos de tráfico de las comunicaciones electrónicas que los operadores de telecomunicaciones deben mantener en virtud de las obligaciones impuestas por la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas

9955, 2021, p. 3 y MONTORO SÁNCHEZ, J. A. *Uso y cesión de datos de carácter personal en el proceso penal*, Aranzadi, Cizur Menor, 2022, p. 331.

13. ORTIZ PRADILLO, J. C., "Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos fundamentales en el proceso penal", *op. cit.*, p. 3.
14. DELGADO MARTÍN, J., "La prueba electrónica en el proceso penal" en Diario La Ley, núm. 8167, 2013.

y a las redes públicas de comunicaciones[15] o la base de dato PNR –Passsenger Name Records– creada *ex* Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves[16].

Visto lo anterior, podría pensarse que tanto los operadores privados como las autoridades implicadas en la represión criminal cuentan con plena libertad para recopilar y hacer uso de los datos de carácter personal de los ciudadanos para perseguir sus propios intereses o ejercer las funciones pública que legalmente le competen. No obstante, nada más lejos de la realidad, toda vez que los datos de carácter personal cuentan con una férrea protección constitucional al situarse bajo el halo protector que brinda el derecho fundamental a la protección de datos de carácter personal, que en España se proclama en el art. 18.4 CE y en el ámbito europeo en el art. 8 tanto del Convenio Europeo de Derechos Humanos Mientras como de la Carta de Derechos Fundamentales de la Unión Europea.

Sobre este derecho, nuestro Tribunal Constitucional, en su célebre Sentencia 292/2000, de 30 de noviembre, ya determinó que se trataba de un derecho fundamental autónomo, distinto de la intimidad personal y familiar, de naturaleza instrumental, que tiene por misión proteger al individuo de los riesgos y peligros que pueden derivarse para los demás derechos reconocidos en el ordenamiento jurídico, de la utilización de sus datos de carácter personal por parte de terceros, incluido el Estado. Y para prestar dicha protección, otorga al titular, como contenido esencial, amplios poderes de control y disposición sobre sus propios datos, que le facultan para decidir cuáles proporciona a un tercero o cuáles puede este recabar, saber quién los posee y para qué finalidad, y oponerse a dicha posesión y uso. Además, para garantizar la efectividad de dichos poderes, se atribuyen al titular una serie de facultades de las que se derivan obligaciones de contenido positivo para el responsable del tratamiento, que se materializan a través de los conocidos por

15. COLOMER HERNÁNDEZ, I., "Uso y cesión de datos de las comunicaciones electrónicas para investigar delitos tras la STJUE de 21 de diciembre de 2016" en RUDA GONZÁLEZ, A. y JEREZ DELGADO, C. (Coords.) *Estudios sobre Jurisprudencia Europea: materiales del I y II Encuentro anual del Centro español del European Law Institute*, Sepín Editorial Jurídica, Las Rozas, pp. 767-781.

16. CATALINA BENAVENTE, M. A., *El uso de los datos PNR en el proceso penal*, Aranzadi, Cizur Menor, 2022 y CATALINA BENAVENTE, M. A., "Entrada en vigor de la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves" en *Diario La Ley*, núm. 9737, 2020.

su acrónimo como derechos ARCO –acceso, rectificación, cancelación y oposición–[17].

Ahora bien, habiendo transcurrido prácticamente cuarenta años desde que se aprobara la primigenia ley reguladora de este derecho fundamental, la ya derogada Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, hallamos un panorama prácticamente disfuncional en lo que atañe a la adecuada y genérica aplicación de las garantías dimanantes de este derecho en el ámbito de la justicia penal, lo cual no ha sucedido, en cambios, en otros ámbitos extrajurisdiccionales dónde también tienen cabida éstas. Por ejemplo, en el sector privado y en el ámbito de las Administraciones Públicas, nos encontramos con una aplicación bastante aceptable y prácticamente generalizada del grueso de la normativa, al menos desde que se aprobara la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal con la que se transpuso al ordenamiento nacional la primera norma europea sobre la materia, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. Si bien, es cierto que cuando se ha conseguido adquirir una verdadera cultura de cumplimiento y la consciencia de la importancia del respeto de la normativa, ha sido a raíz de la entrada en vigor del Reglamento General de Protección de Datos en el año 2016 –en parte por el peso de su rotundo régimen sancionador– y de la intensa y loable labor formativa y educativa llevada a cabo por la Agencia Española de Protección de Datos.

Lamentablemente, en la Administración de Justicia y particularmente en el orden jurisdiccional penal, el nivel de cumplimiento por parte de los órganos judiciales en el ejercicio de sus funciones jurisdiccionales no ha sido equivalente. Puede decirse que se arrastra un importante déficit en la observancia de las garantías asociadas a la privacidad, pese a la especial trascendencia que adquiere este derecho fundamental en el proceso[18]. Y es que, como veremos con posterioridad, la privacidad opera en el ámbito procesal con varias manifestaciones exclusivas que no tienen cabida en otros ámbitos extrajudiciales, que tienen la capacidad de provocar importantes consecuencias jurídicas. De hecho, únicamente en el aspecto organizativo de los medios informáticos utilizados en la oficina judicial es

17. Sentencia 292/2000, de 30 de noviembre de 2000. «BOE» núm. 4, de 4 de enero de 2001.
18. ORTIZ PRADILLO, J. C., "Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos fundamentales en el proceso penal", *op. cit*., p. 7 y PÉREZ GIL, J., "Investigación penal y nuevas tecnologías: algunos de los retos pendientes" en *Revista Jurídica de Castilla y León*, núm. 7, p. 226.

dónde puede haber existido un nivel más satisfactorio de cumplimento, pero en los aspectos puramente procesales, es más complicado verificar una escrupulosa observancia de los principios y obligaciones asociados al derecho a la protección de datos. Salvo casos aislados, la práctica judicial ha demostrado que no suele ir más allá de la mera incorporación a pie de resolución de un mero aviso informativo genérico y estereotipado dirigido a las partes, que en ningún caso no colma las exigencias legales mínimas requeridas.

