LA APORTACIÓN DE DATOS DE CARÁCTER PERSONAL DE TERCEROS AL PROCESO PENAL

The provision of personal data of third parties to the criminal proceedings

Juan Alejandro Montoro Sánchez[1]
Investigador Postdoctoral Margarita Salas[2]
Universidad Pablo de Olavide de Sevilla / Instituto de Justicia y Litigación «Alonso Martínez» Universidad Carlos III de Madrid
jamonsan@upo.es

Palabras Clave: protección de datos de carácter personal, cesión de datos personales, proceso penal, medios de investigación; fuentes de prueba.
Keywords: data protection right, transfer of personal data, criminal proceeding, investigative actions, evidences.

Resumen: El presente trabajo analiza, a la luz de la normativa del derecho a la protección de datos y de la ley procesal, el fenómeno de la aportación de datos de carácter personal de terceros a un órgano judicial del orden penal, con miras a su utilización en el proceso como medio de investigación o como fuente de prueba, con especial atención a sus requisitos y límites.
Abstract: This paper analyses, in the light of data protection law and procedural law, the phenomenon of the provision of personal data of third parties to a criminal court, with a view to its use in the process as a investigative action or as a source of evidence, with special attention to its requirements and limits.

I. LA APORTACIÓN DE DATOS PERSONALES DE TERCEROS COMO FENÓMENO HABITUAL DEL PROCESO PENAL

Los datos de carácter personal que se incorporan a los ficheros jurisdiccionales dependientes de un órgano judicial con ocasión de la tramitación de un proceso penal, para su utilización como medio de investigación o como fuente de prueba, no siempre son facilitados por el interesado al que estos pertenecen[3]. Es habitual en la práctica procesal que el sumario se nutra, en un grado muy importante, de datos personales que son aportados por terceros, sin disponer no ya con el consentimiento previo del titular, sino incluso con su mero conocimiento[4]. Este fenómeno se ve facilitado por el creciente número de bases de datos, tanto de naturaleza pública como privada, en las que se conservan los más abundantes y heterogéneos datos personales con ocasión de la exis-

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.
3. Colmenero Guerra, «La protección de datos en la Administración de Justicia» en *Publicaciones del Portal Iberoamericano de Ciencias Penales*, 2016, pág. 17.
4. Murillo de la Cueva, «La protección de datos en la Administración de Justicia» en *Cuadernos de derecho judicial*, núm. 9, 2004, pág. 241 anticipa que «en aplicación de las leyes de enjuiciamiento, con las que concuerda la LOPD [arts. 6.1 y 11.2 d)], la mayor parte de la información personal existente en los ficheros de datos judiciales se habrá obtenido sin que medie el consentimiento de aquél a quien pertenecen por ofrecer la ley la correspondiente cobertura para lograrla».

tencia de una relación jurídica, principalmente la prestación de un servicio de la sociedad de la información o de comunicaciones electrónicas, o en virtud de una obligación legal que afecta al titular del fichero. De hecho, en el ordenamiento jurídico existen multitud de disposiciones legales, en variados ámbitos sectoriales, que ordenan expresamente al responsable de un fichero registrar y conservar datos de carácter personal a efectos de posibilitar su posterior uso en vía jurisdiccional para la represión del delito, aun cuando estos hubieran sido originariamente recogidos para ser destinados exclusivamente a la conquista de fines propios del titular del fichero[5]. Estas disposiciones son especialmente intensas en ciertas parcelas del ordenamiento jurídico administrativo, en las que conviven regímenes sancionadores con tipos penales, como son las referidas al ámbito fiscal, de la protección social o del derecho de la competencia. Además, desde que se aprobaron las primeras leyes internas en materia de protección de datos, el Consejo General del Poder Judicial ha venido suscribiendo múltiples convenios de colaboración con distintas Administraciones públicas[6] y entidades privadas con el objetivo de agilizar el acceso de los órganos judiciales a los ficheros dependientes de los suscriptores con miras a su utilización con fines estrictamente jurisdiccionales.

No obstante, no es necesario tener la condición de responsable del tratamiento o ser titular de una gran base de datos para necesitar valerse de datos de terceros en un proceso. De hecho, los individuos particulares son, en definitiva, los sujetos que copan mayoritariamente las posiciones de parte en los procesos penales y, por ende, los que pueden precisar el uso de los datos personales de terceros de los que dispongan, a efectos de ejercitar su derecho de defensa o la acusación en el seno del proceso penal, alterando la finalidad originaria para la que fueron obtenidos. Y es que todo lo anterior no puede sino confirmar la máxima que manifiesta que «la conservación de datos personales con una determinada finalidad despierta el deseo de hacer uso de dichos datos con otros fines[7]», fenómeno que, de materializarse, entraña una pérdida de los poderes de control y disposición que el derecho a la protección de datos de carácter personal atribuye a sus titulares.

II. EL RESPONSABLE DEL TRATAMIENTO COMO ARQUETIPO DE COMUNICANTE DE DATOS PERSONALES AL ÓRGANO JUDICIAL

La aportación de datos personales de terceros al proceso penal en cualquiera de sus fases, bien tenga lugar por la libre iniciativa del sujeto que disponga de ellos o bien previo requerimiento judicial de entrega al poseedor de la información[8], exige, como antecedente necesario, la existencia de un tratamiento previo de los datos, siquiera elemental, por parte de una persona distinta del interesado. Quiere esto decir que, para que puedan aportarse cualesquiera datos de carácter personal a un proceso penal por el que no es su titular, la persona que los detente debe, en primer lugar, haberlos obtenido previa y directamente del interesado o indirectamente a través de otro sujeto y, posteriormente, proceder a su registro y conservación para la previsible consecución de, cuanto menos, unos fines, muy probablemente prefijados, legítimos y distintos de la aportación al proceso de destino. Y ello sin perjuicio de

5. Murillo de la Cueva, «La protección de datos en la Administración de Justicia», *op. cit.*, pág. 241, alude a las previsiones legales y mecanismos específicos establecidos en el ordenamiento jurídico a fin de permitir el acceso e intercambio de datos entre diversos entidades privadas y Administraciones públicas con los órganos judiciales.
6. Cabezudo Rodríguez expresa que la gestión del intercambio de información con las entidades colaboradores se lleva a cabo de forma segura e instantánea mediante el uso del Punto Neutro Judicial, al que señala como el gran gestor y fuente de información de juzgados y tribunales. No obstante, cabe decir que hoy día y, al menos, en lo que respecta al orden jurisdiccional penal, las fuentes de información esenciales para la investigación y enjuiciamiento se localizan en el ámbito privado. Cabezudo Rodríguez, «Documentación judicial y protección de datos personales» en *La responsabilidad jurídica y social de los archiveros, bibliotecarios y documentalistas en la sociedad del conocimiento* (García Marco, Ed.), Prensas Universitarias Zaragoza, Zaragoza, 2008, pág. 110.
7. 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 de lo Mercantil núm. 5 de Madrid en el asunto *Promusicae contra Telefónica de España S.A.U.*, asunto C-275/06. *Vid.* Pérez Gil, «Entre los hechos y la prueba: reflexiones acerca de la adquisición probatoria en el proceso penal» en *Revista Jurídica de Castilla y León*, núm. 14, 2018, pág. 233.
8. Aunque el requerimiento para la aportación de datos personales proceda de un órgano judicial, no siempre se estará ante una solicitud de oficio resultante de la voluntad del propio juez, sino que también puede derivar de una solicitud de práctica de diligencias instada por una de las partes del proceso o por el Ministerio Fiscal.

que los datos personales puedan ser sometidos, además, a otras tantas y complejas operaciones adicionales de procesamiento para alcanzar los fines perseguidos.

Sin embargo, para delimitar los eventuales supuestos que tienen cabida bajo este fenómeno, no es imprescindible indagar minuciosamente en las características cuantitativas y cualitativas del tratamiento antecedente a la cesión, así como a su sometimiento o no a la legislación de protección de datos, pues estas circunstancias no son, *a priori*, relevantes.

La situación más habitual coincidirá con aquella en que la persona que pretenda o sea requerida para aportar datos personales a un proceso penal tenga la condición formal de responsable, o incluso, de encargado del tratamiento de acuerdo con las definiciones establecidas en la normativa de protección de datos[9]. Y ello debido a que concurren, en los sujetos que ocupan tales roles, circunstancias que facilitan una acumulación cuantitativa de datos personales de terceros en su condición de titulares de un fichero, y además cualitativa, pues no resulta extravagante que el objeto del proceso penal pueda tener algún punto de conexión con la relación jurídica que les une con el interesado y que, en definitiva, subyace al tratamiento de sus datos. Tal coincidencia es la que convierte a tales responsables en una potencial fuente privilegiada de datos de carácter personal para el proceso penal, respecto de los propios particulares que actúan al margen de una actividad empresarial o comercial. Y ello con independencia de la naturaleza jurídica que ostente el responsable, pues no existe óbice para que tanto sujetos de derecho privado como entidades y organismos públicos puedan no solo poseer datos útiles para el proceso penal, sino incluso ser parte[10] o, al menos, ostentan algún tipo de interés legítimo en el mismo.

No obstante lo anterior, es igualmente viable que una persona física aporte datos de carácter personal de terceros que hayan sido obtenidos y tratados con fines estrictamente domésticos o personales, esto es, sin que la hubiera movido algún tipo de motivación comercial o profesional y sin que ostente la condición de responsable del tratamiento en el modo establecido en la normativa de protección de datos. También es posible que los datos personales objeto de entrega al órgano jurisdiccional los posea la persona física por causas meramente accidentales o por concurrencia de otras razones fortuitas, sin que se hubieran destinado o conservado en un fichero estructurado de datos[11]. Piénsese, por ejemplo, en las fotografías que, como mera actividad recreativa, tome y conserve un sujeto, que documenten accidentalmente aspectos que pueden resultar útiles para el esclarecimiento de los hechos.

III. LA CESIÓN O COMUNICACIÓN DE DATOS COMO TRATAMIENTO PREVIO IMPRESCINDIBLE PARA LA INCORPORACIÓN AL PROCESO

Cuando un responsable o un particular procede a entregar datos personales de terceras personas a un órgano judicial, nos encontramos ante un tratamiento consistente en una comunicación o cesión que provoca, por sí misma,

9. Según las definiciones de responsable del tratamiento y de encargado del tratamiento que se contemplan en los apartados 7 y 8 del art. 4 del Reglamento General de Protección de Datos respectivamente.

10. Debe recordarse que desde la reforma operada en el Código Penal por la Ley Orgánica 5/2010, de 22 de junio, las personas jurídicas pueden ser penalmente responsables de los delitos cometidos en nombre o por cuenta de las mismas, y en su provecho, por sus representantes legales y administradores de hecho o de derecho, como dispone el art. 31 *bis* CP. Por ello, pueden ser parte en el proceso tanto en la posición activa como acusación, como en la pasiva. No obstante, en virtud de lo dispuesto en el art. 31 *quinquies* CP, no serán aplicables al Estado, a las Administraciones públicas territoriales e institucionales, a los organismos reguladores, las agencias y entidades públicas empresariales, a las organizaciones internacionales de derecho público, ni a aquellas otras que ejerzan potestades públicas de soberanía o administrativas, lo que no empece su intervención en el proceso como acusación. Por tanto, la intervención de las Administraciones públicas y demás entidades y organismos de índole pública tan solo podrán actuar como acusación en los casos en que la legislación procesal les otorgue legitimación para ello.

11. Pues tal y como señalan Pérez Gil y González López, «La incorporación de datos personales automatizados al proceso en la propuesta de Código Procesal Penal (1)» en *Diario La Ley*, núm. 8217, 2013, pág. 3, «tratamiento y fichero son conceptos estrechamente vinculados, pero no inevitablemente unidos». Por ello, puede haber un tratamiento de datos sin que exista un fichero organizado en el que se registren y conserven los mismos. Los autores se apoyan en el Informe 0279/2009 de la Agencia Española de Protección de Datos en el que se apuntó que la normativa de protección de datos es de aplicación «si se produce un tratamiento de datos con información concerniente a personas físicas identificadas e identificables (...) con independencia de si se crea o no un fichero». No obstante, el RGPD descarta tal posibilidad en su Considerando (15) al advertir que «Los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del presente Reglamento».

una injerencia en el derecho a la protección de datos del interesado, con independencia de la naturaleza de los datos y del posterior uso que se haga de los mismos[12]. Es decir, nos situamos ante la revelación o manifestación de datos de carácter personal por parte de un sujeto que no es el titular, habitualmente un responsable que tiene la condición de autoridad pública, a un tercero distinto del interesado. En todo acto de comunicación se torna indispensable diferenciar entre las diferentes acciones llevadas a cabo por los dos sujetos involucrados en el proceso de transmisión de los datos, a saber: el particular o responsable tercero como cedente —que puede ser a su vez parte en el proceso o no intervenir— y el órgano judicial como destinatario o cesionario.

