Capítulo 1

Limitaciones en el uso de la información y los datos personales en un proceso penal digital

Ignacio Colomer Hernández

Catedrático de Derecho Procesal
Universidad Pablo de Olavide de Sevilla

I. DELIMITACIÓN DEL OBJETO DE ESTUDIO[1]

El proceso penal es, sin duda, una de las instituciones jurídicas que más capacidad de afectación de los derechos fundamentales tiene, toda vez que la clásica tensión entre libertad y seguridad encuentra en él un campo abonado para su desarrollo. Las investigaciones penales requieren en muchas ocasiones la adopción de medidas que afectan y restringen los derechos de las personas para la obtención de información, datos y evidencias que luego puedan ser utilizados en el juicio oral como pruebas de cargo o de descargo.

En este sentido, es posible constatar que el proceso penal se encuentra actualmente en un período de transición y cambio en el que se van incorporando las nuevas tecnologías de la Sociedad de la Información, lo que está produciendo una transformación hacia un proceso penal digital, o más precisamente, un cambio hacia un proceso penal en el que las principales de fuentes de prueba son digitales, por extraerse de la actividad digital que desarrollan los sujetos.

En España la reforma operada por la LO 43/2015 de reforma de la LECrim ha servido para introducir cambios en la instrucción de los delitos al prever nuevas medidas de investigación tecnológicas, que, no debe

1. Trabajo realizado en el seno del Proyecto PGC2018-095735-B-I00, financiado por FEDER/Ministerio de Ciencia e Innovación – Agencia Estatal de Investigación sobre "*Límites a la utilización de datos, evidencias e información entre procesos y procedimientos diversos en España y la Unión Europea*" (LUDEI).

perderse de vista, tienen una importante capacidad de obtener información y datos de los ciudadanos objeto de la investigación[2]. De manera que en la actualidad el acceso a la información y los datos personales[3] que se encuentran en formato digital se ha convertido en una "autopista" hacia una posible afectación de derechos fundamentales de las personas (tales como, la intimidad, el derecho al entorno virtual, el secreto de las comunicaciones, la protección de datos personales, etc.) en el seno de los procesos penales, bien a través de diligencias de investigación tecnológicas, bien a través de la aportación de esa información y esos datos personales por parte de personas particulares o empresas que los tienen o los poseen de forma legítima, cuando los hayan obtenido con el consentimiento de sus titulares, o de forma ilegítima, cuando los hayan conseguido al margen del consentimiento de sus titulares.

Por ello, en el presente trabajo se va a analizar, en primer lugar, la relación existente entre las nuevas tecnologías, los datos personales y la prueba penal. Para en un segundo momento, abordar el régimen jurídico que presenta la obtención de datos e información personal por parte de los particulares y por parte de las autoridades competentes para su uso como prueba en el proceso penal. Y, finalmente, estudiar la posible exclusión probatoria de la información y los datos personales que se hayan obtenido sin cumplir con las exigencias establecidas en la normativa de protección de datos personales para su uso en los procesos penales.

II. NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN, DATOS PERSONALES Y PRUEBA PENAL

En la era digital en la que vivimos existe un cúmulo de información y datos que se encuentran, se almacenan y se transmiten a través

2. En la actualidad el trabajo más completo sobre datos personales y proceso penal es el de MONTORO SÁNCHEZ, J. A., *Uso y cesión de datos de carácter personal en el proceso penal*, Aranzadi Thomson-Reuters, Cizur Menor, 2022, 528 pp.

3. Sobre la estrecha relación entre los datos, algoritmos y las nuevas tecnologías se puede ver, BARONA VILAR, S., *Algoritmización del derecho y de la justicia: De la inteligencia artificial a la Smart Justice*, Tirant lo Blanch, 2021; MARTÍN DIZ, F., "Inteligencia artificial y derecho procesal: luces, sombras y cábalas en clave de derechos fundamentales", en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M. A. (dir.), Tirant lo Blanch, Valencia, 2021, pp. 969-1006; COLOMER HERNÁNDEZ, I., "Control y límites en el uso de la información y los datos personales por parte de la Inteligencia Artificial en los procesos penales" en *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar*, Barona Vilar, S. (edit.), Tirant lo Blanch, 2021, pp. 287-308; HUERGO LORA, A. "Una aproximación a los algoritmos desde el Derecho Administrativo" en *La regulación de los algoritmos*, Dir. Huergo Lora, A., Thomson-Reuters Aranzadi, Cizur Menor, 2020.

de dispositivos e instrumentos digitales. Esta digitalización de la vida corriente ha traído unas mayores posibilidades para el acceso a la información y a los datos personales que se recogen en formato digital[4]. De hecho, es usual y ordinario que la información personal se pueda encontrar tanto en redes sociales, como en otros canales abiertos o incluso en canales cerrados dependientes de la voluntad de sujetos, lo que ha provocado que la información personal haya pasado a constituir una mercancía más, que se transmite de forma onerosa o gratuita, y que con suma frecuencia cambie de manos entre las personas y las empresas[5]. No hay duda que, esta facilidad en el acceso a la información y a los datos en formato electrónico, ha determinado que en la ciudadanía se haya generado una cierta consciencia acerca de una inexistente libertad en relación con la obtención, uso y tratamiento de los datos personales.

Esta percepción, acerca de que la existencia de un cierto acceso libre a la información y a los datos permite su uso sin limitaciones, ha calado no solo en la ciudadanía en general, sino también en los abogados que introducen informaciones y datos personales en los procesos sin observar las exigencias que conlleva la protección de datos personales. Y es que, en efecto, la aparente libertad en el acceso a la gran mayoría de la información y de los datos no se corresponde con los límites que para la obtención, tratamiento y cesión de los datos personales se han introducido en el ordenamiento de la Unión Europea y por ende en nuestro Derecho. Estos límites en el tratamiento y cesión de los datos personales han venido impuestos desde el reconocimiento y cristalización de un derecho fundamental, el derecho a la protección de datos personales, que no se

4. Como señala VELASCO NÚÑEZ en relación con los datos personales que se obtienen e incorporan al proceso penal a través de las nuevas tecnologías, "*los atestados policiales, informes, periciales y resto de diligencias de investigación que el Juez instructor incorpora al proceso penal, pueden exhibir excesiva información afectante no ya sólo al derecho fundamental a la protección del dato en sus diversas facetas, sino igualmente a otros recogidos también en el Art. 18 CE (como el de a la intimidad, propia imagen, secreto telecomunicativo, …) que requieren un tratamiento específico, muy cuidadoso, no sólo cualitativo –por las garantías que exige– sino también cuantitativo –por el exceso de información–, a veces muy estigmatizante, que puede conllevar*" (*cfr*. "Investigación penal y protección de datos" en *El Cronista del Estado Social y Democrático de Derecho*, n.º 88-89, 2020, p. 139).

5. Como señala PÉREZ GIL "*son estos, los datos electrónicos, los que han de constituir una nueva categoría en las normas procesales (el género) mientras que los que se generen a partir de comunicaciones serán una especie dentro de ellos, ciertamente con particularidades determinantes, pero al fin y al cabo una entre muchas. Identificado el problema, habrá que dársele respuesta en futuras reformas procesales: la singularidad de la regulación de esta materia debe venir por la atención al formato en el que se encuentra la información electrónica en forma de datos y la especificidad que de ello se deriva*" *Cfr*. "Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal" en *Justicia: ¿garantías versus eficiencia?*, Jiménez Conde, F. y Bellido Penadés, R. (dir.), Llopis Nadal, P. y De Luis García, E. (coord.), Tirant lo Blanch, Valencia, 2019, p. 423.

encontraba en el catálogo clásico de derechos y garantías de los ciudadanos integrados en el bloque esencial de la constitucionalidad.