Gran parte de esta problemática se debe a la inexistencia de un marco jurídico específico destinado a reglamentar las actividades de tratamiento de los datos personales por parte de la autoridad judicial. Las distintas leyes que han precedido al nuevo paquete legislativo aprobado por la Unión Europea en el año 2016, ni siquiera mencionaban a los Juzgados y Tribunales como destinatarios y operadores sujetos al cumplimiento de las garantías establecidas en las mismas. De hecho, la Directiva 95/46/CE, norma origen de la Ley Orgánica 15/1999, exceptuaba expresamente de su ámbito de aplicación al procesamiento de datos llevado a cabo por las autoridades con fines de salvaguarda de la seguridad pública y al destinado en materia penal[19]. Por su parte, aunque la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, sí resultaba aplicable a la actividad penal, excluía específicamente de su ámbito el tratamiento llevado a cabo por los órganos judiciales nacionales de los Estados miembros, pues se destinaba específicamente a establecer un nivel de protección mínimo a la información intercambiada mediante mecanismos de cooperación judicial y policial transnacional.

Tan solo en el año 2015, el legislador introdujo en la Ley Orgánica del Poder Judicial un pequeño capítulo de diez artículos[20] –236 *bis* a *decies*– con el objeto de dotar a la Administración de Justicia de un marco jurídico sobre la materia. No obstante, el mismo se limitaba a regular únicamente ciertos aspectos residuales, principalmente de carácter organizativo, por

19. Véase el art. 3.1 de la Directiva 95/46/CE sobre ámbito de aplicación en el que se especificaba que: *"Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales: – efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal…".*

20. Dicho marco jurídico se articuló a través de la Ley Orgánica 7/2015, de 21 de julio, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

lo que resultó claramente insuficiente, al no despejar la práctica totalidad de interrogantes que surgían en torno a la práctica procesal. Finalmente, la inercia de la costumbre en las prácticas judiciales, la falta de formación específica de los operadores jurídicos implicados en el proceso –jueces y magistrados, abogados y fiscales– y la inactividad del Consejo General del Poder Judicial como autoridad de control en la materia, han otros sido los demás factores que han contribuido a la latencia de este escenario de inobservancia general en detrimento de los derechos de los interesados.

No obstante, este panorama está llamado a cambiar a raíz de la aprobación de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Con ella el legislador europeo ha pretendido poner remedio a esta situación de incertidumbre estableciendo las bases de un marco jurídico común para los Estados miembros, con el potente objetivo de permitir la circulación e intercambio de datos personales con fines de represión del delito, garantizando a la par, un alto y homogéneo nivel de protección para los ciudadanos[21].

Se trata del instrumento legislativo revulsivo que está llamado a transformar radicalmente el modo en que todas las autoridades penales de los Estados miembros, pero especialmente, los juzgados y tribunales del

21. Para un estudio del proceso legislativo seguido para la aprobación de la Directiva y de sus fines y principios se recomienda la lectura de: PILLADO GONZÁLEZ, E., "Principios generales de protección de datos en la cesión de información en la persecución criminal a la vista de la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por la que se deroga la Decisión Marco 2008/977" en *Nuevos postulados de la cooperación judicial en la Unión Europea: libro homenaje a la Prof.ª Isabel González Cano*, MORENO CATENA, V. y ROMERO PRADAS, M. A. (Dirs.), Tirant lo Blanch, Valencia, 2021, pp. 783-820; COLOMER HERNÁNDEZ, I., "Control y límites en el uso de los datos personales penales en la investigación y represión de los delitos a la luz de la Directiva 2016/680" en *Nuevos postulados de la cooperación judicial en la Unión Europea: libro homenaje a la Prof.ª Isabel González Cano*, MORENO CATENA, V. y ROMERO PRADAS, M. A. (Dirs.), Tirant lo Blanch, Valencia, 2021, pp. 737-782 y FIODOROVA, A., "Directiva 2016/680: hacia mayor coherencia de protección de datos personales en la cooperación policial y judicial penal" en MORENO CATENA. V. y ROMERO PRADAS, M. I. (Dirs.) *Nuevos postulados de la cooperación judicial en la Unión Europea: libro homenaje a la Prof.ª Isabel González Cano*, Tirant lo Blanch, Valencia, 2021, pp. 709-736 y CARUANA, M., "The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement" en *International Review of Law*, Computers & Technology, núm. 33, 2019, pp. 249-270.

orden penal recopilan y procesan datos de carácter personal no sólo en las distintas fases del proceso penal, sino incluso en las actividades de índole preventiva. Y para ello, impone a los órganos judiciales, como autoridades competentes incluidas expresamente dentro de su ámbito de aplicación, toda una serie de principios, reglas y limitaciones de obligada observancia en todas las actividades y funciones en que tenga lugar el tratamiento de datos con la finalidad última de garantizar, en la medida de lo posible, los poderes de control y disposición que se atribuyen al interesado, en tanto que representan los ejes nucleares sobre los que se articula del derecho fundamental a la autodeterminación informativa.

Antes de examinar su contenido, es imprescindible señalar que la Directiva 2016/680/UE ha sido transpuesta al ordenamiento interno –con prácticamente tres años de retraso[22] y mediando la sanción más elevada impuesta por el Tribunal de Justicia de la Unión Europea hasta la fecha por incumplimiento del plazo máximo previsto en su articulado– a través de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Tal dilación, ha contribuido, sin duda alguna, y a pesar del indiscutible efecto directo de la Directiva, a prolongar innecesariamente el disfuncional escenario reinante en nuestros órganos judiciales penales respecto a las condiciones y garantías en que se desarrolla del tratamiento de datos.

Apuntado todo lo anterior, procede analizar, en primer lugar, las diferentes dimensiones con las que opera el derecho a la protección de datos en el marco del proceso penal, dado que ello permitirá obtener una panorámica de su trascendente influencia. Para después examinar las novedades más relevantes que se derivan de la aplicación efectiva de las medidas contempladas en la Directiva 2016/680, con particular énfasis en aquellas que presentan connotaciones procesales, y que en definitiva, veremos que son de tal alcance, que nos permiten colegir de un cambio de paradigma en lo que respecta al tratamiento de datos judicial encaminado a la investigación y enjuiciamiento del delito.