La primera de ellas, que es la llevada a cabo por el sujeto transmitente y que consiste en el acto de entrega o transferencia de los datos personales al órgano judicial a través de los canales electrónicos implantados para el establecimiento de las comunicaciones con la Administración de Justicia o alternativamente, cuando no sea obligatorio el uso de los anteriores medios, por los cauces tradicionales en soporte físico. Es importante señalar que estas transmisiones de datos pueden encontrar motivación en diferente fundamento, ya que el tratamiento puede tener origen en la voluntad libre y deliberada del transmitente o al contrario obedecer al cumplimiento de un previo requerimiento de entrega que se haya formulado por el tribunal[13]. En cualquiera de estos supuestos, la operación de tratamiento que efectúa el sujeto que realiza la entrega se identifica indiscutiblemente con una cesión de datos personales que debe entenderse desde una doble perspectiva[14]: la subjetiva, en tanto se produce un trasvase de datos entre dos sujetos, el cedente y el destinatario, es decir se revelan estos a un nuevo sujeto que no disponía de ellos —el tribunal— y a todas luces sin la necesaria confluencia del consentimiento ni el conocimiento del interesado. Y, además, la teleológica, debido a que con la comunicación se proyecta, además, la producción de un nuevo y ulterior tratamiento de los datos destinado a la consecución de una finalidad adicional y distinta de para la que fueron inicialmente recopilados en su origen y que se concreta en alguna de las diferentes finalidades plasmadas en el art. 1.1 de la Directiva 2016/680/UE —art. 1 de la Ley Orgánica 7/2021— para la que se encuentran legitimados los órganos judiciales del orden criminal: la investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

El marco normativo que resulta de aplicación a estas comunicaciones de datos de carácter personal no es homogéneo y va a depender, en última instancia, del marco legal en el que se encuadre el tratamiento previo de los datos que son objeto de cesión. En primer lugar, debemos hacer referencia a aquellas cesiones efectuadas por una persona física respecto a datos dedicados exclusivamente para su uso personal o doméstico o que no están destinados a incluirse en un fichero organizado y estructurado al que se pueda acceder con arreglo a criterios organizativos determinados. Dado que estas modalidades de tratamiento subyacentes, en cualquiera de sus modalidades[15], se sitúan explícitamente extramuros del ámbito aplicativo del RGPD[16] y de la LOPDGDD[17], no

12. Muy significativo a este respecto resultan las sentencias TJUE de 17 de octubre de 2013 (asunto Schwarz), C-291/12, apartado 25, y de 8 de abril de 2014 (asunto *Digital Rights Ireland* y otros), C-293/12 y C-594/12, apartado 36, recogen la doctrina del TJUE en base a la que se considera la cesión como un tratamiento de datos del que se deriva una injerencia los derechos a la protección de datos de carácter personal y a la vida privada. En concreto estas sentencias confirman 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». En idéntico sentido se pronunció el TJUE mediante su Dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, apartados 124 y 126, en el expuso que «(…) la comunicación de datos de carácter personal a un tercero, como una autoridad pública, constituye una injerencia en el derecho fundamental consagrado en el artículo 7 de la Carta, cualquiera que sea la utilización posterior de la información comunicada. Lo mismo puede decirse de la conservación de los datos de carácter personal y del acceso a esos datos con vistas a su utilización por parte de las autoridades públicas».
13. En este punto hacemos debe excluirse al sujeto pasivo del proceso penal como destinatario de un requerimiento que prevea la entrega coercitiva de documentos u otros medios en los que se integren datos personales, pues resultaría ilegítimo en cuanto supondría una injerencia no permitida en sus derechos fundamentales a la no autoincriminación y a la presunción de inocencia. Por tanto, los requeridos podrán ser cualesquiera otras personas o entidades, gocen o no de legitimación para adquirir la condición de parte activa.
14. Debe recordarse que, mientras el concepto nacional de cesión obedece al plano subjetivo exclusivamente, el comunitario de comunicación, contempla asimismo al ámbito teleológico. Messía de la Cerda Ballesteros, «La evolución del concepto de cesión o comunicación de datos personales» en *Actualidad Civil*, núm. 10, 2017, págs. 8-9.
15. Automatizada, manual o mixta.
16. El art. 2.2 del RGPD excluye de su ámbito de aplicación al tratamiento efectuado por una persona física en el ejercicio de actividades efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. Regla enfatizada por el Considerando (15) de RGPD *in fine*, al disponer que «La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él. En consecuencia, la acumulación o depósito de datos de forma no estructurada, sin atender a un criterio de ordenación que pudiera permitir la búsqueda e identificación de los datos de una persona, no resultaría sometido al régimen tuitivo establecido en el RGPD».
17. Art. 2.2.a) de la LOPDGDD que reafirma al artículo transcrito en la nota anterior, al establecer que «Esta ley orgánica no será de aplicación:

encontrando tampoco cobijo al amparo de la Directiva 2016/680/UE, es posible colegir su escape a la normativa de protección de datos, sin perjuicio de que le resulten de aplicación las condiciones y restricciones que afecten a la validez y eficacia que puedan derivar de la normativa procesal, especialmente las derivadas del principio de proporcionalidad conforme a los términos establecidos por el Tribunal Constitucional, habida cuenta de la injerencia que se provoca en el derecho fundamental a la protección de datos del interesado. En la otra cara se ubican aquellos datos cedidos que, previamente, sean tratados por un responsable del tratamiento. Las operaciones de comunicación por parte de un responsable sometido a la normativa general de protección de datos, esto es, al Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, se siguen rigiendo por estas normas y, en particular, por sus principios rectores y garantías específicas, pese a que tengan como destinatario a una autoridad competente del orden penal sujeta por las disposiciones especiales dispuestas en la Ley Orgánica 7/2021, de 26 de mayo.

En segundo lugar, es necesario apuntar al ulterior tratamiento que desarrollaría el órgano judicial de los datos cedidos como su destinatario, a fin de cumplimentar el desarrollo de los fines jurisdiccionales que le son propios y que se concretarían, cuanto menos, en la recogida, incorporación al expediente judicial individual, cesión a las demás partes personadas y conservación en los sistemas de gestión de la Administración de Justicia. Este sucesivo tratamiento que recae sobre los datos comunicados, al ejecutarse por una autoridad competente en el cumplimiento de los fines propios a la Directiva 2016/680/UE se sometería igualmente al régimen jurídico impuesto por la Ley Orgánica 7/2021, de 26 de mayo, como norma de transposición de aquella.

IV. LA ALTERACIÓN DE LA FINALIDAD DEL TRATAMIENTO DERIVADA DE LA CESIÓN DE DATOS PERSONALES CON FINES PENALES

El acto por el cual un responsable del tratamiento —o incluso un particular que no ostente tal condición— procede a comunicar datos personales de terceros a un órgano judicial para su incorporación a un proceso penal como material identificativo o probatorio, constituye, por lo general, un supuesto de utilización de los datos objeto de cesión para una finalidad distinta de para la que fueron inicialmente recabados y procesados por el cedente. Y ello porque lo habitual en la *praxis* es que los datos personales se recolecten inicialmente por el responsable con otros fines, por ejemplo, por ser necesarios para la formalización y desarrollo de una relación comercial o contractual, para el cumplimiento de una obligación impuesta por el ordenamiento jurídico o con meros fines domésticos entre otros, y solamente con posterioridad, ante el eventual acaecimiento o conocimiento de unos hechos delictivos, si estos pudieran devenir útiles para su esclarecimiento y el de sus autores o para la defensa, se utilicen, además, para cualquiera de estas nuevas finalidades mediante su puesta a disposición del órgano judicial competente. Por tanto, es posible intuir que difícilmente la recogida y el tratamiento sistemático y organizado de datos personales, puede tener como finalidad, en sus orígenes, la posterior entrega a un órgano judicial para su utilización en la investigación o enjuiciamiento de delitos, sino que, antes al contrario, esta finalidad surgirá comúnmente *a posteriori*, una vez se advierta la utilidad de los datos en un proceso penal específico ya iniciado o cuya iniciación se prevé respecto a unos concretos hechos y sujetos.

Y es que, fuera de los casos en los que el ordenamiento jurídico prevé expresamente el mantenimiento de ficheros para el acopio de información y datos personales con fines penales[18], como pudiera ser el caso de las diferentes bases de datos policiales, de los ficheros integrados en el Sistema de Registros Administrativos de apoyo a la Administración de Justicia o de aquellos otros cuya creación se deriva de legislación sectorial específica, como podrían ser la relativa a la prevención del blanqueo de capitales y de la financiación del terrorismo[19] o a la de conservación

a) A los tratamientos excluidos del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo».

18. Nos referimos a aquellos ficheros de datos, eminentemente de naturaleza pública, cuya creación obedece a la consecución de los fines propios de la Directiva 680/2016/UE.

19. La Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, prevé que los sujetos obligados a adoptar medidas de diligencia debida mantengan ficheros de datos específicos a efectos de cumplimentar las comunicaciones y avisos preceptivos a las autoridades competentes en aquellos casos en que puedan existir riesgos o indicios de blanqueo de capitales. Al respecto: Aneiros Pereira, «Las obligaciones de prevención del blanqueo de capitales a cargo de determinados profesionales: una fuente de

de datos de tráfico[20], resulta descabellada la idea de que un particular o incluso una entidad u organismo público puedan llevar a cabo la creación de un fichero de datos sistematizado destinado exclusivamente a recopilar datos para su posterior entrega a un proceso penal. De hecho, más allá de los ficheros mantenidos por los letrados que ejerzan en el ámbito penal o de aquellos destinados a conservar las grabaciones de sistemas de videovigilancia, la licitud de creación de un fichero con tal objeto específico fuera de los casos antes expresados quedaría claramente en tela de juicio al no tener encaje en ninguno de los supuestos legitimadores del tratamiento listados en el art. 6 del RGPD.

Estaríamos, por tanto, generalmente, ante un uso de los datos personales para una finalidad no prevista inicialmente, pues esta surgiría *ex novo* con ocasión de la comisión de un delito o de la incoación de un proceso penal, teniendo además un carácter contingente, debido a que se exige que los datos presenten cierta relación y relevancia o utilidad, lo cual no siempre acontecerá. Ello no se compadece ni con el principio rector de limitación de la finalidad vinculado al derecho a la protección de datos, ni con la doctrina constitucional establecida en la STC 292/2000, por la cual, aunque los datos se recojan de forma legítima para su tratamiento, estos solo pueden utilizarse para las finalidades previstas y no para otras adicionales, al quebrar esta práctica las facultades de control y disposición de los interesados[21].

Sin embargo, aunque los datos personales no fueren recogidos inicialmente con la intención de ser aportados a un proceso penal y, por tanto, no se explicitara al interesado a la hora de cumplir con el deber de información la posibilidad de usarlos de tal modo ni la eventual comunicación a un órgano judicial[22], lo cierto es que la entrega de datos con meros fines identificativos o para su uso como medio probatorio de cargo o descargo[23] es una práctica habitual que sin duda alguna contribuye a la realización del ejercicio de los derechos fundamentales a la defensa, a la utilización de medios de prueba pertinentes y a la tutela judicial efectiva proclamados en el art. 24 de la CE, amén de a los también constitucionalmente protegidos intereses generales a la seguridad pública y a la represión de la delincuencia[24]. Y ello a pesar de que *a priori*, esta práctica pueda resultar contraria con el principio rector de limitación de la finalidad proclamado en el art. 5.1.b) del Reglamento General de Protección de Datos, toda vez que en virtud del mismo los datos personales deben ser recogidos y tratados para su uso con los fines determinados, explícitos y

información tributaria» en *Revista técnica tributaria*, núm. 91, 2010, págs. 25-66 y Huerta Viesca, «Práctica y crítica de las obligaciones de las entidades de crédito respecto de sus clientes en prevención del blanqueo de capitales» en *Revista de derecho bancario y bursátil*, núm. 117, 2010, págs. 117-140.

20. Nos referimos a los ficheros que todos los operadores de comunicaciones electrónicas deben mantener a fin de conservar los datos de tráfico y localización que se generen como consecuencia de la prestación de servicios de telecomunicaciones con fines de detección, investigación y enjuiciamiento de delitos graves en virtud de las obligaciones dispuestas en la Ley 25/2007 de 18 de octubre, de conservación de datos. Para un estudio y crítica de estos ficheros pueden consultarse: Colomer Hernández, «Uso y cesión de datos de las comunicaciones electrónicas para investigar delitos tras la STJUE de 21 de diciembre de 2016» en *Estudios sobre Jurisprudencia Europea: materiales del I y II Encuentro anual del Centro español del European Law Institute, (*Ruda González y Jerez Delgado, Coords.), Sepín, Las Rozas, 2018, págs. 767-781 y Montoro Sánchez, «El tratamiento de los datos de tráfico y localización con fines penales: estudio de la situación actual» en *Uso y cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios,* (Colomer Hernández, Dir.), Aranzadi, Cizur Menor, 2019, págs. 371-424.

21. Colmenero Guerra, «La protección de datos en la Administración de Justicia» ..., *op. cit.*, pág. 17; y Cabezudo Rodríguez, «Datos personales e informaciones judiciales» en *Revista General de Derecho Procesal*, núm. 17, 2009, págs. 18-19. Aluden los autores a los supuestos en los que el Tribunal Constitucional se ha pronunciado contra la utilización de datos para otras finalidades no previstas inicialmente, como las SSTC 11/1998, de 13 de enero y 202/1999, de 8 de noviembre.