En este sentido, hay que recordar que la Carta de Derechos Fundamentales de la Unión Europea ha supuesto el reconocimiento del derecho a la protección de datos como un derecho autónomo e independiente respecto al derecho a la vida privada y familiar. Su reconocimiento se realizó en el artículo 8 CDFUE[6] bajo la rúbrica "Protección de datos de carácter personal"[7]. En este artículo, junto al general reconocimiento del derecho a la protección de datos, se establecen en su número 2, de un lado, los principios básicos que deben regir el tratamiento de los datos personales, lealtad y limitación de la finalidad; y de otro lado, las bases que legitiman el tratamiento, que se concretan en el consentimiento del interesado, dejando abierta la posibilidad de que el legislador establezca otros fundamentos.

En 2016 se aprobó un importante paquete normativo para la protección y desarrollo del derecho a la protección de datos. De una parte, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE; y de otra parte, la Directiva (UE) 2016/680[8]

6. *"1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*

   2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

   3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

7. Para un análisis del contenido del artículo 8 CDFUE ver, entre otros, ÁVILA RODRÍGUEZ, C. M., "Artículo 8. Protección de datos de carácter personal" en *La Europa de los derechos: estudio sistemático de la Carta de los derechos fundamentales de la Unión Europea*, MONEREO ATIENZA, C. y MONEREO PÉREZ, J. L. (coords.), Comares, Granada, 2012, pp. 157-180; ABERASTURI GORRIÑO, U., "El derecho a la protección de datos de carácter personal. La autodeterminación informativa como derecho autónomo en la Carta de derechos fundamentales de la Unión Europea" en *La Carta de los Derechos Fundamental de la Unión Europea y su reflejo en el ordenamiento jurídico español*, Aranzadi Thomson-Reuters, Cizur Menor, 2014, pp. 161-176.

8. Un análisis general sobre el contenido de la Directiva se puede encontrar en GONZÁLEZ CANO, I., "Cesión y tratamiento de datos personales, Principio de Disponibilidad y cooperación judicial penal en la Unión Europea", en *Cesión de datos personales y evidencias entre procesos penales y procedimientos sancionadores o tributarios*, Colomer Hernández, I. (dir.), Oubiña Barbolla, S. y Catalina Benavente, M. A. (coord.), Thomson-Reuters Aranzadi, Cizur Menor, 2017, pp. 59-79; "Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la directiva (UE) 2016/680" en *Revista Brasileira de Direito Processual Penal*, núm. 3, 2019, pp. 1331-1384; "Garantías del investigado y acusado en orden a la obtención, cesión y tratamiento de datos personales en el proceso penal. A propósito de la Directiva (UE) 2016/680 y su impacto en materia de prueba penal" en González Cano (coord.) *Orden Europea*

del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo[9]; y la Directiva (UE) 2016/681 del Parlamento y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (Directiva PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave[10]. La Directiva (UE) 2016/680 ha sido traspuesta por la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

En el Derecho español el reconocimiento del derecho a la protección de datos personales como derecho fundamental apareció vinculado inicialmente a la previsión contenida en el artículo 18.4 de la Constitución, como derecho a la autodeterminación informativa[11]. Sin embargo, una

---

de Investigación y prueba transfronteriza en la Unión Europea, Tirant Lo Blanch, Valencia, 2019, pp. 98-154. También los trabajos de PILLADO GONZÁLEZ, E., "Principios generales de protección de datos en la cesión de información en la persecución criminal a la vista de la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por la que se deroga la Decisión Marco 2008/977" en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M. A. (dir.), Tirant lo Blanch, Valencia, 2021, pp. 783-820; "Difícil equilibrio entre seguridad y salvaguarda del derecho a la protección de datos personales en la prevención, investigación y represión de delitos en la unión europea" en *Integración europea y justicia penal*, González Cano (dir.), Tirant Lo Blanch, Valencia, 2018, pp. 515-559. COLOMER HERNÁNDEZ, I., "Control y límites en el uso de los datos personales penales en la investigación y represión de los delitos a la luz de la Directiva 2016/680" en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M. A. (dir.), Tirant lo Blanch, Valencia, 2021, pp. 737-782.

9. Para un análisis de los antecedentes de la Directiva se puede ver PÉREZ-LUÑO ROBLEDO, E., "La garantía procesal de los datos personales en la Carta de Niza como fundamento de la Directiva 2016/680 UE", en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M. A. (dir.), Tirant lo Blanch, Valencia, 2021, pp. 957-968; FIODOROVA, A., "Directiva 2016/680: hacia mayor coherencia de protección de datos personales en la cooperación policial y judicial penal" en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M. A. (dir.), Tirant lo Blanch, Valencia, 2021, pp. 709-736.
10. Sobre el uso de los PNR en los procesos penales, ver CATALINA BENAVENTE, M. A., *El uso de los datos PNR en el proceso penal*, Aranzadi Thomson-Reuters, Cizur Menor, 2022, 230 pp.
11. En la STC 254/1993, de 20 de julio se reconoce la existencia de un derecho fundamental de la persona a la autodeterminación informativa que encuentra su anclaje en el artículo 18.4 Constitución. En concreto, el Tribunal señala que: "*en el presente*

evolución en la doctrina del Tribunal Constitucional, muy en particular a partir de la importante STC 292/2000, llevó al reconocimiento del derecho a la protección de datos como derecho autónomo y diferenciado del derecho a la intimidad[12]. En palabras, del Tribunal Constitucional *"el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información"*[13].

El derecho a la protección de datos *"atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer"*.

En consecuencia, la esencia de este derecho a la protección de datos, a juicio del interprete constitucional, se concreta en *"que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos"*[14]. Y esta necesidad o no del consentimiento es un elemento esencial, como se analizará más tarde, para valorar la admisibilidad del uso y tratamiento de los datos personales en el proceso penal, en particular para su empleo como prueba o evidencia de los hechos controvertidos.

Por último, es necesario también poner de relieve el carácter limitado del derecho a la protección de datos, puesto que, como ha señalado el Tribunal Constitucional, *"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,*

---

caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'" (FJ 6.º).

12. El derecho a la protección de datos "*atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer"* (STC 292/2000, de 30 noviembre. FJ 6.º).
13. STC 292/2000, de 30 noviembre. FJ 6.º.
14. En igual sentido, ya se había indicado en la STC 254/1993, identificándolo con el poder de disposición sobre los datos personales.

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)"[15].

El reconocimiento de la naturaleza limitada de este derecho, que por otra parte no constituye algo extraordinario en la configuración constitucional de los derechos fundamentales, ha sido, sin embargo, usado por el CGPJ, más concretamente por el órgano del mismo encargado de la protección de datos en el ámbito jurisdiccional[16], para precisamente adoptar resoluciones en las que el derecho a la protección de datos[17] se ha contrapuesto con el derecho a la tutela judicial efectiva, con la indeseable consecuencia de privar de eficacia en el ámbito jurisdiccional a la protección de datos[18]. Sin embargo, no se puede compartir la argumentación que se realiza en la Resolución, sobre la base del carácter limitado del derecho a la protección de datos, para confrontarlo con el derecho a la tutela judicial efectiva y extraer como consecuencia la consideración de que en el seno de los procesos la protección de datos deba ceder ante el derecho a la tutela judicial efectiva. Dicho, en otros términos, esta Resolución es una muestra clara de una confusión en cuanto a las dimensiones que concurren en esta cuestión. Pues, de lo que se trata, no es que el derecho a la tutela judicial efectiva sea un límite del derecho a la protección datos y éste deba ceder por ello, sino que la efectividad del derecho a la tutela judicial ha de contemplar necesariamente las consecuencias procesales del derecho a la protección de datos personales.