22. El art. 63 de la Directiva establecía como plazo límite para la adopción y publicación de las disposiciones legales, reglamentarias y administrativas necesarias para su transposición, el pasado 6 de mayo de 2018. Dado el retraso del legislador español, la Comisión Europea instó ante el Tribunal de Justicia de la Unión Europea, en fecha 4 de septiembre de 2019 un recurso por incumplimiento con arreglo a los artículos 258 TFUE y 260 TFUE, que dio lugar a la Sentencia de 25 de febrero de 2021, asunto C-658/19, en la que se condenó al Estado al abono de 15 millones de euros a tanto alzado y 89 mil euros por cada día de retraso adicional, todo ello en concepto de multa.

III. LAS DIMENSIONES DEL DERECHO A LA PROTECCIÓN DE DATOS EN EL PROCESO PENAL

El vínculo de conexión entre los datos personales y el proceso penal es particularmente estrecho e intenso. Podría decirse que ambas realidades son indisociables, dado que el tratamiento de datos se prolonga durante todo el desarrollo del proceso, a lo largo de sus distintas fases, sin perjuicio de que sea la instrucción la etapa en la que éste es especialmente relevante por su función recopiladora. Este vínculo es incluso más trascendente si atendemos a la operativa y los efectos con los que se presenta el derecho fundamental a la protección de datos de carácter personal en este ámbito. Y es que este tiene la particularidad de operar desde una perspectiva multidimensional[23] con manifestaciones propias y exclusivas de este entorno que no concurren en otros ámbitos. Procede analizar brevemente a cada una de estas dimensiones y las implicaciones que se derivan de las mismas, puesto que nos permitirá comprobar el importante alcance y repercusión de este derecho fundamental en la justicia penal.

1. DERECHO A LA PROTECCIÓN DE DATOS COMO DERECHO SUBJETIVO: DIMENSIÓN SUSTANTIVA

El derecho fundamental a la protección de datos de carácter personal despliega sus efectos en el marco del proceso judicial a través de su dimensión puramente sustantiva. Esto es, desde su vertiente de derecho subjetivo reconocido a la persona física que atribuye a su titular un haz de facultades positivas, en este caso frente al órgano judicial como responsable del tratamiento, en aras de permitirle el control y el poder de disposición que ostenta sobre sus propios datos personales. Mientras, por su parte, el órgano judicial como responsable del tratamiento, se encuentra sometido a la obligación de dar oportuno cumplimiento a los deberes dimanantes de este

23. MARCOS AYJÓN también destaca las diversas implicaciones del derecho fundamental a la protección de datos en el proceso, mas solo respecto al orden penal, exponiendo que: "*… desde todos los aspectos posibles, se puede estructurar en tres apartados perfectamente diferenciados: 1.º En el ámbito organizativo y de gestión, donde el Letrado de la Administración de Justicia cumple un papel principal. 2.º En el ámbito procesal, ya sea en el aspecto referido a recabar pruebas con pleno respeto al derecho fundamental a la protección de datos de carácter personal, o cuando se accede a los datos e información contenidas en el proceso penal. 3.º En el aspecto sustantivo: Los delitos que protegen el derecho fundamental a la protección de datos de carácter personal*". MARCOS AYJÓN, M., "Protección de datos personales y Letrado de la Administración de Justicia. Un difícil encaje en el marco legal actual" en GUTIÉRREZ ZARZA, M. A. (coord.) *Los retos del espacio de Libertad, Seguridad y Justicia de la Unión Europea en el año 2016: Reunión anual ReDPE*, Wolters Kluwers, Madrid, 2016. En el mismo sentido MONTORO SÁNCHEZ, J. A., *Uso y cesión de datos de carácter personal en el proceso penal*, *op. cit.*, pp. 252-253.

derecho, especialmente el de información así como a dar curso a las solicitudes de derechos ARCO que le sean planteadas respecto al tratamiento que efectúe de los datos personales de los interesados en tanto ejercita la función jurisdiccional. Se trata ésta, de la faceta genuina de este derecho fundamental, correspondiendo a la que se extiende genéricamente a cualquier ámbito en el que sea de aplicación la normativa de protección de datos. En cualquier caso, habida cuenta del cúmulo de derechos e intereses privados y públicos que intervienen en el proceso, el derecho a la protección de datos puede verse modulado en diferentes grados de afección. Por tal motivo, nos encontramos con un régimen específico y modulado de este derecho el orden jurisdiccional penal, que permita aunar el interés del Estado en la represión del delito con los derechos fundamentales de los intervinientes en el mismo. Nos encontraríamos, por tanto, ante una dimensión del derecho a la protección de datos que, aunque vinculada al proceso en tanto que se trata de una fuente de tratamiento de datos personales ante la que despliega su cobertura protectora, carece de naturaleza procesal alguna y actúa, por tanto, en paralelo, desligada del desarrollo y desenlace del proceso. Incluso en el plano legal la normativa de protección de datos atinente a esta faceta discurre de forma separada y no convergente respecto de la normativa procesal en sentido estricto, sin perjuicio de la existencia de algún aspecto que puntual y tangencialmente pueda afectar a este derecho.

2. DERECHO A LA PROTECCIÓN DE DATOS COMO CONDICIONANTE DE LA ORGANIZACIÓN DE MEDIOS DE LOS ÓRGANOS JUDICIALES

Muy ligada a la anterior dimensión, e incluso pudiendo tildarse como su complemento indispensable, el derecho a la protección de datos afecta a la justicia penal desde una perspectiva organizativa. Así tanto el personal perteneciente a la Administración de Justicia, como los medios materiales –especialmente los sistemas y aplicaciones informáticas que intervienen en el tratamiento– que se utilizan y contribuyen en el desarrollo de la actividad jurisdiccional, deben estar orientados y configurados de tal modo que permitan garantizar los principios organizativos y de seguridad reconocidos en la normativa de protección de datos y con ello, la seguridad e integridad de los datos. Ello se traduce en la necesidad adaptar toda la organización judicial a una serie de políticas, directrices, reglas y prácticas que tiendan a garantizar la seguridad e integridad de los datos y con ello los derechos de los interesados cuyos datos son tratados[24].