22. Es necesario recordar que las finalidades a las que se destinan los datos deben resultar explícita, esto es deben expresarse de forma clara, transparente y determinante al interesado y puestos en su conocimiento a través de los cauces informativos establecidos en la normativa, sin que proceda incluir fines encubiertos, solapados o ambiguos. Troncoso Reigada, «El principio de calidad de los datos» en *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (Troncoco Reigada, Dir.), Civitas, Madrid, 2010, pág. 345; Palma Ortigosa, «Principios relativos al tratamiento de datos personales» en *Protección de datos, responsabilidad activa técnicas de garantía* (Murga Fernández, Fernández Scagliusi y Espejo Lerdo de Tejada, Dirs.), Reus, Madrid, 2018, pág. 44 y Aparicio Salom, «La calidad de los datos» en *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (Troncoso Reigada, Dir.), Civitas, Madrid, 2010, pág. 329.

23. O como expresa la Resolución de la AEPD RR/00408/2010, para «lograr la convicción del juez en relación con los hechos que se pretenden acreditar».

24. El Tribunal Constitucional ha declarado expresamente en sentencias como 166/1999, de 27 de septiembre (F. J. 2.º) y 127/2000, de 16 de mayo (F. J. 3.º) que la persecución y castigo del delito constituye, asimismo, un bien digno de protección constitucional, a través del cual se defienden otros también reconocidos en la Carta Magna como la paz social y la seguridad ciudadana que encuentran amparo en los arts. 10.1 y 104.1 de la CE.

ISSN: 2951-844X

legítimos que haya determinado *ex ante* el responsable, no debiendo ser procesados o comunicados ulteriormente para otros fines que resulten incompatibles[25].

Sentado lo anterior, la cuestión se centra en dilucidar si, en abstracto, y sin tener en cuenta otros aspectos y circunstancias coyunturales que pudieran haber afectado al tratamiento previo, la práctica consistente en comunicar datos personales de terceros que pueda efectuar un responsable de un fichero o un sujeto particular a un órgano judicial para su incorporación a un proceso penal con alguno de los fines de la Ley Orgánica 7/2021, esto es, la investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, en tanto consiste en perpetrar un tratamiento no contemplado primitivamente con una finalidad *ex novo*, resulta acorde a los parámetros de licitud propios del derecho a la protección de datos de carácter personal. Lo cual se muestra como condición estrictamente indispensable para que los datos objeto de comunicación puedan ulteriormente desplegar los efectos pretendidos en el proceso con plena garantía de validez y eficacia.

La licitud de este tratamiento y, por tanto, la superación de un primer filtro para la entrada e incorporación de los datos al proceso, estaría condicionada a que el acto de comunicación reuniera conjuntamente los requisitos exigidos por los principios rectores operantes: encontrar sustento en un fundamento o base legal de legitimación del tratamiento de los contemplados en el art. 6 del RGPD —pues no debemos obviar que dichos tratamientos se sujetan a la norma general—, estar prevista la medida en la ley y la superación del juicio de proporcionalidad requerido por el Convenio 108 para la limitación del derecho a la protección de datos. Y ello sin perjuicio de que la entrada al proceso como fuente de prueba y su validez, dependan en última instancia del cumplimiento de otros requisitos adicionales ligados a la propia normativa de protección de datos y otros de naturaleza eminentemente procesal, como adelanta el art. 236 *ter* 3 LOPJ. Procede analizar individualmente cada uno de los motivos exigidos por el Reglamento General de Protección de Datos.

V. BASES LEGALES DE LEGITIMACIÓN DE LA CESIÓN DE DATOS CON FINES PENALES

El primero de los requisitos que debe verificarse como condición *sine qua nom* es la existencia de una base legal de tratamiento que ampare y legitime al responsable del tratamiento para efectuar la entrega de los datos personales a un órgano judicial. Si como veremos el responsable podrá encontrar apoyo legal en varias de ellas, la sujeción a una base en particular dependerá finalmente de la relación que aquel ostente con el objeto del procedimiento.

1. El consentimiento informado

La primera de las bases legales de tratamiento de datos personales que debe analizarse como posible vía de legitimación de la cesión de datos a un órgano judicial con fines penales es la relativa al consentimiento informado del interesado prestado en los términos exigidos por la normativa general de protección de datos. Sin embargo, es de advertir que el interés en proceder a su examen se centra más que en confirmar su potencial aptitud para legitimar la antedicha comunicación, en descartar su intervención forzosa. Lo cierto es que no existe óbice legal alguno que impida que el interesado pueda consentir desde el mismo momento de la recogida de los datos, o incluso *a posteriori*, previo cumplimiento del deber de información, que el responsable destine sus datos a un órgano judicial, para ser utilizados con fines identificativos o probatorios, incluso para ser utilizados en su contra. De hecho, el RGPD valida las comunicaciones de datos que pueda planear el responsable incluso para servir a nuevos fines, por el mero aval prestado por el consentimiento del interesado, el cual se muestra suficiente por sí mismo[26]. Sin embargo, como se anticipó con anterioridad, es incluso extravagante en la práctica se anticipe tal uso, dado que este se muestra como altamente contingente e incluso no deseado, por las connotaciones negativas que derivan de su inclusión. Piénsese la poca confianza que despertaría en el interesado prestar su consentimiento al responsable para que sus datos se utilicen como prueba de cargo en su propio perjuicio en un proceso penal.

25. Palma Ortigosa, «Principios relativos al tratamiento de datos personales» ..., *op. cit.*, pág. 44 y Puyol Montero, «Los principios del derecho a la protección de datos» en *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad* (Piñar Mañas, Dir.), Reus, Madrid, 2016, pág. 140.

26. Así se desprende del art. 6.4 del RGPD *ab initio* cuando afirma que «Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado».

Por otro lado, tampoco resultaría lógico considerar al consentimiento previo del interesado como un requisito imprescindible para que el responsable pueda proceder a aportar sus datos personales a un tribunal, pues ello supondría dejar al arbitrio y voluntad de aquel, la oportunidad de que el órgano judicial conocedor de una causa penal pueda obtener de un tercero parte o no, fuentes de prueba y evidencias que pueden resultar fundamentales para la investigación o enjuiciamiento de hechos delictivos. Máxime si se advierte que ello supondría privar al tribunal de una importante fuente de elementos incriminatorios, sobre todo cuando el potencial cedente de los datos coincida con la acusación, víctima o sujeto pasivo del delito, habida cuenta de la probable relación jurídica que subyace al tratamiento de sus datos[27]. Por ende, la exigencia del consentimiento como base legal del tratamiento podría ser contraproducente y perjudicial, no ya únicamente para el derecho a la tutela judicial efectiva de la parte que viera impedida la entrada en el proceso de las evidencias en las que se insertaran los datos de carácter personal, por verse restringido su derecho a la utilización de la prueba; sino también para otros bienes e intereses colectivos de vital importancia para el Estado que presentan relevancia constitucional y comunitaria, como son los de seguridad pública y el interés la prevención, investigación, descubrimiento y persecución de delitos[28].

Es por ello que, tras la reforma operada en la LOPJ en el año 2015 por la que se introdujo el primigenio régimen de protección de datos operante en la Administración de Justicia, se incorporó una disposición específica, el art. 236.1 *quáter*[29], con el objeto de abordar la problemática de las cesiones de datos a los tribunales desde la perspectiva de todos los sujetos intervinientes, ya que se complementó el contenido del otrora vigente art. 11.2 de la LOPD, desde la dimensión del tribunal como eventual cesionario. Si este último precepto ya legitimaba con anterioridad y, excepcionalmente, la cesión de datos del interesado que pudiera efectuar el responsable del tratamiento, siempre y cuando esta tuviera por destinatario «*al Defensor del Pueblo, el Ministerio Fiscal o los jueces o tribunales o el Tribunal de Cuentas*» para el cumplimiento de los fines que le son propios, esto es, para el ejercicio de la potestad jurisdiccional en el caso de los tribunales, el precepto introducido en la LOPJ tenía el objeto de eximir a los tribunales de la necesidad de obtener el consentimiento del interesado para procesar sus datos personales en el marco del proceso, tanto cuando estos hubieran sido cedidos por alguna de las partes[30] como cuando fueran recabados por sí mismo con la colaboración de terceros o bien a través de diligencias de investigación limitativas de derechos fundamentales. Asimismo, esta disposición venía a aclarar *in fine* que el carácter contingente del consentimiento no obsta a la aplicación de las reglas procesales oportunas respecto a la validez de la prueba, es decir, que la mera licitud de la comunicación no tiene por sí misma ninguna repercusión en la licitud y eficacia probatoria de los datos, debiendo encontrarse en las tradicionales reglas contempladas en la norma procesal. Tras la reforma operada en la Ley Orgánica del Poder Judicial a través de la Ley Orgánica 7/2021, dicha regulación se prevé en la actualidad en el art. 236 *ter* 3 de la LOPJ, en idénticos términos.

Como consecuencia de todo lo anterior, es posible descartar al consentimiento como base imprescindible para la comunicación de datos de terceros por un responsable del tratamiento o por un particular a un órgano judicial, siempre que tuvieren como destino un uso con fines estrictamente jurisdiccionales[31]. Por lo que, de no contar con el consentimiento del interesado, el responsable deberá encontrar respaldo en otro fundamento legal que avale la licitud de la cesión de los datos personales.

27. Esta circunstancia ha sido puesta de manifiesto por la AEPD en varias resoluciones. Por ejemplo, en las núm. 1555/2007 y la más reciente E/06807/2017, en las que con ocasión de la cesión de datos al órgano judicial sin consentimiento resolvió que «la exigibilidad del consentimiento del oponente para el tratamiento de sus datos supondría dejar a disposición de aquél el almacenamiento de la información necesaria para que el denunciante pueda ejercer, en plenitud, su derecho a la tutela judicial efectiva. Así, la falta de estos datos o su comunicación a la contraparte, puede implicar, lógicamente, una merma en la posibilidad de aportación por el interesado de "los medios de prueba pertinentes para su defensa", vulnerándose otra de las garantías derivadas del citado derecho a la tutela efectiva y coartándose la posibilidad de obtener el pleno desenvolvimiento de este derecho». También es destacable el Dictamen CNS 7/2018, de 7 de marzo de la Autoridad Catalana de Protección de Datos.

28. Pueden consultarse en el ámbito europeo las sentencias TJUE de 29 de enero de 2008 (asunto *Promusicae*), apartado 51; de 8 de abril de 2014 (asunto Digital Rights), apartado 62 y de 21 de diciembre de 2016 (asunto *Tele2 Sverige AB*), apartado 120. En relación al artículo 8 del CEDH, puede acudirse a la sentencia TEDH de 12 de enero de 2016 (asunto Szabó y Vissy *vs*. Hungría), apartados 77 y 80.

29. Art. 236.1 *quáter* LOPJ (actualmente reformado): «*De conformidad con lo dispuesto en el artículo 11.2 de la Ley Orgánica 15/1999, de 13 de diciembre, no será necesario el consentimiento del interesado para que los tribunales procedan al tratamiento de los datos en el ejercicio de la potestad jurisdiccional, ya sean* éstos *facilitados por las partes o recabados a solicitud del propio Tribunal, sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba*».

30. En el caso previsto en el art. 11.2.d) Ley Orgánica 15/1999.

31. López Calvo, *Algunas cuestiones relevantes en protección de datos de carácter personal en Tribunales y Fiscalía tras el Reglamento Europeo de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD),* Sepín, Las Rozas, 2019, pág. 23.

ISSN: 2951-844X

2. El tratamiento es necesario para el cumplimiento de una obligación legal del responsable del tratamiento

En virtud de lo dispuesto en los arts. 259, 262 y 264 de la Ley de Enjuiciamiento Criminal[32], los cuales se integran en el libro II de su título I sobre la denuncia, la persona que presencie personalmente o que, por cualquier otro medio, adquiera conocimiento de la comisión de unos hechos delictivos de naturaleza pública y, por ende, perseguible de oficio, tiene obligación[33] de denunciarlo a los tribunales, Ministerio Fiscal o a la policía, bajo pena de multa. Asimismo, en la denuncia que puede interponerse tanto de forma verbal como por escrito[34], se deben recoger, entre otros aspectos, las noticias y circunstancias con las que cuente el denunciante, tal y como ordena el art. 237 de la LECrim.

Es decir, los anteriores preceptos obligan a toda persona, no solo a poner de manifiesto a las autoridades competentes para la investigación criminal la eventual perpetración de unos hechos delictivos, sino incluso, cuando dispongan de ello, deberán aportar aquellos documentos, información o datos complementarios que puedan resultar útiles para esclarecer los mismos, sus circunstancias y su autoría. Por tanto, cuando un responsable del tratamiento o un particular, en cumplimiento de alguna de las obligaciones reseñadas denuncie la comisión de unos hechos delictivos y, además, por contribuir a tales fines, efectúe la entrega de datos de carácter personal de los registrados en sus ficheros o de los que tenga en su poder a un órgano judicial[35], se produciría una cesión de datos, en principio lícita, por encontrar amparo en la base consistente en el cumplimiento de una obligación legal establecida en el art. 6.1.c) del RGPD[36].