Esta posición es criticable[19] pues no se trata de contraponer protección de datos y derecho a la tutela judicial efectiva, sino que lo que debe

15. STC 292/2000, de 30 noviembre. FJ 11.º.

16. La Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial.

17. Ver, sobre la protección de datos en los tribunales, PÉREZ ESTRADA, M. J. "La protección de los datos personales en los órganos judiciales" en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M. A. (dir.), Tirant lo Blanch, Valencia, 2021, pp. 895-916.

18. En concreto, la Resolución de 13 de septiembre de 2021 de la Dirección de Supervisión y Control de Protección de Datos del CGPJ señala que "*no puede existir vulneración de la normativa de protección de datos cuando, como en este caso, los términos concretos en que pueda verse afectado el derecho a la protección de datos personales resultan de la ponderación de los derechos y bienes jurídicos constitucionalmente protegidos concurrentes, realizada en el seno de un procedimiento judicial, en la que, al cabo, se otorga prevalencia al otro derecho fundamental presente. En este caso, es el derecho de tutela judicial efectiva sin que pueda producirse indefensión (artículo 24.1 CE) el que, concurriendo con el de protección de datos personales (artículo 18.4 C.E.), actuaría precisamente como límite de este último*".

19. Sin perjuicio de que la Resolución acierta en cuanto a la falta de competencia de la Dirección de Supervisión y Control de Protección de Datos para conocer de cuestiones relativas a la valoración probatoria que el órgano jurisdiccional deba realizar, por

realizarse es una interpretación conjunta e integradora de ambos derechos. De manera que las posibles vulneraciones del derecho a la protección de datos que se cometan en la obtención y tratamiento de datos personales, que vayan a ser usados como fuentes de prueba en un proceso, tenga su plasmación y consecuencia en la actividad jurisdiccional desarrollada, y más concretamente en la valoración probatoria que puedan recibir esos datos personales como pruebas.

Por todo lo cual, es necesario tener presente que el derecho a la protección de datos personales no sólo se circunscribe a ese poder de disposición de las personas sobre sus datos, que el Tribunal Constitucional reconoce desde la STC 292/2000, sino que despliega también sus efectos en el ejercicio de la potestad jurisdiccional en la actividad de valoración de la prueba.

La trascendencia de esta contraposición entre una libertad absoluta de uso de los datos y la información y una libertad condicionada por las exigencias previstas para la licitud del tratamiento de los mismos, se manifiestan en el seno de los procesos desde el punto de vista de la prueba, o más específicamente, desde la óptica de la valoración de los materiales probatorios que tengan acceso al proceso. Y es que no se debe perder de vista que los datos personales son, desde el punto de vista del proceso, una fuente de prueba[20], por cuanto representan la realidad de unos hechos que habrán de tener acceso al proceso a través de distintos medios prueba (la documental, medios de archivo de la palabra o las imágenes, etc.).

Por tanto, se constata la relación existente entre el proceso y el derecho a la protección de datos, reconociendo que este último puede condicionar

---

ser una manifestación estricta de la potestad jurisdiccional, que en caso de ser desarrollada por terceros supondría una clara inmisión en la independencia del órgano jurisdiccional, ya que como indica la Resolución "*no resulta ocioso recordar que, por imperativo del principio de independencia en el ejercicio de potestad jurisdiccional consagrado en el artículo 117 CE, el Consejo General del Poder Judicial no puede pronunciarse en modo alguno respecto del contenido y alcance de las resoluciones adoptadas en un procedimiento judicial por el órgano competente en ejercicio de la función jurisdiccional. Cualquier posible intervención del Consejo General del Poder Judicial en tal ámbito supondría una intromisión en el ejercicio de dicha función que contravendría la prohibición expresamente contenida en el artículo 12.3 de la Ley Orgánica del Poder Judicial*".

20. MONTORO SÁNCHEZ distingue claramente la finalidad identificativa y la finalidad probatoria de los datos personales. Así respecto de la función identificativa señala que "*en primera instancia, los datos personales cumplen la labor de identificar de forma directa o indirecta a todo individuo vinculado o que deba vincularse o intervenir de algún modo en el proceso*"; y respecto de la función probatoria, que es la que a nosotros interesa en el presente trabajo, indica que "*los datos personales también pueden ser utilizados en el proceso con fines probatorios cuando se introduzcan en el proceso como fuente de prueba*" (*cfr. Uso y cesión de datos de carácter personal en el proceso penal*, Aranzadi Thomson-Reuters, Cizur Menor, 2022, p. 289).

la actividad judicial de valoración de prueba. De ahí que sea necesario para un análisis en profundidad de este condicionamiento que, como se verá a continuación, se desarrolla en el momento de la admisión y valoración de la prueba, proceder a realizar una serie de consideraciones en relación con las condiciones que deben cumplirse en la obtención y tratamiento de los datos personales para que puedan servir como fuente de prueba en el proceso penal.

III. TRATAMIENTO DE DATOS PERSONALES EN EL PROCESO PENAL

El punto de partida, desde el que hay que iniciar el análisis del tratamiento de los datos personales como fuente de prueba en el proceso penal, pasa necesariamente por tener en cuenta el diverso régimen jurídico que tiene el tratamiento de los datos según que sea realizado por autoridades o por los particulares en relación con un concreto proceso o investigación penal. Y es que necesariamente hay que tener en cuenta que el tratamiento por parte de las autoridades competentes con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales se encuentra regulado en la Directiva (UE) 2016/680 y en la LO 7/2021. Mientras que, por el contrario, el tratamiento realizado por los particulares (el acusador particular, el investigado, la víctima, etc.) se encuentra sometido a las previsiones del Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Esta diversidad en el régimen jurídico aplicable al tratamiento de los datos personales que vayan a poder aportarse al proceso penal como fuentes de prueba[21] tiene evidentes consecuencias que afectan a su admisibilidad y a su posible exclusión al amparo de la previsión contenida en el artículo 11 LOPJ por haber sido obtenidos con vulneración de derecho fundamental a la protección de datos. Por ello, en las próximas páginas se van a delimitar las exigencias y requisitos que vienen impuestos por la normativa protectora del derecho a la protección de datos personales para su uso en el seno de los procesos penales.

21. "*Entendemos, además, que el dato personal, por su incorporación a un proceso de esa naturaleza, tan estigmatizante –protección por destino–, es de los calificados como de categoría, y, en consecuencia, protección 'especial' (Arts. 9 y 10 RGPD), lo que implica que sólo se puede recoger e incorporar (y valorar) para el fin del propio proceso penal (Art. 4.1 b) 2016/680 de Tratamiento con fines de investigación penal), debiendo asegurarse que su aportación garantiza que no se use para otro destino que el probatorio*" (*cfr*. VELASCO NÚÑEZ, *op. cit.*, p. 140).

1. TRATAMIENTO DE LOS DATOS PERSONALES CON FINES PENALES POR PARTE DE LAS AUTORIDADES COMPETENTES

La posibilidad de tratamiento de datos personales con fines penales por parte de las autoridades competentes se encuentra específicamente regulada en la Directiva (UE) 2016/680 y en la LO 7/2021 de trasposición de la norma europea. En concreto, en el artículo 1 de la Ley Orgánica expresamente se identifica como objeto de la norma la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública. De manera que en la Ley se regulan los requisitos, límites y condiciones existentes para que las autoridades competentes puedan proceder al tratamiento de los datos personales de personas, vinculadas o no con el proceso, con la finalidad de prevenir, detectar, investigar o enjuiciar delitos.