24. Para un estudio más detallado y pormenorizado de las medidas de seguridad y sus implicaciones en la organización, puede consultarse: TRONCOSO REIGADA, A.,

Aspectos nucleares de esta dimensión del derecho lo constituyen el respeto a las exigencias de seguridad establecidas en el art. 29 y siguientes de la Directiva, la preceptiva realización de la evaluación de impacto y la observancia escrupulosa de los principios de protección de datos desde el diseño y por defecto[25] que deben tenerse en cuenta a la hora de desarrollar e implementar soluciones tecnológicas, protocolos y prácticas por parte de las Administraciones encargadas de proveer las herramientas técnicas utilizadas por los órganos judiciales.

3. DERECHO A LA PROTECCIÓN DE DATOS COMO LÍMITE A LA ACTIVIDAD INVESTIGATORIA Y A LA ACTIVIDAD PROBATORIA

El derecho fundamental a la protección de datos puede operar además en el ámbito del proceso bajo una dimensión puramente procesal, dado que es susceptible de condicionar el modo en que se realizan diversos actos y fases del proceso. Ello viene determinado por la consideración del derecho fundamental que se ve afectado por ciertas actividades procesales de investigación propias de la fase de instrucción penal y en algunos casos por la actividad probatoria pueden efectuar las partes, habida cuenta de que requieren del desarrollo previo de operaciones que suponen un tratamiento de datos de carácter personal. Así pues, el derecho a la protección de datos se constituye como afirmó la Segunda del Tribunal Supremo en su sentencia 471/2017 de 23 de febrero en "*una fuente de limitación de la actividad estatal, en la medida en que la vulneración en el proceso de derechos y libertades fundamentales del investigado abre una grieta en la estructura misma del proceso penal y puede generar efectos contaminantes no solo respecto de las pruebas así obtenidas sino también en lo que concierne a otros actos procesales conectados con las mismas*". Por tanto, la adopción y ejecución de diligencias de investigación de las que se desprenda una aprehensión, recogida o

"La seguridad en el Reglamento General de Protección de Datos de la Unión Europea" en *Actualidad administrativa*, núm. 1, 2019; RECIO GAYO, M., "Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control" en PIÑAR MAÑAS, J. L. (Dir.) *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016, pp. 351-366 y PRADA ESPINA, D., "Análisis y gestión de riesgos de los tratamientos 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*, Reus, Madrid, 2018, pp. 349-374.

25. DUASO CALÉS, R., "Los principios de protección de datos desde el diseño y protección de datos por defecto" en PIÑAR MAÑAS, J. L. (Dir.) R*eglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016, pp. 295-320.

tratamiento de datos deben producirse con pleno respeto al derecho fundamental, lo que exige la toma en consideración de los principios rectores y demás reglas establecidas en la Directiva como elementos adicionales tradicionales establecidos en la Ley de Enjuiciamiento Criminal. Idéntico planteamiento puede ser extrapolado a la actividad de obtención y práctica de fuentes de prueba en el plenario. Los efectos de la transgresión de dichas prácticas es susceptible de provocar, en los supuestos más graves, la exclusión e ineficacia procesal de los resultados de dichas diligencias o de las fuentes de prueba por operatividad de la regla establecida en el art. 11.1 LOPJ[26].

4. DERECHO A LA PROTECCIÓN DE DATOS COMO LÍMITE LA TRANSFERENCIA E INTERCAMBIO DE DATOS ENTRE AUTORIDADES PENALES INTERNACIONALES

La última de las facetas con las que este derecho fundamental se presenta guarda relación con uno de los objetivos perseguidos por el legislador europeo en la Directiva 2016/680: la libre circulación e intercambio de datos personales entre autoridades de los Estados miembros y de terceros. Si bien este se marca como un objetivo perseguido, no es menor cierto, que también está sujeto a estrictas limitaciones para garantizar los derechos de

26. Alcanzan las mismas conclusiones: COLOMER HERNÁNDEZ, I., "Control y límites en el uso de los datos personales penales en la investigación y represión de los delitos a la luz de la Directiva 2016/680" en Nuevos postulados de la cooperación judicial en la Unión Europea: libro homenaje a la Prof.ª Isabel González Cano, MORENO CATENA, V. y ROMERO PRADAS, M. A. (Dirs.), Tirant lo Blanch, Valencia, 2021, pp. 737-782; GUTIÉRREZ ZARZA, M. A., "La protección de datos personales como derecho fundamental del imputado, ¿también en el ámbito del proceso penal?" en *La ley penal: revista de derecho penal, procesal y penitenciario*, núm. 71, 2010; PÉREZ ESTRADA, M. J., "Efectos de la vulneración de la protección de los datos personales en el proceso penal" en *La Ley Penal: revista de derecho penal, procesal y penitenciario*, núm. 135, 2018; FRÍAS MARTÍNEZ, E., "Obtención de datos personales en procesos penales y administrativos" en *Diario La Ley*, núm. 9404, 2019; DELGADO MARTÍN, J., "Protección de datos y prueba en el proceso" en *Diario La Ley*, núm. 9383, 2019 y CASERO LINARES, L., "Nulidad de la prueba por vulneración de los principios y derechos sobre protección de datos" en GUTIÉRREZ ZARZA, M. A. (coord.) *Nuevas Tecnologías, protección de datos personales y proceso penal*, La Ley, Las Rozas, 2012, pp. 399-400; AZAUSTRE RUÍZ, P., "Acercamiento al régimen jurídico-procesal previsto para la utilización de la información obtenida en un proceso penal distinto" en COLOMER HERNÁNDEZ, I. (Dir.) *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios*, Aranzadi, Cizur Menor, 2017, pp. 345-366 y GÓMEZ ÁLVAREZ, F. J., "La cesión de datos de carácter personal entre procesos penales ante la doctrina del tribunal constitucional y el nuevo marco normativo de la protección de datos de carácter personal" en COLOMER HERNÁNDEZ, I. (dir.) *Uso y cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios*, Aranzadi, Cizur Menor, 2019, pp. 69-118.

los interesados. En un marco de cooperación judicial cada vez más desarrollado, que pivota sobre el reconocimiento mutuo y el principio de disponibilidad, el derecho a la protección de datos aparece como un límite a dichos intercambios. Por tal motivo, se requiere que el ordenamiento jurídico del Estado o el instrumento convencional de la organización internacional al que se destinen los datos garantice niveles de protección de este derecho, al menos equivalentes a los de la Unión Europea.