Mención especial requiere, en este punto, la obligación legal de denunciar delitos que se establece para determinadas Administraciones públicas y otros organismos de naturaleza pública. Piénsese que, durante el desarrollo de las competencias y funciones de algunos organismos públicos, es viable que se pueda advertir, por las autoridades o funcionarios que intervengan, posibles conductas u omisiones que pueden resultar delictivas directamente. En otras ocasiones, particularmente en aquellos ámbitos sectoriales que reprimen conductas que atentan contra bienes jurídicos protegidos en las que convergen el régimen sancionador administrativo con el penal, tras la incoación de un procedimiento sancionador puede advertirse que los hechos revisten gravedad delictiva. En tales casos, los responsables de estos servicios públicos deben también denunciar los hechos a la autoridad competente. Ejemplo paradigmático de tal obligación es la prevista en el art. 95 de la Ley General Tributaria respecto de los funcionarios de las Administraciones tributarias. Ante la apreciación de la posible existencia de un delito no perseguible únicamente a instancia de persona agraviada, estos deberán deducir el tanto de culpa o remitir al Ministerio Fiscal relación circunstanciada de los hechos que se estimen constitutivos de delito.

Asimismo, también serían asimilables a tal supuesto, resultando amparadas bajo la base legitimadora del tratamiento de datos referida al cumplimiento de una obligación legal, aquellas cesiones de datos que pudieran efectuarse por un responsable del tratamiento o una persona física a un tribunal, en virtud de un requerimiento de entrega de datos. Y ello con independencia de que el sujeto requerido para ceder datos de carácter personal no tenga vincu-

32. El art. 259 de la LECrim obliga al «que presenciare la perpetración de cualquier delito público (…) a ponerlo inmediatamente en conocimiento del juez de instrucción, de paz, comarcal o municipal o funcionario fiscal más próximo al sitio en que se hallare, bajo la multa de 25 a 250 pesetas». Mientras, el art. 262 de la LECrim extiende esta obligación a «Los que por razón de sus cargos, profesiones u oficios tuvieren noticia de algún delito público, estarán obligados a denunciarlo inmediatamente al Ministerio fiscal, al Tribunal competente, al juez de instrucción y, en su defecto, al municipal o al funcionario de policía más próximo al sitio si se tratare de un delito flagrante».

33. Debe recordarse que la obligación de efectuar la denuncia no se extiende a cualquier persona, pues en la propia LECrim se recogen ciertos supuestos de dispensa. Así el art. 260 de la LECrim exime a los impúberes y a los que no gozaren del pleno uso de su razón; el art. 261 del mismo texto legal a los familiares más cercanos del delincuente y, finalmente, el art. 264 de la norma rituaria dispensa a los abogados y procuradores respecto de las instrucciones o explicaciones que recibieren de sus clientes.

34. Art. 265 de la LECrim.

35. Obviamente, el acompañamiento a la *notitia criminis* de datos de carácter personal, ya fuere a través de la entrega de documentación o de cualquier otro soporte, ocurrirá en el mayor de los supuestos cuando el denunciante sea, a su vez, víctima o sujeto pasivo del hecho criminal. Aunque ello tampoco es condición indispensable, ya que el denunciante puede contar con datos personales que colaboren a la investigación de los hechos sin tener vinculación alguna con estos, como sucede, por ejemplo, en aquellos supuestos en que un sujeto se limite a denunciar algún delito captado por un sistema de video vigilancia del que es responsable y que, sin embargo, no le perjudiquen ni afecten directamente.

36. Legitimación que ha respaldado incluso la Agencia Española de Protección de Datos en el Informe del Gabinete Jurídico 9/2019 y el GTA29 en su Dictamen 1/2006 sobre la aplicación de las normas de la UE relativas a la protección de datos a programas internos de denuncia de irregularidades en los campos de la contabilidad, controles contables internos, asuntos de auditoría, lucha contra el soborno, delitos bancarios y financieros, respecto a los canales de denuncias internos.

lación alguna con el objeto del proceso penal y, por tanto, no ostente la condición de parte ni tenga legitimación para ello. Con la entrega al juzgado de los datos personales objeto de requerimiento, se estaría dando cumplimento a la obligación de colaboración con la Administración de Justicia impuesta tanto por la normativa procesal penal[37] como por la de protección de datos[38], pero cuyo origen último se incardina en el art. 118 de la Constitución Española[39].

3. El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento

Ante la inexistencia de consentimiento del interesado o de otra base legal, la cesión de datos personales de terceros a un órgano judicial también puede, en ciertos casos, estar avalada por la causa de legitimación prevista en el art. 6.1.f) del RGPD, esto es, estar el tratamiento basado en la satisfacción del interés legítimo perseguido por el responsable o de un tercero al que se puedan comunicar dichos datos[40].

Ahora bien, pese a que el Grupo de Trabajo del art. 29 ha reconocido la importancia y utilidad de esta base siempre que concurran las circunstancias exigidas y el tratamiento se sujete a las garantías adecuadas, pues contribuye a la circulación de los datos evitando una dependencia excesiva de las demás bases legales, ha enfatizado que esta no debe de servir como cajón de sastre ni como último recurso para situaciones extrañas o inesperadas, y, por tanto, no es apropiada la extensión de su uso indebidamente habida cuenta de la aparenta relajación de exigencias[41].

La utilización de la presente causa exige que, sobre los intereses legítimos[42] del responsable, «no prevalezcan los intereses o los derechos y libertades fundamentales del interesado[43] que requieran la protección de datos persona-

37. Son diversas las normas de índole procesal en las que se encuentran concreciones que materializan genérica o específicamente el deber y obligación de colaboración con los tribunales proclamado en el art. 118 de la CE. Es el art. 17.1 de la LOPJ el que proclama, con carácter general y respecto a todas las personas y entidades de carácter público o privado, la obligación en la forma que la ley pueda establecer, de prestar la colaboración requerida por los jueces y tribunales en el curso del proceso y en la ejecución de lo resuelto, con las excepciones que establezcan la Constitución y las leyes, y sin perjuicio del resarcimiento de los gastos y del abono de las remuneraciones debidas que procedan conforme a la ley. *Vid.* Garberi Llobregat, «Artículo 118 CE: La obligación de cumplir las sentencias y demás resoluciones firmes de Jueces y Tribunales» en *Diario La Ley*, núm. 9365, 2019, pág. 2. Imposición que en el ámbito del proceso penal encuentra cobijo al amparo del art. 575 de la LECrim, mas solo respecto a la dimensión de colaboración de exhibición de los objetos y papeles que se sospeche puedan tener relación con la causa. Rodríguez Lainz ubica en esta obligación por conexión con el ya derogado art. 11.2.b) de la LOPD, la legitimación necesaria para ceder datos y documentos de terceros relevantes para el proceso. *Vid.* Rodríguez Lainz, «Sobre la previsible incidencia de la cuestión prejudicial C-207/16 en la definitiva defenestración del régimen legal español sobre conservación de datos relativos a las comunicaciones» en *Diario La Ley*, núm. 9273, 2018, pág. 4.

38. El art. 7 de la Ley Orgánica 7/2021, de 26 de mayo, ha incluido expresamente el deber de colaboración de los ciudadanos con las distintas autoridades competentes penales —incluidos los órganos judiciales— ante la petición de datos de carácter personal que fueren necesarios para la consecución de alguno de los fines perseguidos vinculados a la norma, siempre y cuando atienda a las competencias atribuidas *ex lege* y medie una petición concreta, específica y motivada.

39. Se trata de la obligación constitucional consagrada en el art. 118 del texto constitucional predicable de toda persona, sean parte o no de un proceso, y por la que deben de prestar a los juzgados y tribunales toda la colaboración necesaria para la tramitación de los procesos judiciales y su ejecución. Garberí Llobregat, «Artículo 118 CE: La obligación de cumplir las sentencias y demás resoluciones firmes de Jueces y Tribunales», *op. cit.*, págs. 2-4.

40. Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE y Palma Ortigosa, «Principios relativos al tratamiento de datos personales» …, *op. cit.*, pág. 42.

41. Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE.

42. Es posible considerar a un interés como legítimo cuando sea compatible con el ordenamiento jurídico en general y con la normativa de protección de datos en particular. Por ello ha sido también descrito como aquel aceptable en virtud de la ley en el Dictamen 3/2013 del Grupo de trabajo del Art. 29 sobre la limitación de la finalidad, pág. 9. Entre otros fines, se han reconocido como legítimos por el Grupo del art. 29 «la ejecución de derechos reconocidos en procedimientos judiciales, incluido el cobro de deudas mediante procedimientos extrajudiciales» o la «prevención del fraude». Ello garantiza, en gran medida, la utilización de esta vía de licitud para la aportación de datos. *Vid.* Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, pág. 30.

43. El ámbito de protección de los bienes jurídicos que pueden afectar al interesado para efectuar la ponderación es más amplio que la del responsable, motivo por el que se alude a intereses en general, sin exigir que su legitimidad, y amén de sus derechos y libertades fundamentales. Por ello, expresa el GTA29 «las personas implicadas en actividades ilegales no deberán estar sujetas a una injerencia desproporcionada en sus derechos e intereses». *Vid.* Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, pág. 36.

les»[44]. Por tanto, para verificar la procedencia de su aplicación, habrá que efectuar, caso a caso, una ponderación de los intereses y/o derechos en liza del responsable[45] y del interesado, no pudiendo extraer una regla general aplicable a todo supuesto[46]. A tal fin, será pertinente valorar particularmente «si en el supuesto concreto objeto de análisis existirá un interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos que prevalezca sobre el interés o los derechos y libertades fundamentales del interesado que requieran protección conforme a lo dispuesto en el artículo 1 del RGPD o si, por el contrario, los derechos fundamentales o intereses de los interesados a los que se refiera el tratamiento de los datos han de prevalecer sobre el interés legítimo en que el responsable pretende fundamentar el tratamiento de los datos de carácter personal[47]».

En el caso que nos pende, el interés legítimo del responsable se situaría en el ejercicio pleno de los derechos fundamentales a la utilización de los medios de prueba pertinentes en el proceso y en el derecho a la defensa, que trascenderían, a su vez, en el también derecho fundamental al que indisociablemente se encuentran unidos: la tutela judicial efectiva[48]. En relación al derecho a la utilización de prueba, el Tribunal Constitucional ha reconocido que su núcleo esencial consiste en el poder jurídico reconocido a quien interviene como litigante en un proceso provocar la actividad procesal necesaria para lograr la convicción del órgano judicial sobre la existencia o inexistencia de los hechos relevantes para la decisión del conflicto objeto del proceso[49]. Por tanto, impedir al responsable que sea parte en un proceso[50] de la posibilidad de valerse de medios probatorios que contengan o consistan en datos de carácter personal útiles para el ejercicio de la estrategia de defensa planteada por el sujeto, con justificación en que se precisa una comunicación y utilización de los datos de nuevo cuño, es de tal envergadura que la privación podría mermar sobremanera el derecho fundamental a la tutela judicial efectiva. Incluso si nos situáramos en un supuesto extremo, la restricción de aportación de ciertos medios probatorios podría tener una trascendencia tal que es posible la derivación de una condena o absolución injustas.

Tampoco podrían perderse de vista otros intereses concurrentes para este tipo de comunicaciones, concretamente los perseguidos por el potencial destinatario, ya que la propia norma alude a ello para el caso de que exista una comunicación de datos como sucedería en el teórico y genérico caso que analizamos. Los intereses legítimos del cesionario —que no olvidemos, es el órgano judicial del orden penal que conozca de la instrucción— se identificarían con el interés público general en combatir la delincuencia y en el mantenimiento de la seguridad pública[51], bienes

44. Las sentencias TJUE de 4 de mayo de 2017 (asunto *Rīgas Satiksme*), apartado 28A y, posteriormente, la de 11 de diciembre de 2019 (asunto TK), apartado 32, fijaron tres requisitos para que el tratamiento de datos personales resulte lícito: «primero, que el responsable del tratamiento o el tercero o terceros a quienes se comuniquen los datos persigan un interés legítimo; segundo, que el tratamiento de datos personales sea necesario para la satisfacción de ese interés legítimo; y, tercero, que no prevalezcan sobre el interés legítimo perseguido los derechos y libertades fundamentales del interesado en la protección de los datos».
45. Y también del destinatario para el caso de que sea este quien requiere los datos para destinarlos a sus intereses legítimos.
46. STJUE de 24 de noviembre de 2011 (asunto ASNEF y FECEDM), apartado 40, que afirma que «No obstante, ha de tenerse en cuenta que el segundo de esos requisitos exige una ponderación de los derechos e intereses en conflicto, que dependerá, en principio, de las circunstancias concretas del caso particular de que se trate y en cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea confieren al interesado». En el mismo sentido, cabe mencionar también la más reciente STJUE de 11 de diciembre de 2019 (asunto TK), apartado 32.
47. Informe 09/2019 del Gabinete Jurídico Agencia Española de Protección de Datos sobre interés legítimo, SSTJUE de 24 de noviembre de 2011 (asunto ASNEF y FECEDM), apartado 38 y de 11 de diciembre de 2019 (asunto TK), apartado 32.
48. La jurisprudencia constitucional ha advertido la íntima relación del derecho a la prueba con otros derechos integrados en el art. 24 de la CE. Sirva a ello el siguiente pasaje contenido en las SSTC 212/2013, de 16 de diciembre y 88/2014, de 28 de mayo: «Concretamente, en nuestra doctrina constitucional hemos hecho hincapié en la conexión de este específico derecho constitucional con el derecho a la tutela judicial efectiva (art. 24.1 CE), cuyo alcance incluye las cuestiones relativas a la prueba (SSTC 89/1986, de 1 de julio, FJ 2; 50/1988, de 22 de marzo, FJ 3; 110/1995, de 4 de julio, FJ 4; 189/1996, de 25 de noviembre, FJ 3; y 221/1998, de 24 de noviembre, FJ 3), y con el derecho de defensa (art. 24.2 CE), del que es inseparable (SSTC 131/1995, de 11 de septiembre, FJ 2; 1/1996, de 15 de enero, FJ 2; y 26/2000, de 31 de enero, FJ 2)».
49. SSTC 19/2001, de 29 de enero y 133/2003, 37/2000, de 14 de febrero.
50. En base a estas circunstancias y a los intereses legítimos afectados, es claro que la presente base jurídica de legitimación solo podrá sustentar, en su caso, la comunicación de datos que haga alguna de las partes personadas en el proceso, descartándose la de terceras personas o responsables ajenos que pudieran, por ejemplo, intervenir como testigos o contar con documentación útil.
51. También ha sido validada la persecución de un interés público general como causa de utilización de esta vía de licitud para efectuar la comunicación de datos personales a un tercero. Y no debe obviarse que el Considerando (50) del RGPD considera a este supuesto como de interés legítimo, al precisar que «La indicación de posibles actos delictivos o amenazas para la seguridad pública por parte del responsable del tratamiento y la transmisión a la autoridad competente de los datos respecto de casos individuales o casos diversos relacionados con un mismo acto delictivo o amenaza para la seguridad pública debe considerarse que es en interés legítimo del responsable».

colectivos que resultan de una notable relevancia constitucional desde el punto de vista nacional y que trascienden al ámbito internacional y comunitario.