Lo primero que hay que tener claro es el concepto de autoridades competentes para el tratamiento de los datos personales con fines penales. Al respecto, la normativa vigente considera que tendrán la consideración de autoridades competentes a estos efectos toda autoridad pública que tenga competencias encomendadas legalmente para el tratamiento de datos personales con fin de prevenir, detectar, investigar o enjuiciar delitos (artículo 4.1 LO 7/2021)[22]. Mientras que en el artículo 4.2 se reconoce la habilitación como autoridades competentes para el tratamiento de datos personales con relevancia penal a las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal[23].

Este listado de autoridades competentes ha sido recientemente ampliado por la Ley Orgánica 9/2022, de 28 de julio, por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales, de modificación de la Ley Orgánica 8/1980, de 22

22. El propio apartado 1 del precepto detalla esa mención genérica a las autoridades públicas considerando que se incluyen dentro de ese concepto *"a) Las Fuerzas y Cuerpos de Seguridad. b) Las Administraciones Penitenciarias. c) La Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria. d) El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias. e) La Comisión de Vigilancia de Actividades de Financiación del Terrorismo"*.

23. Esta distinción entre los dos apartados del precepto tiene su relevancia, ya que se conecta, como luego se verá, con el distinto régimen jurídico que se aplica al tratamiento de datos por parte de jueces y fiscales (artículo 26 LO 7/2021), respecto del tratamiento de las demás autoridades competentes.

de septiembre, de Financiación de las Comunidades Autónomas y otras disposiciones conexas y de modificación de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

En concreto, la LO 9/2022 ha introducido como autoridades competentes a la Fiscalía Europea en el ámbito de sus competencias; a las Policías Autonómicas con competencias estatutariamente asumidas en la investigación de delitos graves; y a la Oficina de Recuperación y Gestión de Activos del Ministerio de Justicia y las oficinas de recuperación de activos designadas por España de conformidad con la Decisión 2007/845/JAI, de 6 de diciembre de 2007[24].

En segundo lugar, hay que determinar qué significado tiene el concepto de tratamiento de datos personales en el seno de actuaciones o actividades de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales[25]. A estos efectos, la propia LO 7/2021 recoge el amplio concepto de tratamiento que se maneja en la Directiva (UE) 2016/680 cuando señala que ha de entenderse por tratamiento "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*" (artículo 5 b LO 7/2021). De manera que, por tanto, la recogida, obtención, uso o cesión de datos personales[26] en el seno de las investigaciones policiales y judiciales son

24. De manera que como autoridades competentes quedan habilitadas, de una parte, para acceder y consultar el Fichero de Titularidades Financieras, en el ejercicio de sus respectivas competencias para la prevención, detección, investigación o enjuiciamiento de infracciones penales graves delitos graves (artículo 3.1 LO 9/2022); y de otra parte, para solicitar y recibir información financiera o análisis financieros del Servicio Ejecutivo de la Comisión, en el ejercicio de sus respectivas competencias para la prevención, detección, investigación o enjuiciamiento de infracciones penales graves (artículo 3.2).

25. Una aproximación a esas finalidades del tratamiento de datos con relevancia penal se puede ver en VILLAR FUENTES, I., "Datos personales al servicio de la investigación y detección de infracciones penales" en *Revista General de Derecho Procesal*, n.º 48 (2019), 41 pp.

26. La LO 7/2021 define los datos personales como "*toda información sobre una persona física identificada o identificable ('el interesado'); se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*" (artículo 5.a). De lo que se desprende que en la mayor parte de los casos el resultado de las diligencias de investigación de los procedimientos penales podrá tener la consideración

manifestaciones claras de un tratamiento de datos por parte de las autoridades competentes que deberá estar sometido a las exigencias y requisitos establecidos en la LO 7/2021 y en la Directiva (UE) 2016/680.

La tercera de las cuestiones que hay que abordar es identificar las exigencias necesarias para que las autoridades competentes puedan realizar un tratamiento lícito de los datos personales en el seno de las actuaciones de prevención, detección, investigación y enjuiciamiento de delitos. Al respecto, el artículo 11 LO 7/2021 establece de forma taxativa que sólo será lícito el tratamiento en la medida en que sea necesario para los fines señalados en el artículo 1 y se realice por una autoridad competente en ejercicio de sus funciones. Lo que supone que la licitud del tratamiento de los datos personales con relevancia penal viene determinada, de una parte, por las finalidades que se persigan con su obtención y tratamiento (artículo 6.1 b LO 7/2021); y, de otra parte, por estar realizado por autoridades competentes.

Por lo que se refiere a la finalidad que habilita el tratamiento de datos personales con relevancia penal hay que tener presente que los fines previstos en la norma se concretan en la prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública. Esta identificación genérica contenida en el artículo 1 LO 7/2021 debe ser concretada con la referencia a los principios básicos que rigen el tratamiento de los datos personales[27] con relevancia penal. En particular, según lo dispuesto en el artículo 6 LO 7/2021, que concreta el alcance del principio de finalidad de los datos personales, se pueden distinguir dos dimensiones: (i) Finalidad en la recogida de los datos; (ii) Finalidad en el tratamiento.

En primer lugar, la recogida y obtención de los datos personales debe realizarse con "*fines determinados, explícitos y legítimos*" (artículo 6.1.b LO 7/2021). De manera que en el seno de las investigaciones criminales la recogida y obtención de los datos debe tener lugar para un fin determinado, que resulte claramente explicitado en la actuación que se lleve a cabo, en particular cuando la diligencia de investigación mediante la que se obtengan los datos personales afecte o limite derechos fundamentales,

---

de datos personales, lo que obliga a que en su obtención se hayan respetado las garantías de la protección de datos para su posterior uso en el proceso penal como prueba de cargo o de descargo.

27. En esta materia se puede ver RODRÍGUEZ AYUSO, J. F., "Principios rectores en materia de protección de datos personales" en *Nuevos postulados de la cooperación judicial en la Unión Europea*, Moreno Catena, V. y Romero Pradas, M. A. (dir.), Tirant lo Blanch, Valencia, 2021, pp. 945-956.

y que además resulte legítimo por servir a la finalidad de prevenir, investigar o enjuiciar conductas delictivas.

Con relación a la determinación del fin que motiva la obtención o la recogida de los datos personales es necesario establecer una correspondencia con los principios rectores que presiden la adopción de diligencias de investigación tecnológica mediante autorización jurisdiccional[28], tal como expresamente prevé el artículo 588 bis a) LECrim[29]. En concreto, la necesidad de determinación se encuentra directamente imbricada con el principio de especialidad que debe regir en la adopción de las diligencias de investigación tecnológica[30]. De manera que, si la especialidad exige que una medida de investigación tecnológica esté relacionada con la investigación de un delito concreto, la recogida y la obtención de los datos personales que se consigan en el desarrollo de esa medida de investigación habrá de haber sido realizado de conformidad con un fin determinado y explícito que se concretará en la investigación del delito concreto que esté siendo objeto de la diligencia de investigación. Y, por tanto, la alteración de los hechos que estén siendo objeto de investigación mediante la medida tecnológica supondrá un cambio en la concreta finalidad que habilita la obtención de los datos personales que consecuentemente podrá provocar la falta de licitud de esa recogida, y de su tratamiento ulterior, siempre que ese cambio en el concreto fin no se corresponda con algún caso de descubrimiento casual[31].