IV. LOS PRINCIPIOS RECTORES DEL TRATAMIENTO DE DATOS EN LA JUSTICIA PENAL

En el Capítulo II de la Directiva 2016/680, que tiene como rúbrica "Principios" se enuncian una serie de reglas y fundamentos heterogéneos sobre los que se articula todo el sistema de protección de datos[27]. Estos principios vertebradores constituyen el núcleo fundamental de las obligaciones que incumben a los órganos judiciales como autoridades responsables del tratamiento, motivo por el que deben ser observados minuciosa y diligentemente a lo largo de todas las fases del tratamiento[28].

Son, por tanto, elementos que gozan de especial trascendencia en la materia puesto que se erigen en parámetros de referencia para la toma de decisiones y el aseguramiento de una respuesta respetuosa con los derechos fundamentales[29]. Es más, estos actúan como auténticos principios informadores, en tanto en cuanto permiten extraer criterios con los que cubrir las lagunas normativas que puede surgir ante la ausencia de soluciones específicas en la legislación sectorial. Por su parte, a los interesados, el modo en que se apliquen estos principios les permiten valorar la adecuación del tratamiento llevado a cabo por la autoridad judicial a las exigencias que dimanan del derecho a la protección de datos y su regulación. Por tanto, su inobservancia, especialmente en la adopción o ejecución de

27. 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*, Civitas, Cizur Menor, 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.
28. *Vid*. 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*, Civitas, Cizur Menor, 2010, pp. 340-343.
29. PILLADO GONZÁLEZ, E., "Principios generales de protección de datos en la cesión de información en la persecución criminal a la vista de la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por la que se deroga la Decisión Marco 2008/977", *op. cit*., pp. 783-820.

diligencias de investigación, podrá servir a las partes como motivo para impugnar e intentar excluir datos del proceso que se hayan tratado sin la suficiente adecuación. Motivo por el que los órganos instructores deben velar especialmente por su estricto cumplimiento. Y es que, a pesar de que los mismos no se dispongan expresamente en la Ley de Enjuiciamiento Criminal, es posible colegir que los mismos adquieren una relevancia procesal indiscutible, hasta el punto de que deben ser tenidos en cuenta por el juez, de forma adicional a los principios rectores genéricos establecidos en el art. 588 bis a) LECrim, cuando se adopte una medida de investigación de la que se derive el tratamiento de datos.

Estos principios rectores se proclaman en el art. 4 de la Directiva –art. 6 de la Ley Orgánica 7/2021–, encontrándose entre éstos: el principio de licitud; principio de lealtad; principio de limitación de la finalidad del tratamiento; principio de minimización; principio de exactitud; principio de seguridad y principio de proactividad. No obstante, nos centraremos en el estudio de los que cuentan con un mayor protagonismo en el ámbito procesal.

1. PRINCIPIO DE LICITUD

Es el art. 8 de la Directiva 2016/680/UE el que conceptúa y configura a este principio rector. En virtud del mismo, el tratamiento de datos será lícito cuando se cumplan acumuladamente los siguientes presupuestos: 1) Como presupuesto subjetivo, que se acometa por una autoridad competente del sistema de justicia penal. En este caso, los tribunales de dicho orden jurisdiccional lo son. 2) Como factor teleológico, que el tratamiento de datos tenga por finalidad la investigación o enjuiciamiento de un delito, o la ejecución de una pena. 3) Como factor legitimador, que la autoridad cuente con la correspondiente habilitación legal para el tratamiento de los datos que se pretenden procesar. Reserva de ley que viene motivada por la necesaria adecuación que debe existir entre la medida restrictiva de derechos fundamentales a la que nos enfrentamos y los cánones y parámetros de proporcionalidad y necesariedad establecidos en la Carta de Derechos Fundamentales de la Unión Europea y la jurisprudencia del Tribunal Europeo de Derechos Humanos. 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 constante jurisprudencia[30].

30. 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

En base a lo expuesto, toda obtención de datos que se consiga sin cobertura legal específica debe reputarse ilícita, y en consecuencia, los datos así obtenidos no deberían teóricamente tener entrada en el proceso de conformidad con la regla prevista en el art. 7.3 de la Directiva 2016/680. Lo cierto es que en nuestro ordenamiento encontramos en el art. 236 ter LOPJ una cláusula general habilitante para el tratamiento de datos por parte de los órganos judiciales. No obstante, es imprescindible advertir que el tratamiento de categorías de datos sensibles o especialmente protegidos a los que se hace referencia en el art. 10 de la Directiva 2016/680 –datos relativos a la salud, vida sexual y genética, a las creencias y convicciones internas de todo tipo, datos biométricos, etc.–, requiere de una base legal específica que habilite el tratamiento[31] habida cuenta de su naturaleza y la especial capacidad que presentan para revelar aspectos nucleares sobre la vida privada de las personas. Es decir, la base legitimadora del art. 236 *ter* LOPJ no ampara, por sí misma, la obtención de datos pertenecientes a estas categorías especiales, si no que se exige una reserva de ley específica. En el ordenamiento jurídico podemos encontrar diversos ejemplos de habilitaciones específicas para el acceso y uso de dichos datos por los órganos judiciales penales, como la prevista 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

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 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]"*.

31. El art. 10 de la Directiva exige para su tratamiento una autorización específica y concreta para la autoridad en el ordenamiento interno o de la Unión, únicamente cuando los datos fueren manifiestamente públicos o el uso fuere imprescindible proteger los intereses vitales del interesado o de otra persona física, podrían tratarse sin esa base.

clínica respecto del acceso al historial clínico y datos de salud o la prevista en el art. 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria respecto a los datos con trascendencia tributaria. No obstante, debe advertirse que existen ciertos datos sensibles, como los relativos a convicciones religiosas o la vida sexual, que no cuentan con dicha habilitación, lo que impide teóricamente su utilización en el proceso penal.