Mientras, el derecho en liza del interesado cuyos datos van a ser comunicados se identificaría con algún interés o derecho y libertad fundamental que encuentre protección a través del derecho a la protección de los datos de carácter personal, como garante de los demás derechos del individuo. Cierto es que habrá que atender al caso concreto y las propias expectativas razonables de los interesados basadas en su relación con el responsable[52], si bien, debe advertirse que la lesión que pudiera producirse en interesado será superior cuando la cesión consistiera en datos que figuran en fuentes no accesibles al público o que pertenecieran a categorías especiales de datos[53], pues como afirma el TJUE, el órgano judicial, como destinatario primero y las demás partes personadas, dispondrían de ciertas informaciones sobre la vida privada del interesado que pueden incidir en su núcleo irreductible. De modo que la probable «lesión en los derechos del interesado consagrados en los artículos 7 y 8 de la Carta debe ser apreciada en su justo valor, contrapesándola con el interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos»[54].

Una vez definidos todos los derechos e intereses enfrentados, deberá procederse a efectuar una meticulosa ponderación[55] entre todos ellos basada en los siguientes factores. De su resultado dependerá *prima facie* la eventual licitud de la comunicación:

a) La evaluación del interés legítimo del responsable del tratamiento: debemos tener en cuenta que se tratan de derechos fundamentales e intereses públicos colectivos que trascienden a toda la sociedad y que se reconocen en los principales Convenios sobre Derechos Humanos. También la jurisprudencia ha admitido la primacía general de ambos intereses en detrimento del derecho a la protección de datos[56]. Dada la importancia de estos y lo apremiante de su uso, es posible, *a priori*, y a falta de sopesar los demás criterios, justificar «una intrusión significativa en la privacidad o cualquier otra repercusión importante en los intereses o derechos de los interesados».
b) El impacto sobre el interesado: se trata de valorar la repercusión que se deriva para el interesado de la comunicación de sus datos personales al órgano judicial. Se deben sopesar factores como la naturaleza de los datos personales cedidos[57], la manera en que se trata la información, las expectativas razonables de privacidad con las que contaba y la posición de equilibrio entre el responsable del tratamiento y del interesado. En este

52. Considerando (47) del RGPD.
53. «Al estar dotados de garantías reforzadas, su uso para la investigación y prueba de delitos, presenta un grado de injerencia superior en la esfera jurídico fundamental, por lo que estas barreras de protección robustas, podrían generar un *óbice* a la persecución penal no siempre justificable». *Vid*. Pérez Gil, «Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal» en *Justicia* ¿Garantías *"versus" eficiencia?* (Jiménez Conde y Bellido Penadés, Dirs.), Tirant Lo Blanch, Valencia, 2019, pág. 416.
54. STJUE de 24 de noviembre de 2011 (asunto ASNEF y FECEDM), apartado 45.
55. Así lo exige el Considerando 47 del RGPD al afirmar que «En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin». Palma Ortigosa, «*Principios* relativos al tratamiento de datos personales» …, *op. cit.*, pág. 42.
56. En la STC 292/2000, de 30 de noviembre se afirmó que «*…el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, FJ 7; 196/1987, de 11 de diciembre, FJ 6; y respecto del art. 18, la STC 110/1984, FJ 5). En cuanto a los límites de este derecho fundamental no estará de más recordar que la Constitución menciona en el art. 105 b) que la ley regulará el acceso a los archivos y registros administrativos "salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas" (en relación con el art. 8.1 y 18.1 y 4 CE), y en numerosas ocasiones este Tribunal ha dicho que la persecución y castigo del delito constituye, asimismo, un bien digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana. Bienes igualmente reconocidos en los arts. 10.1 y 104.1 CE (por citar las más recientes, SSTC 166/1999, de 27 de septiembre, FJ 2, y 127/2000, de 16 de mayo, FJ 3.a; ATC 155/1999, de 14 de junio)*».
57. La presencia de datos pertenecientes a categorías especiales se tratará de un factor determinante y un hándicap para el uso del interés legítimo como base de tratamiento, si bien tampoco insalvable, pues el Considerando 52 autoriza expresamente «*a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial*».

ISSN: 2951-844X

aspecto, es incontestable que si el interesado es conocedor de los datos que son objeto de tratamiento y de su posible utilidad en el proceso, es razonable que pueda prever su potencial uso.

c) Equilibrio provisional: se refiere al grado de cumplimiento de la normativa de protección de datos y transparencia por el responsable. De este modo, un mejor cumplimiento podría implicar un uso justificado de la base legitimadora.
d) Las garantías adicionales para mantener la seguridad e integridad de los datos y para minimizar el impacto en los derechos del interesado que pueda adoptar el responsable o cesionario[58].

En términos generales, deberemos indicar que, con carácter habitual, la parte en el proceso que tenga interés en aportar medios probatorios basados en datos personales con el objeto de ejercer su derecho de defensa en garantía de la tutela judicial efectiva, encontrará en el interés legítimo a un aliado para asegurar la licitud del tratamiento. La jurisprudencia de todos los ámbitos es prácticamente unánime al determinar que el derecho a la protección de datos del interesado no es ilimitado, y que puede ceder cuando se enfrenta a otros derechos fundamentales y bienes jurídicos protegidos constitucional o convencionalmente. Habiendo señalado explícitamente a «la seguridad y defensa del Estado[59]» y a «la persecución y castigo del delito[60]» como algunos de los límites que pueden prevalecer frente al derecho a la autodeterminación informativa. En cualquier caso, se torna esencial y prioritario que el responsable proceda, con carácter previo a materializar la comunicación de datos al juzgado, a realizar una minuciosa ponderación de los intereses y derechos en liza, en el que, además de valorar los precitados factores orientadores, se preste una especial atención a la proporcionalidad de la medida, pues de su resultado se verificará la viabilidad del uso de tal vía legal para realizar la aportación de datos al proceso y garantizar así su licitud y eficacia.

4. El tratamiento es necesario para una misión de interés público o para el ejercicio de poderes públicos

Ante la imposibilidad de aplicación de cualquiera de las anteriores bases, en ciertos supuestos muy concretos es posible ampararse para realizar una cesión de datos a un órgano judicial en la base consistente en la necesidad del tratamiento de los datos por el destinatario para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos. El Grupo del art. 29 ha estimado válida la revelación de datos a la autoridad competente cuando sean útiles para la investigación o enjuiciamiento de delitos como forma de cooperación voluntaria y espontánea del responsable que cede los datos, en aquellos casos en que no exista un previo requerimiento formal y coactivo del tribunal en el que se solicite su entrega[61]. Ello puede deberse a que el órgano judicial desconozca la

58. Resulta especialmente interesante e ilustrativa la lectura del Informe del Gabinete Jurídico de la AEPD con número 0456/2015, pues efectúa una ponderación de todos y cada uno de los factores expuestos respecto a la eventual comunicación de las grabaciones de un sistema de video vigilancia a un órgano judicial para proceder al enjuiciamiento penal, basado en la existencia de interés legítimo.

59. En el plano nacional destacan las SSTC 166/1999, de 27 de septiembre (F. J. 2º), 127/2000, de 16 de mayo (F. J. 3º), 292/2000, de 30 de noviembre y el ATC 155/1999, de 14 de junio. En el ámbito del TEDH, las sentencias de 26 de marzo de 1987 (asunto Leander *vs*. Suecia), apartado 47. Y de la jurisprudencia del TJUE, las sentencias de 29 de enero de 2008 (asunto *Promusicae*), apartado 53; 8 de abril de 2014 (asunto *Digital Rights Ireland*), y 21 de diciembre de 2016 (asunto *Tele 2 Sverige AB)*, apartados 41 a 44.

60. También en el ámbito nacional puede citarse la siguiente jurisprudencia nacional: SSTC 166/1999, de 27 de septiembre (F. J. 2º) y 127/2000, de 16 de mayo (F. J. 3º). Y en el ámbito del CEDH, las SSTEDH de 25 de febrero de 1997 (asunto Z. *vs*. Finlandia), y de 25 de febrero de 1993 (asunto Funke *vs*. Francia). Y de la jurisprudencia del TJUE, las sentencias de 23 de noviembre de 2010 (asunto *Tsakouridis*) apartados 46 y 47; de 29 de enero de 2008 (asunto *Promusicae*), apartado 53; 8 de abril de 2014 (asunto *Digital Rights Ireland*), apartado 29 y de 21 de diciembre de 2016 (asunto *Tele 2 Sverige AB*), apartado 90.

61. El Dictamen 06/2014 del GTA29 alude específicamente a este caso como incluido en tal base legal, explicando que esta «comprende situaciones en las que el responsable del tratamiento no tiene una potestad oficial, pero una tercera parte con dicha potestad le solicita que revele los datos. Por ejemplo, un funcionario de un organismo público competente para investigar delitos puede pedir al responsable del tratamiento que coopere en una investigación en curso, en vez de ordenar al responsable del tratamiento que cumpla una solicitud específica de cooperación. El artículo 7, letra e), cubre además situaciones en las que el responsable del tratamiento comunica de forma proactiva los datos a una tercera parte con dicha potestad oficial. Este puede ser el caso, por ejemplo, de que el responsable del tratamiento advierta que se ha cometido un delito penal y facilite esta información a las autoridades competentes con funciones coercitivas por iniciativa propia. A diferencia del caso del artículo 7, letra c), no se exige que el responsable del tratamiento actúe en virtud de una obligación jurídica. Utilizando el ejemplo anterior, puede que un responsable del tratamiento que advierta de manera accidental que se ha cometido un robo

existencia de tales datos, su concreta ubicación en un fichero o porque exista un retraso o una averiguación pendiente en la solicitud.

En vista de lo anterior, cabe colegir que solamente sujetos que no ostenten la condición de parte en el proceso para el que resulten beneficiosos los datos personales y que no tengan una obligación legal de aportarlos podrán ampararse en esta base de legitimación, mostrándose este como un fundamento residual para aquellas situaciones que no encuentren apoyo en alguno de los principios vistos con anterioridad.

VI. REQUISITOS LEGITIMADORES DE LA CESIÓN DE DATOS PERSONALES PARA FINES INCOMPATIBLES

El segundo y último de los requisitos que, con carácter general, exige el RGPD en su art. 6.4 para efectuar una comunicación de datos personales que pueda entenderse lícita, es que la finalidad a la que se destinen sea compatible con la primitiva que dio lugar a su recogida inicial, aun no siendo ambas plenamente coincidentes. Dada la indeterminación del concepto jurídico de compatibilidad, la norma establece una serie de factores orientadores con los que el responsable podrá guiarse, a fin de llevar a cabo una evaluación que permita dilucidar la afinidad de los diferentes fines que resulten[62]. Sin embargo, consciente el legislador comunitario del probable surgimiento *ex novo* de inéditos e imperiosos fines a los que destinar los datos personales[63], en principio sin conexión alguna con los primitivos, lo que impediría de plano su uso, ha instaurado un régimen alternativo y excepcional que sustituye la aplicación del criterio de la compatibilidad de fines, por el de la habilitación legal expresa que sea respetuosa con el examen de proporcionalidad característico del CEDH y Convenio 108[64].

Al resultar esta vía alternativa para la legitimación de las cesiones de datos de carácter especialmente extraordinario, se reserva exclusivamente para la salvaguarda de alguno de los bienes jurídicos individuales o colectivos más valiosos de la sociedad, que son recogidos en el artículo 23 del RGPD. En este listado es posible localizar aquellos intereses que, de un modo u otro, se involucran en una cesión de datos que tenga por destinatario a un órgano judicial del orden penal para la tramitación de un proceso. De este modo, se relacionan como bienes jurídicos colectivos y se hace expresa mención a la seguridad pública; a la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención y, finalmente, a la protección de la independencia judicial y de los procedimientos judiciales. Mientras tanto, como bien jurídico individual se localiza a la defensa, que debe ser interpretada de forma amplia, para dar cobijo a cualquiera de las dimensiones del derecho a la defensa, incluida la utilización de los medios probatorios necesarios para el convencimiento del juez.