Dicho, en otros términos, el fin determinado que habilita la recogida de datos personales en el seno de una investigación tecnológica queda circunscrito a los hechos delictivos que sean objeto de la investigación, sin

28. Sobre el principio de proporcionalidad en relación con la obtención y cesión de datos personales en el proceso penal, ver LARO GONZÁLEZ, E., "Principio de proporcionalidad en la obtención, cesión y tratamiento de datos personales en materia penal" en *Exclusiones probatorias en el entorno de la investigación y prueba electrónica*, González Granda, P. (dir.), Ariza Colmenarejo, M. J. (coord.), Sanjurjo Ríos, E. (coord.), Reus, 2020, pp. 161-174.

29. "*Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida*".

30. Artículo 588 bis a) LECrim "*2. El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva*".

31. Artículo 588 bis i) LECrim. Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales. "*El uso de las informaciones obtenidas en un procedimiento distinto y los descubrimientos casuales se regularán con arreglo a lo dispuesto en el artículo 579 bis*".

perjuicio de la calificación jurídico penal que puedan revestir[32]. En consecuencia, la habilitación para la recogida de los datos no puede extenderse para hechos diversos de los contemplados en la autorización de la medida tecnológica sin que se produzca un supuesto de descubrimiento casual que, reunidas las exigencias previstas en el artículo 579 bis LECrim[33], podrá, en su caso, permitir que se habilite la recogida de datos mediante la continuación de la medida de investigación tecnológica en relación con los nuevos hechos descubiertos.

En segundo lugar, por lo que se refiere al principio de finalidad en relación con el tratamiento de los datos personales, esto es, para el tratamiento de los datos obtenidos en el desarrollo de una investigación a través de alguna medida tecnológica, se constata también que los fines que habilitan a las autoridades competentes para el tratamiento son los generales previstos en el artículo 1 LO 7/2021, es decir, aquellos incluidos en la finalidad de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales. De manera que, los datos personales obtenidos mediante medidas tecnológicas podrán ser usados para la investigación y el enjuiciamiento de los delitos por parte de las autoridades competentes constituyendo un tratamiento lícito que será acorde con la protección de los datos personales de las personas afectadas, sean partes en el proceso penal o terceros ajenos al mismo[34].

32. El fin que habilita la recogida u obtención de los datos personales por parte de la autoridad competente es la investigación de unos concretos hechos delictivos, con independencia de las posibles modificaciones en la calificación jurídico penal de los mismos que puedan sufrir a lo largo del procedimiento. De modo que, si la medida de investigación a través de la que se recabaron los datos personales estaba dirigida al esclarecimiento de una muerte, la obtención de los datos estará habilitada y será lícita con independencia de que en el curso de la instrucción los hechos delictivos pasen a ser calificados como asesinato cuando inicialmente lo hubieran sido como homicidio. De manera que lo esencial para la lícita obtención de los datos personales a través de cualquier diligencia de investigación, en particular en las que se producen a través de medidas tecnológicas, es que se produzcan en relación con unos concretos hechos delictivos y nunca en investigaciones prospectivas.

33. "*3. La continuación de esta medida para la investigación del delito casualmente descubierto requiere autorización del juez competente, para la cual, éste comprobará la diligencia de la actuación, evaluando el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento. Asimismo, se informará si las diligencias continúan declaradas secretas, a los efectos de que tal declaración sea respetada en el otro proceso penal, comunicando el momento en el que dicho secreto se alce".*

34. Sobre el tratamiento de los datos personales de terceros en el proceso penal ver DE LEMUS VARA, F. J., "Límites para el tratamiento de los datos de los no investigados en el proceso penal" en *Uso de la información y de los datos personales en los procesos: los cambios en la Era Digital*, Colomer Hernández, I. (dir.), Catalina Benavente, M. A. y Oubiña Barbolla, S. (coord.), Aranzadi Thomson-Reuters, Cizur Menor, 2022, pp. 545-570.

Ahora bien, en relación con los fines que habilitan el tratamiento lícito de los datos personales, tanto la Directiva (EU) 2016/680 como la LO 7/2021, contemplan la posibilidad de que se produzca algún cambio o modificación en los fines para los que son tratados los datos y para ello establecen un régimen diferenciado según que la modificación de la finalidad sea respecto a fines de naturaleza penal o no. Es necesario distinguir, por tanto, dos posibilidades en relación con los eventuales cambios en la finalidad del tratamiento de datos personales: de un lado, los casos en los que la nueva finalidad resulte ajena a los fines penales previstos en el artículo 1 LO 7/2021; y de otro lado, los supuestos en los que se produzca un cambio en la concreta finalidad de naturaleza penal habitante del tratamiento, pero manteniéndose dentro de alguno de los fines previstos en el indicado precepto.

El primero de los supuestos, los cambios en la finalidad para la que habrán de ser tratados los datos personales que hayan sido recogidos u obtenidos por una autoridad competente bajo la habilitación de un fin penal, como por ejemplo la investigación de un delito, se encuentra regulado en el artículo 6.2 LO 7/2021. Al respecto, el precepto establece una clara proscripción para que los datos personales recogidos por las autoridades competentes no sean tratados para otros fines distintos de los establecidos en el artículo 1, salvo que dicho tratamiento esté autorizado por el Derecho de la Unión Europea o por la legislación española. Lo que supone que los datos personales que hayan sido recogidos al amparo de la habilitación penal, como esencialmente puede ser la investigación de un delito a través de una medida tecnológica, solo podrán ser tratados o usados para una finalidad ajena al fin penal cuando esté autorizado por una norma del Derecho de la Unión Europea o por la legislación europea. Es decir, los datos personales obtenidos al amparo de una finalidad penal solo podrán dedicarse a una finalidad no penal cuando exista habilitación expresa de una norma de la UE o española.

La trascendencia de este límite en relación con el tratamiento de datos personales obtenidos en la investigación de delitos es de suma relevancia, ya que los datos obtenidos en el desarrollo de una medida de investigación tecnológica no podrán ser tratados para fines no penales, como por ejemplo su uso en un proceso civil, sin que exista esa habilitación legal que lo autorice. Pero, aún más, el propio artículo 6.2 LO 7/2021 no solo requiere esa expresa autorización, sino que en los casos en que exista la habilitación legal para el tratamiento para fines no penales se aplicará el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre. De modo que el tratamiento para fines no penales de datos personales obtenidos bajo la habilitación de un fin penal estará sometido

a las exigencias generales de la protección de datos, lo que supone que, como regla general, la licitud del tratamiento vendrá condicionada al consentimiento del titular de los datos[35].

Un segundo grupo de casos está constituido por aquellos en los que el fin penal habilitante del tratamiento de los datos sea distinto de aquel que permitió su recopilación y obtención. Al respecto, el artículo 6.3 LO 7/2021 prevé que *"los datos personales podrán ser tratados por el mismo responsable o por otro, para fines establecidos en el artículo 1 distintos de aquel para el que hayan sido recogidos, en la medida en que concurran cumulativamente las dos circunstancias siguientes: a) Que el responsable del tratamiento sea competente para tratar los datos para ese otro fin, de acuerdo con el Derecho de la Unión Europea o la legislación española. b) Que el tratamiento sea necesario y proporcionado para la consecución de ese otro fin, de acuerdo con el Derecho de la Unión Europea o la legislación española"*.

Ambas exigencias deben concurrir simultáneamente, de manera que el fin penal distinto del que inicialmente permitió el tratamiento de los datos solo podrá ser desarrollado por alguna autoridad competente responsable del nuevo tratamiento cuando éste sea necesario y proporcionado para la consecución de ese nuevo fin.

En consecuencia, en la práctica esta posibilidad de cambio en el fin penal habilitante del tratamiento de los datos se produce en dos supuestos: de un lado, en los casos de hallazgos casuales en el curso de diligencias de investigación, en particular en las que se desarrollan a través de medidas tecnológicas (artículo 579 bis y 588 bis i LECrim); y de otro lado, los casos de uso en un procedimiento distinto de los datos personales obtenidos en el seno de una investigación criminal (artículo 588 bis i LECrim).