2. PRINCIPIO DE LIMITACIÓN DE LA FINALIDAD DEL TRATAMIENTO

El principio de limitación de la finalidad puede 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, 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 mediante una medida de investigación– y su posterior tratamiento deben obedecer, necesariamente, a la consecución de unos fines perfectamente definidos. A su vez, estos fines pueden interpretarse en dos sentidos diferenciados[32]. En primer lugar, como fines generales para los que la autoridad está legalmente habilitada a actuar, que en este caso sería la investigación o enjuiciamiento de unos actos delictivos o para la ejecución de una pena. En segundo, como fines específicos, y que se refieren al concreto delito que se pretende investigar o enjuiciar o a la pena que se pretende ejecutar, y que por lo tanto deben ser correctamente predefinidos por la propia autoridad judicial con carácter previo a la obtención del dato a través de la resolución habilitante que permita su recogida o tratamiento.

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.

32. RODRÍGUEZ-MEDEL NIETO, C., "La Directiva 2016/680 relativa a la protección de las personas físicas en el tratamiento de sus datos personales para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales" en ARANGÜENA FANEGO, C. y HOYOS SANCHO, M. (Dirs.) *Garantías procesales de investigados y acusados: situación actual en el ámbito de la Unión Europea*, Tirant Lo Blanch, Valencia, 2018, pp. 381-420.

Ello implica que, en principio, los órganos judiciales se verían impedidos de destinar los datos obrantes en un sumario que han sido obtenidos para investigar un concreto delito, para ser utilizados en la investigación o enjuiciamiento de otros delitos distintos. Es decir, existe una prohibición de transmutar o ampliar los fines específicos a los que se destinan los datos personales que obran en poder de un órgano judicial.

No obstante, en nuestro ordenamiento procesal encontramos dos preceptos que chocan frontalmente con este planteamiento. Nos referimos a los arts. 579 *bis* y 588 *bis* i) LECRim, los cuales permiten la reutilización de datos obtenidos en un procedimiento en otro distinto, bien como medio de investigación o como fuente de prueba, sin ningún tipo de límite.

Lo cierto es que la Directiva 2016/680 prevé en el apartado 2.º del artículo 4 una regla excepcional a dicho 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, a unos fines penales distintos y desconectados de los que motivaron su recogida inicial. En cualquier caso, esta cesión de datos está fuertemente restringida y para que se repute conforme con las garantías del derecho fundamental a la protección de datos exige que concurran acumuladamente los siguiente requisitos.

1) 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. 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.

2) En segundo lugar, que el nuevo tratamiento pretendido debe ser necesario y proporcionado con relación a los nuevos fines. Es decir, cada cesión debe ser individualmente sometida a un previo juicio de proporcionalidad desde la óptica de la jurisprudencia constitucional y del Tribunal Europeo de Derechos Humanos, que atienda a las circunstancias específicas de cada caso y a los derechos e intereses confrontados.

De este modo, únicamente cuando se supere dicho filtro, debería operar la regla de reutilización establecida en la LECrim y permitirse la limitación del principio de finalidad del tratamiento[33].

3. PRINCIPIO DE MINIMIZACIÓN

El principio de minimización de los datos, se establece en el art. 4.1c) Directiva 2016/680. En su virtud, los datos personales que se traten por una autoridad judicial deben de ser *"adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados"*. Como puede comprobarse, mediante este principio se persigue minimizar, en la medida de lo posible, el número de datos personales que se tratan para conseguir unos fines concretos[34]. Por ello, la autoridad debe de ceñirse, de modo estricto, a la recopilación y utilización de aquellos datos que resulten imprescindibles para lograr los fines perseguidos. De esta manera, se consigue reducir el riesgo de afección sobre aquella de la privacidad superflua para la investigación del delito. Se trata, por tanto, de una limitación que afecta a la actividad que desarrolla la autoridad judicial, tanto a nivel cuantitativo como cualitativo.

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 y pertinencia. Elementos que implican en primer lugar que los datos deben ser apropiados para el tratamiento[35] y además tener cierta relevancia para el alcance del fin perseguido respectivamente.

En segundo lugar, este principio conculca que los datos personales que se traten deben de limitarse a aquellos estrictamente necesarios en

33. Idéntica conclusión alcanzan LÓPEZ JIMÉNEZ, R., "Régimen jurídico de los datos personales obtenidos en los descubrimientos casuales durante la investigación de los delitos" en COLOMER HERNÁNDEZ, I. (Dir.) *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios*, Aranzadi, Cizur Menor, 2017, pp. 315-343 y AZAÚSTRE RUÍZ, P., "Acercamiento al régimen jurídico-procesal previsto para la utilización de la información obtenida en un proceso penal distinto"…*op. cit.*, pp. 345-366.

34. 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"…*op. cit.*, p. 345.

35. 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. 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. *Vid*. 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*, Editorial Reus, Madrid, 2016, p. 135.

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 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.

Las implicaciones procesales de este principio son notorias, especialmente durante la fase de instrucción y la adopción de medidas limitativas de derechos orientadas a la recopilación de datos en soporte papel o digital. Véase como 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. Requiere por tanto, una especial diligencia del órgano judicial, e incluso una labor proactiva en favor de los derechos fundamentales del interesado que pueden verse injeridos por la medida a adoptar.

Más complejo resulta el estricto 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.

4. PRINCIPIO DE LIMITACIÓN DEL PLAZO DE CONSERVACIÓN

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.

Consecuentemente, una vez que los datos dejen de ser útiles para los fines perseguidos, debe de procederse a su borrado definitivo, evitando de este modo prolongar su uso o facilitar su destino a otros fines[36]. 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. No obstante, dada la incertidumbre temporal que acontece con la duración de un proceso y sus diferentes modos de resolución, lo cierto es que no es posible predefinir dichos plazos de modo absoluto, operando los plazos relativos definidos en el art. 588 *bis* k) LECrim. En cualquier caso, es necesario enfatizar en la necesariedad de que al término de los plazos, el órgano judicial adopte las medidas necesarias para que se proceda a la correcta destrucción de los datos y de todas las copias que pudieran conservarse en manos de la Policía Judicial cuando hubieren intervenido en su obtención.

5. PRINCIPIO DE PROACTIVIDAD O RESPONSABILIDAD ACTIVA

Como colofón a los principios rectores vinculados al tratamiento de datos, el legislador europeo ha introducido *ex novo* al principio responsabilidad activa o proactividad[37], que se recoge en los arts. 4.4 Directiva 2016/680/UE. 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. Éste se proclama bajo la siguiente consigna: *"El responsable del 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

36. *"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.