En este punto, se torna necesario verificar la concurrencia de las condiciones exigidas por el precepto: en primer lugar, la existencia en el ordenamiento nacional o comunitario de una norma legal que habilite expresamente a un responsable del tratamiento o a individuo a título particular a comunicar datos personales de terceros a un órgano judicial para su uso con fines probatorios y de defensa o por resultar imprescindibles para el ejercicio de la potestad jurisdiccional en el ámbito penal. Y, en segundo término, de ser la anterior confirmada, comprobar si la medida resulta necesaria y proporcional en un estado democrático (en sentido abstracto y concreto). La superación de ambos requisitos supondrá la superación del canon de proporcionalidad exigido por el art. 9 del Convenio 108 y por

o un fraude no tenga la obligación jurídica de informar de ello a la policía, pero puede, no obstante, en determinados casos, hacerlo así voluntariamente». *Vid.* Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, pág. 23.

62. Puyol Montero, «Los principios del derecho a la protección de datos» …, *op. cit.*, págs. 138-139 y Palma Ortigosa, «Principios relativos al tratamiento de datos personales» …, *op. cit.*, págs. 44-45.

63. Tanto si el tratamiento para un nuevo uso tendrá lugar por el propio responsable o por un destinatario.

64. El Considerando (50) del RGPD lo explica tal que así: «Si el interesado dio su consentimiento o el tratamiento se basa en el Derecho de la Unión o de los Estados miembros que constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, en particular, objetivos importantes de interés público general, el responsable debe estar facultado para el tratamiento ulterior de los datos personales, con independencia de la compatibilidad de los fines».

ISSN: 2951-844X

el art. 8 del CEDH[65] para el establecimiento de limitaciones al derecho a la protección de datos de carácter personal[66], presupuestos esenciales para garantizar la validez de la cesión de datos a efectos penales.

1. Norma legal habilitante para la cesión de datos de carácter personal en el ámbito procesal penal

El primero de los requisitos exigidos por el art. 5.4 del RGPD en relación con el 23 del mismo texto es que el tratamiento y su finalidad deben de estar basados en el derecho de la Unión o del Estado miembro. Regla que, con carácter general, contemplan los diferentes sistemas jurídicos de protección de los derechos fundamentales y que se identifica con la necesaria reserva de ley que se precisa de cualquier medida que implique una limitación de aquellos[67]. Pues la reserva de ley exigida por la Constitución para la regulación de los derechos y libertades fundamentales que reconoce desempeña una doble función. En primer lugar, la función de asegurar que los derechos de los ciudadanos no se vean afectados por ninguna injerencia estatal no autorizada por sus representantes; y, por otro lado, otra función es garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas, habida cuenta del sometimiento de los jueces y magistrados al imperio de la ley en la aplicación del ordenamiento jurídico. Derivándose de estas funciones una doble exigencia. En primer lugar, la necesaria existencia de una ley que desarrolle o limite al derecho fundamental que reúna, a su vez, «todas aquellas características indispensables como garantía de la seguridad jurídica», esto es, «ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención»[68]. Y, en segundo lugar, que congregue, además, las exigencias de

65. Recuérdese que el art. 52.3 de la CDFUE remite al CEDH en lo tocante al sentido y alcance de los derechos reconocidos por ambos instrumentos, al precisar que «En la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán iguales a los que les confiere dicho Convenio. Esta disposición no impide que el Derecho de la Unión conceda una protección más extensa». La sentencia del TJUE de 17 de diciembre de 2015 (asunto *Web Mind Licenses*) señaló, en relación al derecho a la intimidad familiar y personal, aunque es plenamente trasladable al ámbito del derecho a la protección de datos, que «el artículo 7 de la Carta, referido al derecho al respeto de la vida privada y familiar, contiene derechos equivalentes a los garantizados por el artículo 8, apartado 1, del CEDH, y que, por consiguiente, conforme al artículo 52, apartado 3, de la Carta, debe darse a dicho artículo 7 el mismo sentido y el mismo alcance que los conferidos al artículo 8, apartado 1, del CEDH, tal como lo interpreta la jurisprudencia del Tribunal Europeo de Derechos Humanos».

66. Y más específicamente, como afirma el TJUE en su sentencia de 9 de noviembre de 2010 (asunto *Markus Schecke*) «las limitaciones al derecho a la protección de los datos de carácter personal que pueden establecerse legítimamente [en el plan comunitario] corresponden a las toleradas en el contexto del artículo 8 del CEDH».

67. Por mandado constitucional, toda injerencia en el ámbito de los derechos fundamentales y libertades, que incida sobre su desarrollo o que limite o condicione su ejercicio precisa una habilitación legal, *vid*. STC 49/1999, de 5 de abril (F.J. 4.º). Habiendo confirmado el Tribunal Constitucional en aplicación de estas reglas al derecho a la protección de datos en su STC 292/2000, de 30 de noviembre (F.J. 11.º) que «(…) este Tribunal ha declarado que el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, FJ 7; 196/1987, de 11 de diciembre, FJ 6; y respecto del art. 18, la STC 110/1984, FJ 5). Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE. La primera constatación que debe hacerse, que no por evidente es menos capital, es que la Constitución ha querido que la Ley, y sólo la Ley, pueda fijar los límites a un derecho fundamental (SSTC 57/1994, de 28 de febrero, FJ 6; 18/1999, de 22 de febrero, F.J. 2)». En el ámbito comunitario ,de acuerdo a lo dispuesto en el artículo 52, apartado 1, de la CDFUE, «cualquier limitación del ejercicio de los derechos y libertades reconocidos por *ésta* deberá ser establecida por la ley, respetar su contenido esencial y, dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones a dichos derechos y libertades cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás». Mientras, en el plano del CEDH, su art. 8.2 dispone que «No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

68. STC 49/1999, de 5 de abril (F.J. 4.º).

previsibilidad y certeza de las medidas restrictivas en el ámbito de los derechos fundamentales[69]. La falta de cualquiera de estos elementos, además de lesionar al principio de seguridad jurídica que se proclama en el art. 9.3 de la CE y se materializa en la necesaria certeza sobre el ordenamiento y en la expectativa fundada de la persona, sobre las consecuencias de la aplicación de la norma, lesionaría el contenido esencial del derecho fundamental que se restringe, «dado que la forma en que se han fijado sus límites lo hacen irreconocible e imposibilitan, en la práctica, su ejercicio»[70]. En similares términos se ha expresado el TEDH en relación con el art. 8 del CEDH, en el que se reconoce el derecho a la vida privada y familiar, pero en el que se integra, además, la protección de datos de carácter personal. A tal efecto, se exige que las limitaciones que se planteen deben estar previstas en una ley accesible para el individuo y que las consecuencias de su aplicación sean previsibles[71].

En cualquier caso, el Tribunal Constitucional ha tenido ocasión de pronunciarse sobre la modalidad de ley que requiere adoptar una norma que regule la cesión de datos personales para destinar los mismos a otra finalidad distinta y sin consentimiento del interesado, expresando al efecto que «de acuerdo con el art. 53.1 CE, el ejercicio de los derechos y libertades reconocidos en el capítulo segundo, del título I, solo podrá regularse por ley, por lo que hay que deducir que, si bien los límites al derecho a consentir la cesión de datos para fines distintos para los que fueron recabados está sometido a reserva de ley»[72].

Sentado lo anterior, resulta necesario acudir al ordenamiento nacional para verificar la existencia de una norma que avale y legitime la comunicación de datos personales de terceros que un responsable o particular pueda efectuar a un órgano judicial para la tramitación de un proceso penal. Lo cierto es que, hasta la derogación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal., existía en esta un precepto específico que facultaba a los responsables para ceder datos personales a un órgano judicial, sin consentimiento del titular, cuando la finalidad radicara en el ejercicio de las funciones que por ley se le atribuyen. Este elemento normativo suponía, en toda regla, una habilitación legal y específica para la entrega de datos de terceros que permitiría colmar las exigencias planteadas por el RGPD.

De hecho, la Agencia Española de Protección de Datos[73] y la jurisprudencia[74] consideraron a este precepto como suficiente para legitimar la cesión de datos a un órgano judicial. Nos referimos al hoy derogado art. 11.2.d), que expresaba: «1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para

69. En la STC 292/2000, de 30 de noviembre (F.J. 15.º), el Tribunal Constitucional ya señaló al respecto que «aun teniendo un fundamento constitucional, las limitaciones del derecho fundamental establecidas por una ley "pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad en los propios límites que imponen y su modo de aplicación", pues "la falta de precisión de la ley en los presupuestos materiales de la limitación de un derecho fundamental es susceptible de generar una indeterminación sobre los casos a los que se aplica tal restricción"; "al producirse este resultado, más allá de toda interpretación razonable, la ley ya no cumple su función de garantía del propio derecho fundamental que restringe, pues deja que en su lugar opere simplemente la voluntad de quien ha de aplicarla"».

70. SSTC 11/1981, de 8 de abril (F.J. 15.º); 142/1993, de 22 de abril (F.J. 4.º); y 341/1993, de 18 de noviembre (F.J. 7.º).

71. Sentencias del Tribunal Europeo de Derechos Humanos, de 26 de marzo de 1985 (asunto X e Y *vs*. Países Bajos); de 26 de marzo de 1987 (asunto Leander *vs*. Suecia); de 7 de julio de 1989 (asunto Gaskin *vs*. Reino Unido) y de 25 de febrero de 1993 (asunto Funke *vs*. Francia).

72. STC 139/2016, de 21 de julio de 2016 (F. J. 13º).

73. Resoluciones de la AEPD de 18 septiembre de 2009 y de 21 septiembre de 2007, que con un contenido similar expresaban que «la aportación de la documentación con la que el correspondiente perito ha elaborado su informe, tanto a la demandante, como a los tribunales, existiría una habilitación legal para la comunicación de datos sin consentimiento, en base a la aplicabilidad del artículo 11.2 de la LOPD, como de la LEC. Además, hemos de recordar la aplicabilidad del principio del derecho a la tutela judicial efectiva y a la utilización por las partes de los medios de prueba que estimen oportunos, que se encuentra recogido en la propia constitución y que jurisprudencialmente ha recibido una valoración que determina su prevalencia sobre el derecho a la protección de datos de carácter personal».

74. La sentencia AN de 26 noviembre 2008 ha avalado las cesiones de datos producidas en virtud de este precepto, al considerar la preponderancia del derecho a la defensa y a la tutela judicial efectiva sobre el derecho a la protección de datos de carácter personal. Por su parte, la Audiencia Provincial de Madrid en su sentencia de fecha 5 de septiembre de 2005, posteriormente avalada por la STS (Sala 3.ª) 1106/2012, de 27 de febrero, consideró que «A la vista de estos preceptos, el legislador ha creado un sistema en que el derecho a la protección de datos de carácter personal cede en aquellos supuestos en que el propio legislador (constitucional u ordinario) haya considerado la existencia de motivos razonados y fundados que justifiquen la necesidad del tratamiento de los datos, incorporando dichos supuestos a normas de, al menos, el mismo rango que la que regula la materia protegida. En efecto, la exigibilidad del consentimiento del oponente para el tratamiento de sus datos supondría dejar a disposición de aquél el almacenamiento de la información necesaria para que el denunciante pueda ejercer, en plenitud, su derecho a la tutela judicial efectiva Así, la falta de estos datos o su comunicación a la contraparte, puede implicar, lógicamente, una merma en la posibilidad de aportación por el interesado de "los medios de prueba pertinentes para su defensa", vulnerándose otra de las garantías derivadas del citado derecho a la tutela efectiva y coartándose la posibilidad de obtener el pleno desenvolvimiento de este derecho. En consecuencia, la comunicación de los datos del denunciante al citado Tribunal se encontraba amparada por el citado artículo 11.2.d) de la LOPD».

el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. 2. El consentimiento exigido en el apartado anterior no será preciso: (…) d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los jueces o tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas (…)».

Dada la derogación de la norma que albergaba el precitado precepto, debemos comprobar si el legislador ha previsto una base legal alternativa que sirva de soporte a las cesiones de datos que puedan producirse entre un responsable del tratamiento y un órgano judicial penal. Tras la reforma operada por la Ley Orgánica 7/2021 en los preceptos encargados de regular el marco jurídico del derecho a la protección de datos Ley Orgánica del Poder Judicial, la habilitación genérica, para cualquier orden jurisdiccional, podría entenderse ubicada hoy día en el tercero de los apartados del art. 236 *ter* de la LOPJ[75]. Este expresa textualmente que «No será necesario el consentimiento del interesado para que se proceda al tratamiento de los datos personales en el ejercicio de la actividad jurisdiccional, ya sean éstos facilitados por las partes o recabados a solicitud de los órganos competentes, sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba». Como puede comprobarse de su lectura, el precepto avala de modo indirecto la comunicación de datos personales que se produce entre un responsable o particular y un órgano judicial para su uso con fines jurisdiccionales. Si bien, es cierto que, sin distinguir si los datos pertenecen a la aportante o a un tercero, cabe entender implícitamente que la autorización abarca a ambos, dada la condición de responsable o encargado del tratamiento que se presupone como destinatario de la ley y la distinción que efectúa entre interesado y parte aportante. De este modo, aunque sería deseable un precepto que autorizara expresamente a un responsable o particular a entregar datos personales de terceros con fines de defensa o por el interés común de reprimir la criminalidad a través del buen fin del proceso penal, lo cierto es que puede entenderse colmado el requisito de exigencia de ley formal, de calidad y accesible con los preceptos vigentes hoy día, que deben, a su vez, integrarse con el art. 118 de la CE respecto a los supuestos en que la cesión traiga consecuencia de un requerimiento judicial.