En los supuestos en que se produzca un hallazgo casual en el seno de la práctica de unas medidas tecnológicas de investigación las exigencias de necesidad y proporcionalidad, que impone el artículo 6.3 LO 7/2021 para un tratamiento de los datos con un fin penal distinto, se han de concretar en los requisitos que el artículo 579 bis LECrim establece. De manera

35. Imaginemos que en el curso de una investigación por un delito grave se procede al registro de un ordenador, obteniéndose datos de naturaleza financiera del investigado, que no olvidemos son datos personales recogidos con un fin penal de investigación de un delito, pero que posteriormente el acusador particular pretenda usarlos en un proceso civil ajeno a la responsabilidad civil *ex delicto*, lo que supondría un uso para fin no penal, que debería estar autorizado por una ley, y que en todo caso estaría sometida al Reglamento General de Protección de datos y a la LO 3/2018, lo que exigirá, para la licitud de ese tratamiento para fines no penales, que ese uso y tratamiento para un fin no penal sea consentido por el titular de los datos (artículo 6.1.1 RGDP).

que, para el tratamiento de los datos personales hallados casualmente se requiere que el juez de instrucción proceda a verificar la legitimidad de la injerencia[36] que ha permitido llevar a cabo la medida de investigación restrictiva de los derechos fundamentales en la que se ha obtenido casualmente la información personal que se va a tratar, esto es, que se va a usar en la investigación o enjuiciamiento de un delito distinto[37].

Para los casos en los que los datos personales obtenidos en una investigación de un concreto delito se vayan a usar/tratar en otro procedimiento distinto resulta claro que las dos exigencias de necesidad y proporcionalidad del nuevo tratamiento sólo podrán concurrir si el nuevo procedimiento es de naturaleza penal. Ello significa, por tanto, que el cambio de la concreta finalidad que permita el tratamiento lícito de esos datos solo podrá justificarse si su cesión se produce a otro proceso penal, y no en cambio si se usan en un proceso de otra naturaleza[38].

Por otra parte, buena prueba de la transcendencia que tiene el principio de limitación de la finalidad en el tratamiento de los datos personales en el seno de los proceso la podemos encontrar en el hecho de que el Reglamento (UE) 1783/2020 del Parlamento Europeo y del Consejo de 25 de noviembre de 2020 relativo a la cooperación entre los órganos jurisdiccionales de los Estados miembros en el ámbito de la obtención de pruebas en materia civil o mercantil (obtención de pruebas), que ha entrado en vigor muy recientemente, recoja expresamente el principio de finalidad

36. Artículo 579 bis LECrim "*2. A tal efecto, se procederá a la deducción de testimonio de los particulares necesarios para acreditar la legitimidad de la injerencia. Se incluirán entre los antecedentes indispensables, en todo caso, la solicitud inicial para la adopción, la resolución judicial que la acuerda y todas las peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen*".

37. Sobre el tratamiento de los hallazgos casuales resulta interesante la Sentencia del Tribunal Supremo (Sala Tercera) 3162/2022 de 26 de julio cuando indica que "*la Administración tributaria no puede realizar válidamente comprobaciones, determinar liquidación eso imponer sanciones a un obligado tributario tomando como fundamento fáctico de la obligación fiscal supuestamente incumplida los documentos o pruebas incautados como consecuencia de un registro practicado en el domicilio de terceros (aunque se haya autorizado la entrada y registro por el juez de esta jurisdicción), cuando tales documentos fueron considerados nulos en sentencia penal firme, por estar incursos en vulneración de derechos fundamentales en su obtención. Aun cuando tal declaración penal no se hubiera llevado a cabo formalmente, la nulidad procedería delo establecido en el art. 11 LOPJ, conforme al cual 'no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales'*".

38. Hay que tener en cuenta que esos datos personales obtenidos por una autoridad competente en el seno de una investigación penal, particularmente si se han obtenido a través de medidas que limiten derechos fundamentales, no pueden ser cedidos para ser usados en otros procedimientos de naturaleza no penal si no es de acuerdo a las exigencias que marca con carácter general el Reglamento (UE) 2016/679 y que se concretan en la necesidad de contar con el consentimiento del titular de los datos.

en cuanto a los datos y la información personal que se hayan podido recopilar en la actividad de obtención de pruebas en el seno de la cooperación entre órganos jurisdiccionales de los Estado miembros de la UE.

En el artículo 30 del Reglamento (UE) 1783/2020, con una rúbrica muy ilustrativa de su contenido "*Protección de la información transmitida*", expresamente se exige que todo tratamiento de datos personales realizado al amparo del Reglamento de obtención de pruebas en materia civil o mercantil, incluidos el intercambio o la transmisión de datos personales por las autoridades competentes, deberá ser conforme al Reglamento (UE) 679/2016. Lo que implica una clara declaración de principios conforme a la cuál la obtención de pruebas en el seno de la cooperación jurisdiccional entre Estados miembros de la UE tiene que respetar, en todo caso, las exigencias del derecho a la protección de datos, tal y como se prevé en el RGPD.

En concreto, en aplicación de la necesaria protección de datos en esta actividad de obtención de prueba expresamente se prevé que *"los datos personales que no sean pertinentes para la tramitación de un caso específico se eliminarán inmediatamente"* (artículo 30.1). De forma que, como regla general, no resulta aceptable la conservación de datos o informaciones personales que se hayan podido recopilar en una actividad de obtención de prueba transfronteriza que no sean pertinentes para el desarrollo del concreto y específico caso para el que se hayan obtenido, debiendo ser eliminados de inmediato. Esta clara e inequívoca prescripción que impone el legislador europeo resulta extremadamente importante, puesto que supone que la obtención de pruebas, en el caso de la norma cuando la obtención tenga lugar de forma transfronteriza, está limitada y condicionada por el concreto objeto, esto es por el caso, que se esté ventilando o se pueda tramitar ante los tribunales civiles o mercantiles.

Dicho de otro modo, los datos personales y la información personal que pueda obtenerse en la recopilación llevada a cabo en la obtención de la prueba transfronteriza sólo podrá ser usada en el concreto pleito y asunto para el que se haya recopilado, sin que pueda ser conservada o usada en casos diversos de aquel que sea objeto del procedimiento en el que se hayan obtenido. Hay que tener presente que se ordena la eliminación de todos aquellos datos personales obtenidos en la diligencia transfronteriza de cooperación jurisdiccional que no resulten pertinentes para la tramitación del caso específico, lo que significa que no estén vinculados con el concreto objeto de ese procedimiento.

Además de esa vinculación de la recopilación y tratamiento de los datos personales como fuentes de prueba con el específico caso para el que se obtengan, el propio Reglamento recoge expresamente la vigencia

del principio de limitación de la finalidad para esta clase de tratamientos. Puesto que en el número 3 del artículo 30 establece que *"la información transmitida en el marco del presente Reglamento será utilizada por el órgano jurisdiccional requerido solo para los fines para los que se transmitió"*. Lo que quiere decir que el órgano jurisdiccional requerido, esto es, el de Estado en el que se va a obtener la prueba, no podrá disponer del resultado de la misma, es decir, de los datos personales o la información personal obtenida para cualquier otra finalidad que no sea su transmisión al órgano jurisdiccional requirente, que lo usará, como se ha señalado anteriormente, exclusivamente en relación con el caso específico para el que se le haya transmitido.