37. Los términos de responsabilidad activa o proactividad –tal y como ha sido señalado mayoritariamente por la doctrina– han sido los vocablos utilizados para la traposición 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, p. 120 y MARTÍNEZ MARTÍNEZ, R. "Diligencia y responsabilidad en protección de datos: la llamada accountability" en *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.

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[38]. 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 al propio interesado, a la autoridad de control o incluso a las instancias superiores que pudieran conocer de recursos planteados frente a cuestiones que afectaren a la obtención y posterior tratamiento de datos. 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[39], máxime ostentando el juez la posición de garante de sus derechos.

6. EL AUTO MOTIVADO: RESOLUCIÓN IMPRESCINDIBLE PARA LA OBTENCIÓN DE DATOS

De acuerdo con lo establecido en el art. 141 LECrim, las resoluciones que adopten forma de auto serán siempre fundadas, contendrán en párrafos separados y numerados los antecedentes de hecho y los fundamentos de derecho y, por último, la parte dispositiva, debiendo ser firmados por el juez o magistrado. Prosigue el precepto preceptuando que revestirán forma de auto las resoluciones del juez, que entre otros aspectos, decidan sobre *"la admisión o denegación de prueba (…) o afecten a un derecho fundamental…"*. Por su parte, el art. 588 *bis* c) LECrim exige que las medidas

38. 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*, Wolters Kluwer, Las Rozas de Madrid, 2019, p. 975.

39. 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".

de investigación tecnológica sean adoptadas por el juez de instrucción durante dicha fase se acordarán mediante auto motivado, una vez oído el Ministerio Fiscal.

Cuando en la práctica forense debe adoptarse una medida de investigación tecnológica –o incluso una tradicional no tecnológica– de las expresamente reguladas en Ley de Enjuiciamiento Criminal, no hay dudas sobre la necesariedad de que se recoja en un auto motivado de acuerdo con los preceptos anteriormente citados y que haga mención al contenido mínimo exigible en el art. 588 bis c) LECrim. Sin embargo, no es infrecuente que todavía, cuando se pretenden obtener datos personales como medio de investigación o fuente de prueba a través de un requerimiento efectuado a un tercero o una de las partes del proceso, se continue utilizando la providencia –recordemos que es una resolución inmotivada– como modalidad escogida de resolución habilitante o mediante auto carente de motivación o insuficiente.

Habiendo constatado a lo largo de este trabajo que de acuerdo con la jurisprudencia europea toda recopilación de datos personales constituye por sí misma una injerencia en el derecho fundamental a la protección de datos, con independencia del uso que posteriormente se efectúe de los mismos y de su propia naturaleza, no cabe duda de que el auto debe ser la resolución que debe adoptarse para su obtención en cualquier caso– ya sea mediante requerimiento o a través de una medida limitativa de derechos–, lo que nos lleva a descartar a la providencia como resolución apta para tal finalidad. Y es que como tiene establecido la doctrina constitucional acerca de los requisitos necesarios para la adopción de una medida restrictiva de derechos fundamentales, ésta debe de estar *"prevista por la Ley, [debe ser] adoptada mediante resolución judicial especialmente motivada, y que sea idónea, necesaria y proporcionada en relación con un fin constitucionalmente legítimo"*. Resolución que además deberá exponer las razones que justifiquen la adopción de la medida y la posible contribución a la investigación o enjuiciamiento[40].

Pero amén de los anteriores puntos, debemos hacer énfasis en la necesidad de que cuando se pretenda obtener datos de carácter personal, el juez deberá de justificar y motivar de modo suficiente e independiente la adecuación de la medida a los principios rectores del derecho a la protección de datos que puedan verse implicados. De este modo, será imprescindible hacer mención a la base legitimadora del tratamiento de los

40. MORENO CATENA, V., *Derecho Procesal Penal*, Colex, Madrid, 1997, p. 266 y SSTEDH de 25 marzo 1998, *Kopp*, de 30 julio 1998. En el plano constitucional son relevantes las SSTC 299/2000, 236, 171, 166, 141 y 49/1999, 229 y 58/1998.

datos, en función de su naturaleza y tipología; se deberá especificar los fines concretos a los que los datos se destinan, es decir al delito o delitos objeto de investigación; y se deberán de delimitar del modo más estrecho posible los datos o categorías de datos que deben ser objeto de entrega o aprehensión, ponderando la imposibilidad de obtener dicha información a través de otros medios distintos menos lesivos para la privacidad. La insuficiencia de dicha motivación, podrá servir de base indiscutiblemente para impugnar la resolución judicial habilitante, hasta el punto de conseguir su ineficacia procesal y la imposibilidad de utilización de los datos obtenidos.

V. EL DEBER DE INFORMACIÓN

Los arts. 12 y 13 de la Directiva 2016/680 imponen a la autoridad judicial responsable del tratamiento que procese datos de carácter personal en el ejercicio de sus competencias, la obligación de cumplir con el deber de información con los interesados cuya información se vea afectada en el curso de una investigación o proceso penal. Y ello con independencia de la posición que ocupe el titular en el proceso, o incluso de que sus datos se utilicen de forma accidental, como sucede en el caso de que los datos pertenezcan a un tercero que se ve afectado por una medida restrictiva de derechos sin tener la condición de investigado.