Asimismo, no se pueden obviar otros supuestos específicos que se localizan en ciertos sectores del ordenamiento jurídico, en los que la ley habilita, o incluso obliga, expresamente a terceros sujetos públicos o privados para ceder datos personales a un órgano judicial para su uso con fines penales. Son supuestos que, por las circunstancias cuantitativas y/o cualitativas del tratamiento y de los datos, han merecido una atención específica del legislador. Habitualmente nos situaremos ante datos que, por su naturaleza, disponen de una importante capacidad para revelar aspectos íntimos y reservados de la vida de las personas o que son conservados expresamente con fines preventivos del delito. Por tanto, requieren de unas condiciones de tratamiento y cesión mucho más estrictas que las que pudieran exigirse de un responsable del tratamiento ordinario. Recordemos el art. 95.1.a) de la LGT respecto a los datos de trascendencia tributaria, que autoriza su cesión cuando sean necesarios para «La colaboración con los órganos jurisdiccionales y el Ministerio Fiscal en la investigación o persecución de delitos que no sean perseguibles únicamente a instancia de persona agraviada». El art. 77.1.a) del Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social, respecto a los datos obrantes en los ficheros de todos los organismos de la Seguridad Social. El art. 6 de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, respecto a los datos de comunicaciones electrónicas conservados para fines penales. O el art. 43.3 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo respecto de la cesión de los datos contenidos en los Ficheros de Titularidades Financieras para la investigación exclusiva de delitos relacionados con el blanqueo de capitales o la financiación del terrorismo. En cualquier caso, para las cesiones de datos que se producen mediante requerimiento judicial, nos topamos con el art. 7 de la Ley Orgánica 7/2021, de 26 de mayo, que, regulando el deber de colaboración de los ciudadanos, sirve como cláusula legal habilitante suficiente para cubrir tales supuestos.

2. Juicio de proporcionalidad de la medida

El segundo de los requisitos que debe cumplir la medida legal que habilite a la cesión de datos de un tercero a un órgano judicial para su tratamiento con alguno de los fines de naturaleza penal que se enumeran en el art. 1 de la Ley Orgánica 7/2021, de 26 de mayo, puede concretarse en la superación del juicio de proporcionalidad, en tanto en cuanto nos hallamos ante una medida legislativa restrictiva de un derecho fundamental. Este presupuesto debemos analizarlo desde dos puntos de vista. En primer lugar, en abstracto, como proporcionalidad de la medida legal que

75. Acuerdo adoptado por el Pleno del Consejo General del Poder Judicial de 26 de octubre de 2017 que aprueba el Informe Complementario sobre el Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal, pág. 5.

avala la cesión de datos sin consentimiento. Y la segunda, desde el punto de vista material de aplicación, es decir, desde su perspectiva práctica.

Para poder avalar la legitimidad de la injerencia, la medida deberá respetar en lo esencial al derecho en el que se produce la lesión y, además, debe ser necesaria y proporcionada para la salvaguarda de otros derechos o intereses legítimos. Pues, como ha considerado la constante jurisprudencia del Tribunal Constitucional, la Constitución no impide al legislador proteger derechos o bienes jurídicos a costa del sacrificio de otros igualmente reconocidos constitucionalmente. Es decir, habilita a este para que pueda establecer limitaciones al contenido de los derechos fundamentales o a su ejercicio, con la condición de que estas encuentren justificación en la protección o salvaguarda de otros derechos e intereses[76] y, además, sean proporcionadas al fin perseguido[77].

Debemos traer a colación, una vez más, la jurisprudencia del TC en la que se concreta al núcleo del derecho a la protección de datos, que identifica con «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. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos[78]».

Por tanto, se integran en su núcleo los derechos del interesado a consentir el tratamiento de sus datos por un responsable y a obtener información sobre su identidad y los usos a los que van a ser destinados, pudiendo en cualquier momento oponerse al mantenimiento de la posesión. Extendiéndose dichas facultades no únicamente respecto del responsable que recogió los datos inicialmente, sino también a los eventuales cesionarios a los que los datos pudieran haber sido comunicados[79]. De modo que puede considerarse al derecho a la protección de datos como un derecho que faculta a la persona para controlar el flujo de su información personal y para oponerse a que sus datos sean utilizados para fines distintos de aquel legítimo que justificó su obtención[80]. Y ello con respecto a todos los datos personales, con independencia de que se refieran a los ámbitos más íntimos y reservados de la vida privada o no.

De lo expuesto, puede colegirse que se comprende en el núcleo duro del derecho a la autodeterminación informativa la facultad de consentir la cesión de datos a terceros para su empleo con nuevos fines. Interpretación que ha sido confirmada por el Tribunal Constitucional, incluso teniendo en cuenta los principales convenios internacionales en la materia, como son el art. 8 de la CDFUE y el Convenio 108 del Consejo de Europa de 1981, de conformidad con el mandato dispuesto en el art. 10.2 de la CE[81].

Visto lo anterior, debemos continuar el análisis, mencionando que el derecho a la protección de datos no es absoluto y por tanto puede ser objeto de limitación. Así lo ha considerado la jurisprudencia constitucional y la procedente de los principales tribunales internacionales cuya doctrina es vinculante para nuestro Estado[82]. Y aunque Constitución no haya fijado directamente ningún límite específico a este derecho, éstos deben de hallarse, como en cualquier

76. SSTC 104/2000, de 13 de abril (F.J. 8.º); 27/1981, de 20 de julio (F.J. 10.º); 66/1985, de 23 de mayo (F.J. 1.º) y 108/1986, de 29 de julio (F.J. 18º.).

77. SSTC 11/1981, de 8 de abril (F.J. 5.º) y 196/1987, de 11 de diciembre (F.J. 6.º).

78. STC 292/2000, de 30 de noviembre (F.J. 7.º).

79. Pues el Tribunal Constitucional ha declarado que las facultades del titular del derecho a la protección de datos consistentes en exigir del titular del fichero que le informe de los datos que trata, sus usos acceder a los registros «alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele». STC 292/2000, de 30 de noviembre (F.J. 7.º).

80 SSTC 11/1998, de 12 de febrero (F.J. 5.º) y 94/1998, de 4 de mayo (F.J. 4.º).

81. En su STC 292/2000, de 30 de noviembre (F.J. 8.º) declaró sobre el Convenio 108 que «Ahora bien, aun habiendo llegado a esta conclusión no es ocioso señalar, de un lado, que el derecho a consentir la recogida y el tratamiento de los datos personales no implica en modo alguno consentir la cesión de tales datos a terceros, pues constituye una facultad específica que también forma parte del contenido del derecho fundamental a la protección de tales datos. Y, por tanto, la cesión de los mismos a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aun cuando puedan ser compatibles con éstos, supone una nueva posesión y uso que requiere el consentimiento del interesado».

82. En el plano nacional puede verse la STC 292/2000, de 30 de noviembre (F.J. 8.º). En el ámbito comunitario, el TJUE ha dictaminado que «El derecho a la protección de los datos de carácter personal no constituye una prerrogativa absoluta, sino que debe ser considerado en relación con su función en la sociedad». *Vid.* STJUE de 9 de noviembre de 2010 (asunto *Volker und Markus Schecke y Eifert*), apartado 48 y jurisprudencia citada.

otro caso, en los demás «derechos fundamentales y bienes jurídicos constitucionalmente protegidos, por mor del principio de unidad constitucional[83]». Habiendo reconocido expresamente el Tribunal Constitucional que, entre los bienes jurídicos que pueden prevalecer ante el derecho a la protección de datos, se sitúan algunos de los que entran en confrontación en los supuestos en que un responsable cede datos personales a un órgano judicial penal. Como pudieran ser el interés de la sociedad en investigar y reprimir las actuaciones delictivas[84], dado que, a través de ellos, se defienden otros intereses generales reconocidos en el plano constitucional, como son la paz social y la seguridad ciudadana, localizados en los arts. 10.1 y 104.1 de la CE[85]. Límites viables de este derecho que también han sido reconocidos por el TEDH, tras atender a lo dispuesto en el art. 9 del Convenio 108 de 1981. Por ejemplo, el tribunal se ha referido claramente a la seguridad del Estado en la sentencia de 26 de marzo de 1987 (asunto Leander *vs*. Suecia) y a la persecución de infracciones penales en las sentencias relativas a los casos de 25 de febrero de 1997 (asunto Z. *vs.* Finlandia) y de 25 de febrero de 1993 (asunto Funke *vs*. Francia).

Cierto es que, respecto al derecho fundamental a la tutela judicial efectiva en su dimensión a la garantía de utilización de pruebas pertinentes para la defensa, no existe un pronunciamiento constitucional que haya refrendado a este como un eventual límite del derecho a la protección de datos, aunque no por ello debe desecharse tal posibilidad, puesto que el Tribunal Constitucional ha declarado que «el apoderamiento legal que permita a un Poder Público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, sólo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos», categoría en la que, evidentemente, se encuadran los derechos procesales señalados.

En todo caso, la doctrina de la AEPD[86] y una escasa, pero cierta jurisprudencia[87] han avalado este argumento. Responde, por tanto, esta medida legal a objetivos de interés general, tal y como exige igualmente el art. 52.1 de la CDFUE, puesto que persigue que los datos personales de los que disponga un tercero puedan ser utilizados con fines de investigación o enjuiciamiento criminal. También la jurisprudencia del Tribunal de Justicia de la Unión Europea ha reconocido a estos como intereses generales europeos, apoyándose, en primer lugar, en los derechos a la seguridad y libertad que se reconocen en el art. 6 de la CDFUE. Pues la lucha contra la delincuencia colabora para garantizar la seguridad pública[88] y, particularmente, la que tiene lugar contra el terrorismo internacional, para el mantenimiento de la paz y la seguridad internacionales[89]. En último lugar, respecto al derecho a la tutela judicial efectiva, no cabe duda de que se puede considerar un elemento de interés general para la Unión, habida cuenta de su reconocimiento como derecho fundamental autónomo en el art. 47.1 de la CDFUE y su función instrumental para la defensa de los demás derechos. Pero más allá de ello, el TJUE ha afirmado que constituye un objetivo legítimo de interés general no impedir la utilización de documentos en procedimientos judiciales, como dimensión de aquel derecho[90].

Ahora bien, según la doctrina constitucional, los límites que se impongan a los derechos fundamentales y libertades públicas deben de ser respetuosos con el contenido esencial del derecho restringido, ser necesarios para lograr la finalidad prevista y, en todo caso, proporcionados[91]. Canon también se establece, en términos más o menos similares, por el art. 52.1 de la CDFUE y el art. 8 del CEDH. Pues el primero exige que «cualquier limitación del ejercicio de los derechos y libertades reconocidos por ésta deberá ser establecida por la Ley, respetar su contenido esencial y dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones al ejercicio de esos derechos y libertades cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás[92]». Mientras, el segundo exige que «tales limitaciones estén previstas legalmente y sean las indispensables en una sociedad democrática, lo que implica que la ley que establezca esos límites sea accesible al individuo concernido por ella, que resulten previsibles las consecuencias que para él pueda tener su aplicación, y que los límites respondan a una necesidad social impe-

83. SSTC 11/1981, de 8 de abril (F.J. 7.º); 196/1987, de 11 de diciembre (F.J. 6.º); y respecto del art. 18, la STC 110/1984, de 26 de noviembre (F.J. 5.º).
84. STC 292/2000, de 30 de noviembre (F.J. 8.º).
85. SSTC 166/1999, de 27 de septiembre (F.J. 2.º), y 127/2000, de 16 de mayo (F.J. 3.º).
86. Entre otros, el Informe Jurídico Gabinete Jurídico AEPD 0456/2015, el Informe 469/2011 de 30 de diciembre de 2011 y el Informe de 21 de febrero de 2001.
87. Sirvan de ejemplo la STS 1106/2012, de 12 de marzo de 2013 y la SAN 4691/2008, de 26 de noviembre.
88. STJUE de 23 de noviembre de 2010 (asunto Tsakouridis), apartados 46 y 47.
89. SSJUE de 3 de septiembre de 2008 (asunto *Kadi y Al Barakaat International Foundation vs.* Consejo y Comisión), apartado 363 y de 13 de noviembre de 2012 (asunto *Al-Aqsa vs*. Consejo), apartado 130.
90. Autos TJUE de 23 de octubre de 2002 (asunto Austria *vs*. Consejo), apartado 12; de 23 de marzo de 2007 (asunto *Stadtgemeinde Frohnleiten y Gemeindebetriebe Frohnleiten*), apartado 19, y de 29 de enero de 2009 (asunto *Donnici vs.* Parlamento), apartado 13.
91. SSTC 57/1994, de 28 de febrero (F. J. 6º); 18/1999, de 22 de febrero (F.J. 2.º).
92. STJUE de 15 de febrero de 2016 (asunto N**),** apartado 50.

riosa y sean adecuados y proporcionados para el logro de su propósito»[93]. Y, más concretamente, respecto a la limitación del derecho a la protección de datos consistente en la realización de una cesión de datos sin que intervenga el consentimiento del titular, el Tribunal Constitucional se ha pronunciado refiriéndose a ella como «Una facultad que sólo cabe limitar en atención a derechos y bienes de relevancia constitucional y, por tanto, esté justificada, sea proporcionada y, además, se establezca por Ley, pues el derecho fundamental a la protección de datos personales no admite otros límites»[94].