Al tiempo, los órganos jurisdiccionales requeridos, de acuerdo con su derecho nacional, garantizarán la confidencialidad de la mencionada información. De modo que no solo habrán de limitar el tratamiento a la finalidad para la que se obtuvieron los datos, esto es, para su transmisión al órgano jurisdiccional requirente, sino que además deberán de garantizar la confidencialidad de esa información obtenida y transmitida a un tribunal de otro Estado miembro de la UE.

Por último, hay que destacar la consolidada doctrina del Tribunal de Justicia de la Unión Europea que en reiteradas ocasiones ha venido estableciendo límites al acceso por parte de las autoridades competentes a los datos de tráfico de las comunicaciones electrónicas de los ciudadanos. Así, por ejemplo, en la reciente Sentencia del Tribunal de Justicia (Gran Sala) de 20 de septiembre de 2022 (peticiones de decisión prejudicial planteadas por el Bundesverwaltungsgericht – Alemania) – Bundesrepublik Deutschland/SpaceNet AG (C-793/19), Telekom Deutschland GmbH (C-794/19), se ha establecido que *"el artículo 15, apartado 1, de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, en relación con los artículos 7, 8, 11 y el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que se opone a medidas legislativas nacionales que establezcan, con carácter preventivo, a efectos de la lucha contra la delincuencia grave y la prevención de amenazas graves contra la seguridad pública, una conservación generalizada e indiferenciada de los datos de tráfico y de localización"*.

De manera que el TJUE admite a efectos de la lucha contra la delincuencia grave[39] que en las legislaciones nacionales se puedan implementar

39. Nótese que la Sentencia acepta que se puedan adoptar esas medidas en la lucha contra la delincuencia grave, pero también prevé que en relación con la lucha contra la

medidas de: (i) conservación selectiva de los datos de tráfico y de localización que esté delimitada, sobre la base de elementos objetivos y no discriminatorios, en función de las categorías de personas afectadas o mediante un criterio geográfico, para un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse; (ii) conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión, para un período temporalmente limitado a lo estrictamente necesario; (iii) requerimiento a efectuar a los proveedores de servicios de comunicaciones electrónicas, mediante una decisión de la autoridad competente sujeta a un control jurisdiccional efectivo, para que procedan, durante un período determinado, a la conservación rápida de los datos de tráfico y de localización de que dispongan estos proveedores de servicios.

En todo caso, estas medidas legislativas que puedan adoptar los distintos Estados deberán garantizar siempre *"mediante normas claras y precisas, que la conservación de los datos en cuestión está supeditada al respeto de las condiciones materiales y procesales correspondientes y que las personas afectadas disponen de garantías efectivas contra los riesgos de abuso"*[40].

2. TRATAMIENTO DE LOS DATOS PERSONALES CON FINES PENALES POR PARTE DE LOS PARTICULARES

Como se ha podido ver en el acápite anterior el régimen establecido en la Directiva (UE) 2016/680 y en la LO 7/2021 respecto del tratamiento de datos personales para fines penales queda reservado en su aplicación a las autoridades competentes. De ahí que la recogida y tratamiento de datos personales para su uso en el proceso penal por parte de los particulares queda claramente fuera de esa regulación y está sometida a la normativa general de protección de datos, en concreto a lo establecido en la Reglamento (UE) General de Protección de datos y en la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

La circunstancia de que los particulares no estén sometidos a la normativa específica relativa al tratamiento de datos personales con fines penales supone que, en su actuación para la obtención de pruebas de cargo o de descargo que supongan afectación y manejo de datos personales,

---

delincuencia, no necesariamente grave, se puedan adoptar medidas "*que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia y de la protección de la seguridad pública, una conservación generalizada e indiferenciada de los datos relativos a la identidad civil de los usuarios de medios de comunicaciones electrónicas*".

40. *Cfr*. STJUE (Gran Sala) de 20 de septiembre de 2022 Bundesrepublik Deutschland / SpaceNet AG (C-793/19), Telekom Deutschland GmbH (C-794/19).

estarán sometidos a las exigencias y condicionamientos del Reglamento General de Protección de datos. En este sentido, a los efectos del presente trabajo, lo que interesa analizar son los principios del tratamiento que se prevén en el artículo 5 del Reglamento (UE) 2016/679, y los efectos que su infracción tiene para el uso de los datos personales como fuente de prueba en los procesos.

En concreto, de acuerdo con la previsión de la norma europea, el tratamiento de datos personales debe respetar el principio de licitud, lealtad y transparencia[41]; el principio de limitación de la finalidad[42]; el principio de minimización de los datos; el principio de exactitud; el principio de limitación del plazo de conservación; y el principio de integridad y confidencialidad. De todos ellos, sin duda, los más relevantes, por su trascendencia en relación con el valor probatorio de los datos en el proceso, son: el principio de licitud y el principio de finalidad en el tratamiento de los datos. Puesto que, si la recopilación y su posterior tratamiento no se hace de forma lícita y para la finalidad para la que se recogieron, los datos personales no podrán ser considerados fuentes de prueba válidas para su uso en el seno de un proceso. Y por eso vamos a analizar a continuación la esencia de su contenido y las exigencias o requisitos que su vigencia impone a la recogida y tratamiento de los datos personales para un posterior uso en un proceso jurisdiccional.

2.1. Licitud del tratamiento de los datos personales por parte de los particulares

La principal exigencia del tratamiento de los datos personales es su licitud (artículo 5.1.a Reglamento UE 679/2016). De modo que el tratamiento de los datos, para respetar las exigencias y previsiones del Reglamento General de Protección de Datos, habrá de cumplir al menos una de las condiciones previstas en el artículo 6 para que pueda ser considerado lícito. De entre las distintas condiciones que se prevén en el artículo sobresale, sin la menor duda, como condición esencial para la licitud el consentimiento del interesado para el tratamiento de sus datos personales para

41. Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado (artículo 5.1 a).

42. Lo que supone que los datos serán "*recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales*" (artículo 5.1.b). Este principio es esencial para la determinación del valor que debe darse a los datos como fuente de prueba para los procesos.

uno o varios fines específicos (artículo 6.1.a). Las restantes condiciones para el tratamiento que se prevén en el precepto tienen en la práctica una menor incidencia[43], ya que la gran mayoría de los tratamientos de datos personales resultan lícitos por contar con el consentimiento del interesado titular de los datos.

En consecuencia, la condición por excelencia que debe cumplirse para el lícito tratamiento de los datos es el consentimiento del interesado. La importancia del consentimiento para el uso de los datos personales por parte de terceros, también en el desarrollo de los procesos, obliga a hacer unas consideraciones específicas sobre el alcance, la necesidad y los efectos que produce el consentimiento, o más correctamente la falta del mismo, en el uso de los datos en el seno de un proceso penal. Por ello, en este apartado se aborda un análisis del papel del consentimiento del titular de los datos en el proceso penal.

El consentimiento del titular de los datos se configura como la pieza clave para su recopilación, uso y tratamiento por terceros. Ahora bien, no debe perderse de vista que el consentimiento de los titulares de los datos no es una manifestación de una voluntad única y simple, sino que es un acto de voluntad complejo, cuyo objeto se extiende a varias actuaciones que pueden hacer los terceros respecto de los datos personales de alguien, que van desde la obtención y recogida de los mismos, hasta su posterior tratamiento.