La información que debe prestarse, relacionada en el segundo de los preceptos citados[41], se refiere principalmente a los principales parámetros que caracterizarán las operaciones de tratamiento que se van a desarrollar y a las facultades y derechos que asisten al interesado respecto al uso. Se trata, en definitiva, del derecho del interesado a recibir una síntesis de los elementos esenciales que configuran el tratamiento al que se van a someter sus datos personales, con el objeto de que pueda tomar consciencia

41. En particular, la autoridad judicial está obligada a poner en disposición del interesado, al menos, la siguiente información: *"a) La identificación del responsable del tratamiento y sus datos de contacto. b) Los datos de contacto del delegado de protección de datos, en su caso. c) Los fines del tratamiento a los que se destinen los datos personales. d) El derecho a presentar una reclamación ante la autoridad de protección de datos competente y los datos de contacto de la misma. e) El derecho a solicitar del responsable del tratamiento el acceso a los datos personales relativos al interesado y su rectificación, supresión o la limitación de su tratamiento"*. Y además, atendiendo a las circunstancias del caso concreto, deberá de trasladar asimismo los siguientes datos: *"a) La base jurídica del tratamiento. b) El plazo durante el cual se conservarán los datos personales o, cuando esto no sea posible, los criterios utilizados para determinar ese plazo. c) Las categorías de destinatarios de los datos personales, cuando corresponda, en particular, los establecidos en Estados que no sean miembros de la Unión Europea u organizaciones internacionales. d) Cualquier otra información necesaria, en especial, cuando los datos personales se hayan recogido sin conocimiento del interesado"*.

del tratamiento y verificar *ab initio* y durante todo el periodo en que se prolongue éste, la adecuación y mantenimiento de éste a los principios y garantías establecidos en la legislación, y a la par, asistirle en el ejercicio de las eventuales acciones y facultades que le corresponden como titular de los datos en aras de garantizar el cumplimiento de la legislación. Nos encontramos ante un derecho cuya función principal es asegurar la plenitud de las facultades de control y disposición inherentes al derecho a la protección de datos de carácter personal, pues como concluyera al respecto la STC 292/2000, de 30 de noviembre, en su Fundamento de Derecho 6.º, *"el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado (…). Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin"*. Debe advertirse que este derecho posee un contenido y fines distintos a los derechos informativos estrictamente procesales que derivan de la Directiva 2012/13/UE del Parlamento Europeo y del Consejo, de 22 de mayo de 2012, relativa al derecho a la información en los procesos penales.

Por tanto, nos situamos ante una obligación de la autoridad que adquiere especial relevancia en la materia junto al elenco de derechos ARCO, tal y como ha confirmado el TJUE, habida cuenta de que es el medio que permite a los interesados tener constancia de que sus datos han sido recopilados y son tratados por un órgano judicial concreto, a efectos de poder ejercitar cualquiera de las facultades reconocidas en le legislación sectorial, reclamar la tutela de la autoridad de control o plantear los recursos que procedan para impugnar el tratamiento[42].

Si bien dicha información debe proporcionarse a la mayor brevedad tras la recogida de los datos, lo cierto es que en ciertos supuestos es posible retrasar el cumplimiento de dicho deber, aunque no anularlo. En concreto cuando su prestación pueda obstaculizar, comprometer o perjudicar una investigación o enjuiciamiento penal en curso o poner en riesgo la seguridad nacional o los derechos y libertades fundamentales de un tercero. No obstante, el uso de dichas causas debe estar plenamente justificada y una vez desaparecida el órgano judicial deberá de comunicar al interesado la información exigida[43].

42. Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2020, *La Quadrature du Net*, C-511/18, C-512/18 y C-520/18, apartados 190-192.

43. Dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, apartados 222-224.

VI. CONCLUSIONES

Tal y como hemos podido comprobar a lo largo del presente trabajo, el derecho a la protección de datos es un instituto protector de los demás derechos del ordenamiento jurídico que pueden verse en riesgo por razón del uso de datos personales, que ha adquirido una relevancia inusitada en esta época caracterizada por la digitalización de la sociedad y la penetración de las tecnologías de la información y comunicación en todas las facetas de nuestra vida cotidiana. No obstante, a la par, los datos personales objeto de protección por dicho derecho, se erigen en elementos indispensables del proceso penal, que se incorporan a este como medios de investigación o fuentes de prueba especialmente fructíferos para el esclarecimiento de los delitos en general y particularmente los que presentan un componente informático o telemático.

Hasta recientes fechas y por lo general, cuando las autoridades judiciales tenían que recurrir a la obtención de datos, no proporcionaban un tratamiento que tuviera en cuenta las garantías y limitaciones dimanantes del derecho fundamental a la protección de datos para los interesados, pese a tener plena vigencia. Podría decirse que primaba el interés público en el uso de los datos para el esclarecimiento de los hechos delictivos. Ello desde luego ha supuesto que durante un largo espacio de tiempo ha existido un escenario judicial en el que las injerencias e intromisiones excesivas, injustificadas o inmotivadas en la esfera de la privacidad han sido una constante.

No obstante, este panorama ha venido a solventarse de la mano del paquete legislativo en materia de protección de datos aprobado en el seno de la Unión Europea en el año 2016. A través del mismo se ha incorporado al ordenamiento europeo una Directiva específica, con la que se pretende extender las garantías tradicionalmente vinculadas a este derecho, aunque con ciertas modulaciones, al tratamiento acometido por las autoridades del sistema de justicia penal con fines de investigación y persecución del delito. Si bien, compaginando dicho objetivo con el de creación de un contexto en el que se facilite el intercambio y circulación de datos entre las autoridades nacionales y de los Estados miembros.

La Directiva 2016/680 prevé una extensa y compleja regulación en la que se incorporan expresamente todo un elenco de novísimos principios, condiciones y límites de obligada observancia por las autoridades responsables, así como toda una serie de derechos en favor de los interesados con el objeto de establecer un equilibrio entre el interés del Estado en reprimir el delito y los derechos fundamentales de los ciudadanos.

La vigencia y efectividad de dichos principios y reglas, va a suponer un cambio sustancial en las arraigadas prácticas judiciales, toda vez que

como hemos desarrollado a lo largo del trabajo, van a implicar que cualquier actuación orientada a la obtención de datos, va a requerir, entre otros puntos, la verificación de la legitimidad de la obtención, de la finalidad el uso y de la adecuación y pertinencia de los datos a los fines perseguidos. Examen judicial que desde luego deberá exteriorizarse a través de las oportunas resoluciones judiciales habilitantes, al igual que cualquier otra actuación que pudiera surgir incidentalmente respecto a los datos.

Desde luego, la aplicación de la normativa en su integridad, va a suponer en toda regla un cambio de cosmovisión y de cultura en lo que respecta al tratamiento de datos que tiene lugar en el seno del proceso penal. La observancia y respeto general a esta nueva norma, requerirá de cierto tiempo de adaptación y de concienciación de todos los operadores jurídicos, si bien, en buena medida, dependerá de la labor formativa que el Consejo General del Poder Judicial efectúe entre jueces y magistrados en su calidad de autoridad de control.