Comprobada la necesariedad y proporcionalidad en abstracto de la medida restrictiva de derechos fundamentales, procede examinar el respeto a su contenido esencial. De acuerdo con la jurisprudencia constitucional, una medida no será respetuosa con el núcleo esencial de un derecho fundamental cuando este «qued[e] sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección[95]». Lo cierto es que es no puede deducirse que una medida como la analizada atente contra el núcleo fundamental del derecho a la protección de datos, pues el propio Tribunal Constitucional ha avalado la acomodación constitucional de este tipo de tratamiento. Desde el plano de la jurisprudencia del TJUE, también debe rechazarse tal posibilidad, toda vez que, como ya advirtió en la sentencia *Digital Rights Ireland* en relación a la cesión de datos de tráfico y localización a las autoridades penales, aunque la medida constituya una injerencia grave en el derecho a la protección de datos, la existencia de «principios de protección y de seguridad de los datos» y la obligación de adoptar medidas «medidas técnicas y organizativas adecuadas contra la destrucción accidental o ilícita de los datos y su pérdida o alteración accidental» impide apreciar tal circunstancia[96]. Cabe precisar que la Directiva 2016/680/UE —y por ende la Ley Orgánica 7/2021— establece como principio rector del tratamiento en su art. 4.1.f) al de seguridad, obligando a que los datos sean «tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas», debiendo además el responsable ser capaz de demostrar el cumplimiento de este principio[97].

Toca en último lugar analizar la proporcionalidad de la medida que impone una injerencia en un derecho fundamental, como último requisito necesario para avalar la validez de la norma. Juicio que debe basarse en la superación de los siguientes tres requisitos: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)».

Con relación a la idoneidad de esta medida legal limitativa del derecho a la protección de datos hay que señalar que los datos que un responsable del tratamiento conserva sobre terceras personas que hayan sido previamente recopilados con alguna otra finalidad legítima, pueden resultar indudablemente útiles para la investigación y enjuiciamiento de hechos de índole criminal. La importante casuística a la que puede cooperar es imposible de recopilar, pero habida cuenta del importante número de datos personales que se recopilan hoy día en las más variadas bases de datos mantenidas en la práctica totalidad de sectores de la vida económica y social, puede advertirse su potencial y heterogéneo provecho para ser utilizados como fuentes de prueba de cargo o descargo. Ello resulta más evidente aun, de la tendencia legislativa expansiva por la que se ha obligado *ex lege* a la creación y mantenimiento de distintas bases de datos específicas para su uso en el ámbito penal, con fines preventorios o de enjuiciamiento. Las conclusiones del Consejo de Justicia e Interior de la UE de 19 de diciembre de 2002 dan buena muestra de ello al expresar que «(…) la conservación de datos se ha acreditado como una herramienta de investigación necesaria y eficaz para aplicar la ley en diferentes Estados miembros, en particular en asuntos de gravedad como la delincuencia organizada y el terrorismo, es necesario garantizar que los datos conservados se pongan a disposición de las fuerzas y cuerpos de seguridad durante un determinado período de tiempo». Mientras, la STJUE de 8 de abril de 2014 (asunto *Digital Rights Ireland*) ya advirtió, específicamente en relación a los datos de tráfico de las comunicaciones electrónicas, que «considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relacio-

93. Sentencias del Tribunal Europeo de Derechos Humanos, de 26 de marzo de 1985 (caso X e Y vs. Holanda); de 26 de marzo de 1987 (asunto Leander vs. Suecia); de 7 de julio de 1989 (asunto Gaskin vs. Reino Unido); de 25 de febrero de 1993 (asunto Funke vs. Francia); de 25 de febrero de 1997 (asunto Z. vs. Finlandia).

94. STC 292/2000, de 30 de noviembre (F. J. 11º).

95. STC 11/1981, de 8 de abril (F. J. 8º).

96. STJUE de 8 de abril de 2015 (asunto Digital Rights Ireland), apartado 40.

97. Véase al respecto los artículos 30 y siguientes de la Directiva 2016/680/UE.

nes sociales y los medios sociales que frecuentan»[98], aunque dichas manifestaciones podrían ser perfectamente extrapolables a datos personales de otra naturaleza. Por tanto, puede estimarse que la cesión de datos personales de terceros a un órgano judicial sin el consentimiento del interesado encuentra justificación en su condición de instrumento valioso para la lucha contra la delincuencia y para garantizar el derecho a la tutela judicial efectiva que encuentra justificación.

Datos personales que, en múltiples ocasiones, y cada vez en una proporción mayor, se muestran como únicas o principales fuentes probatorias para poder acreditar hechos y aspectos esenciales para el éxito de la incriminación o alternativamente para el descargo. Máxime si tenemos en cuenta el auge e incremento de las actividades delictivas que se llevan a cabo con apoyo en las tecnologías de la información y comunicación o en canales telemáticos, utilizando a estas algunos de ellos como medio para la impunidad. Es por ello por lo que la propia LECrim ha incorporado, a través de la reforma operada por la Ley Orgánica 13/2015, de 5 de octubre, todo un potente marco jurídico específico para la creación y configuración de varias medidas de investigación tecnológica que permitan abordar la instrucción de una importante cantidad de hechos delictivos que presenten al menos un componente tecnológico. Ello demuestra la necesariedad de disponer en el ordenamiento jurídico de medidas que faciliten y legitimen la entrega de datos personales por terceros, especialmente para aquellos supuestos en que el responsable se identifica con la víctima o la acusación o cuando no sea viable acudir a las precitadas medidas de investigación tecnológica.

Finalmente, cabe apuntar a la proporcionalidad en sentido estricto del art. 236 *ter* 3 de la LOPJ como medida limitativa del derecho a la protección de datos. La importancia de los bienes jurídicos colectivos e individuales que entran en liza con el derecho a la protección de datos es indudable. La seguridad de la comunidad, la lucha contra la criminalidad y el derecho a la tutela judicial efectiva representan algunos de los valores constitucionales más destacables y apreciados por en la sociedad. Cierto es que también el derecho a la protección de datos es un derecho que en pleno siglo XXI y en la era del *big data* alcanza una trascendencia inmensa; sin embargo, ante supuestos de criminalidad, debe ceder. Máxime cuando, como hemos tenido oportunidad de mencionar con anterioridad, existen diversas normas, sustantivas o procesales que establecen regímenes específicos para la cesión de los datos que puedan resultar más íntimos para las personas o que revelan información sobre los aspectos más reservados de los individuos. Por tanto, esas normas ya contemplan un régimen más riguroso, que establece límites y condicionantes específicos más restrictivos, medidas de seguridad específicas y garantías para el interesado[99]. Sin embargo, sin que se pueda descartar que ciertos datos que puedan ser entregados por terceros, también puedan integrarse en alguno de estos campos, lo cierto, es que, en cualquier caso, quedará la actuación judicial para evitar que se produzca una situación anómala y desproporcionada, a través de la ponderación caso a caso de los derechos confrontados, teniendo en consideración elementos como el particular contexto, las expectativas de privacidad y el respeto a los principios rectores del tratamiento de datos.

Por todo lo expuesto, parece posible colegir que la medida legal que habilita a la cesión, supera en abstracto, el canon de necesariedad y proporcionalidad exigido por el art. 5.4 del RGPD en relación con el 23, de acuerdo con los parámetros planteados en la CDFUE, el Convenio 108 y el Tribunal Constitucional. Debiendo, en definitiva, el órgano judicial competente examinar *ad casum* la proporcionalidad de cada comunicación de datos personales efectuada por un responsable distinto del interesado de la que tengan la condición de destinatarios. Únicamente de este modo podrá cohonestarse la eficacia del proceso penal con la salvaguarda del derecho a la protección de datos de carácter personal de los ciudadanos.

VII. BIBLIOGRAFÍA

Aneiros Pereira, «Las obligaciones de prevención del blanqueo de capitales a cargo de determinados profesionales: una fuente de información tributaria» en *Revista técnica tributaria*, núm. 91, 2010, págs. 25-66.

Aparicio Salom, «La calidad de los datos» en *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (Troncoso Reigada, Dir.), Civitas, Madrid, 2010, págs. 324-339.

98. STJUE 8 de abril de 2014 (asunto *Digital Rights Ireland*), apartado 27.

99. Se cumple con ello el margen de maniobra del Estado que, conforme a la jurisprudencia del TEDH, será menor cuando el derecho de la persona sea crucial para el efectivo disfrute de derechos íntimos o esenciales, *vid*. STEDH 27 de mayo de 2004 (asunto Connors *vs*. Reino Unido), apartado 82. Gómez Álvarez, «La cesión de datos de carácter personal al proceso penal. En especial los datos relativos a la salud» en *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios* (Colomer Hernández, Dir.), Aranzadi, Cizur Menor, 2017, pág. 632.

Colmenero Guerra, «La protección de datos en la Administración de Justicia» en *Publicaciones del Portal Iberoamericano de Ciencias Penales*, 2016.

Colomer Hernández, «Uso y cesión de datos de las comunicaciones electrónicas para investigar delitos tras la STJUE de 21 de diciembre de 2016» en *Estudios sobre Jurisprudencia Europea: materiales del I y II Encuentro anual del Centro español del European Law Institute (*Ruda González y Jerez Delgado, Coords.), Sepín, Las Rozas, 2018, págs. 767-781.

Murillo de la Cueva, «La protección de datos en la Administración de Justicia» en *Cuadernos de derecho judicial*, núm. 9, 2004, págs. 223-263.

Cabezudo Rodríguez, «Documentación judicial y protección de datos personales» en *La responsabilidad jurídica y social de los archiveros, bibliotecarios y documentalistas en la sociedad del conocimiento* (García Marco, Ed.), Prensas Universitarias Zaragoza, Zaragoza, 2008, pág. 109-132.

Cabezudo Rodríguez, «Datos personales e informaciones judiciales» en *Revista General de Derecho Procesal*, núm. 17, 2009, págs. 1-33.

Garberi Llobregat, «Artículo 118 CE: La obligación de cumplir las sentencias y demás resoluciones firmes de jueces y tribunales» en *Diario La Ley*, núm. 9365, 2019,

Gómez Álvarez, «La cesión de datos de carácter personal al proceso penal. En especial los datos relativos a la salud» en *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios* (Colomer Hernández, Dir.), Aranzadi, Cizur Menor, 2017, pág. 632.

Huerta Viesca, «Práctica y crítica de las obligaciones de las entidades de crédito respecto de sus clientes en prevención del blanqueo de capitales» en *Revista de derecho bancario y bursátil*, núm. 117, 2010, págs. 117-140.

López Calvo, *Algunas cuestiones relevantes en protección de datos de carácter personal en Tribunales y Fiscalía tras el Reglamento Europeo de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD)*, Sepín, Las Rozas, 2019.

Messía de la Cerda Ballesteros, «La evolución del concepto de cesión o comunicación de datos personales» en *Actualidad Civil*, núm. 10, 2017, págs. 1-20.

Montoro Sánchez, «El tratamiento de los datos de tráfico y localización con fines penales: estudio de la situación actual» en *Uso y cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios* (Colomer Hernández, Dir.), Aranzadi, Cizur Menor, 2019, págs. 371-424.

Palma Ortigosa, «Principios relativos al tratamiento de datos personales» en *Protección de datos, responsabilidad activa técnicas de garantía* (Murga Fernández, Fernández Scagliusi y Espejo Lerdo de Tejada, Dirs.), Reus, Madrid, 2018, págs. 39-49.

Pérez Gil, «Entre los hechos y la prueba: reflexiones acerca de la adquisición probatoria en el proceso penal» en *Revista Jurídica de Castilla y León*, núm. 14, 2018, págs. 223-248.

Pérez Gil, «Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal» en *Justicia* ¿Garantías *"versus" eficiencia?* (Jiménez Conde y Bellido Penadés, Dirs.), Tirant Lo Blanch, Valencia, 2019, págs. 399-441.

Pérez Gil y González López, «La incorporación de datos personales automatizados al proceso en la propuesta de Código Procesal Penal (1)» en *Diario La Ley*, núm. 8217, 2013.

Puyol Montero, «Los principios del derecho a la protección de datos» en *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad* (Piñar Mañas, Dir.), Reus, Madrid, 2016, pág. 140, págs. 135-150.

Rodríguez Lainz, «Sobre la previsible incidencia de la cuestión prejudicial C-207/16 en la definitiva defenestración del régimen legal español sobre conservación de datos relativos a las comunicaciones» en *Diario La Ley*, núm. 9273, 2018, pág. 4.

Troncoso Reigada, «El principio de calidad de los datos» en *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (Troncoso Reigada, Dir.), Civitas, Madrid, 2010, págs. 340-396.