De manera que es necesario distinguir claramente los diversos consentimientos que debe prestar la persona titular de los datos. Pues, de una parte, ha de consentir la recogida y recopilación de sus datos, y de otra parte, consentir el tratamiento posterior de los mismos para unas finalidades que debe conocer en el momento de aceptar el tratamiento. Esta distinción entre los consentimientos, que presta el titular de los datos, resulta fundamental a la hora de analizar el uso de los datos personales en los procesos, ya que, como veremos con detalle posteriormente, la normativa prevista en la Ley Orgánica del Poder Judicial para el tratamiento jurisdiccional de los datos personales (artículo 236 ter 3) no toma en consideración esos dos momentos del consentimiento, el de la recogida y el del posterior tratamiento, centrando su atención exclusivamente en

43. Algunas de las condiciones previstas en el artículo son: "*b)el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; c)el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; d)el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; e)el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*".

el momento del tratamiento jurisdiccional de los mismos. De forma que se produce una confusión sobre el alcance que tiene la imprescindible exigencia de consentimiento del interesado para la recogida y tratamiento de sus datos, aun en los casos en que los mismos puedan acabar siendo tratados en un proceso.

El consentimiento del interesado para la recogida y tratamiento de sus datos personales presenta un elemento que lo caracteriza, y es el hecho de que la voluntad de consentir ha de estar dirigida teleológicamente a unos fines concretos y determinados. En este sentido, el artículo 6.1.a) del Reglamento (UE) 2016/679 expresamente prevé que una de las condiciones que pueden determinar la licitud del tratamiento es que *"el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos"*. De manera que, el consentimiento del titular de los datos para que puedan ser tratados lícitamente no se manifiesta en una aceptación incondicionada, sino que es una aceptación que se vincula y condiciona a las concretas finalidades que se puedan cumplir con los datos recopilados u obtenidos. Este elemento teleológico es fundamental en relación con el consentimiento que puedan prestar las personas, que deben comprender y aceptar las finalidades para las que se recopilan sus datos.

Hay, pues, una evidente transcendencia del principio de finalidad en el tratamiento de los datos (artículo 6.1.b Reglamento UE 2016/679), que se proyecta sobre la voluntad del interesado al aceptar la recogida y uso de sus datos personales. De manera que, en principio, un tratamiento de datos al margen de las finalidades para las que se consiente no constituirá un tratamiento lícito de los mismos.

El respeto del principio de finalidad en el tratamiento lícito de los datos personales resulta especialmente importante en aquellos casos en los que un particular proceda a tratar los datos personales para una finalidad, como es la prevención, investigación o enjuiciamiento de los delitos, claramente diversa de aquella que consintió el titular de los datos[44]. En este supuesto el uso que realice el particular aportando esos datos al proceso penal como prueba supondrá un tratamiento ilícito de los mismos que debe provocar su exclusión probatoria por haber sido utilizados con vulneración del derecho fundamental a la protección de datos.

44. Por ejemplo, que una compañía de telefonía móvil utilice los datos de alguno de sus clientes, que tiene recopilados con fines de facturación y gestión comercial de sus servicios, para aportarlos como prueba en un proceso penal concreto, supone, no debe perderse de vista, un uso o tratamiento de esos datos para un fin distinto del consentido por el titular de los mismos, y constituye un tratamiento ilícito.

Por otra parte, en el Reglamento (UE) 2016/679 se establece que el consentimiento debe ser libre, específico, informado e inequívoco[45].

En primer lugar, hay que tener presente que la libertad exigida en el momento de aceptar el tratamiento de los datos personales es un requisito axiomático del consentimiento[46]. De manera que es un requisito que necesariamente deberá concurrir en la voluntad expresada para consentir y que se concreta en que *"el consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno"*[47].

En segundo lugar, el consentimiento ha de ser específico, lo que implica que, cuando los datos proporcionados vayan a ser tratados para varias finalidades, el interesado deberá prestar su consentimiento para cada una de ellas. Esta exigencia está directamente conectada, de una parte, con la dimensión teleológica del consentimiento que se reconoce en el artículo 6.1.a del Reglamento (UE) 2016/679, y de otra parte, con el principio de finalidad en el tratamiento de los datos (artículo 6.1.b). De hecho, es un elemento esencial en relación con el uso de datos personales en el proceso, dado que se vincula con los dos consentimientos que concurren, el necesario para la recopilación y tratamiento de los datos por el responsable, y en un segundo momento, el eventual consentimiento para el tratamiento jurisdiccional de los mismos, que como ya se ha indicado no resulta necesario a tenor de lo dispuesto en el artículo 236.3 ter LOPJ a pesar de ser una finalidad que puede no haber estado presente cuando se consintió la recopilación e inicial tratamiento de los datos.

En definitiva, como indica el Reglamento (UE) 2016/679 *"el consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos"* (Cdo. 32). En igual sentido, el artículo 6.2. LO 3/2018 de Protección de Datos Personales y garantía de los derechos

45. En similares términos se contempla la necesidad de consentimiento prevista en artículo 6.1 de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.

46. Así lo indica ARJONA GUAJARDO-FAJARDO cuando señala que "*un requisito que, dado su carácter axiomático, no necesita demostración ni justificación. Por ello, su análisis práctico debe realizarse adoptando una perspectiva negativa, esto es indagando cuándo puede entenderse que el consentimiento no ha sido prestado libremente*" (*cfr*. "El consentimiento para el tratamiento de datos personales: requisitos del mismo y capacidad para prestarlo a la luz del nuevo Reglamento europeo (Reglamento UE 2016/679)" en *Uso y cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios*, Oubiña Barbolla, S. y Catalina Benavente, M. A. (coord.), Colomer Hernández, I. (dir.), Aranzadi Thomson-Reuters, Cizur Menor, 2019, p. 707.

47. Cdo. 42 Reglamento (UE) 2016/679.

digitales prevé que *"cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas"*.

En tercer lugar, el consentimiento ha de ser informado, lo que supone que el interesado reciba una información clara y precisa sobre los datos que se le solicitan y sobre el tratamiento que se vaya a realizar con ellos.

Por último, el consentimiento debe ser inequívoco, lo que supone que no podrá ser presunto ni expresado en forma ambigua o genérica, sino que debe ser expreso, concreto y afirmativo.

2.2. Regulación de la LOPJ sobre el consentimiento para el tratamiento jurisdiccional de los datos

En un escenario como el que se ha ido describiendo en los anteriores apartados, y en el que la garantía del derecho a la protección de datos se materializa en la exigencia de licitud en el tratamiento de los datos personales, básicamente a través del consentimiento de los titulares de los datos que se extiende a la finalidad para la que son recogidos y tratados, nuestro legislador se ha visto impelido a introducir en la Ley Orgánica del Poder Judicial[48], una regulación específica en relación con el uso de los datos personales por parte de la Administración de Justicia con fines no jurisdiccionales y en relación con el uso de los datos por jueces y fiscales con finalidad jurisdiccional.

En particular hay que tener presente la previsión del artículo 236 ter 3 LOPJ cuando expresamente establece 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"*.

Esta norma merece una valoración crítica, dado que no distingue entre recopilación y posterior uso de los datos, limitándose a establecer una genérica habilitación para el tratamiento jurisdiccional de los datos sin que resulte necesario el consentimiento del titular, prescindiendo del origen y obtención de esos datos. El precepto no distingue entre el momento

48. El Capítulo I bis del Título III de la LOPJ, que lleva por rúbrica "*Protección de datos de carácter personal en el ámbito de la Administración de Justicia*" (artículos 236 bis a 236 decies), se introdujo por la Ley Orgánica 7/2015, de 21 de julio y ha sido objeto de modificación por la Ley Orgánica 7/2021, de 26 de mayo.

en que se recogen los datos y el tratamiento inicial de los mismos y el posterior momento en que son tratados en el seno de un proceso.

En este sentido, hay que hacer notar que la norma sólo exonera el consentimiento del interesado para el tratamiento que se realice con fines jurisdiccionales, pero no exime de la necesidad del consentimiento para la recopilación y recogida de los datos, así como para el tratamiento y la finalidad para la que inicialmente fueron recogidos. Por tanto, el no cumplimiento de las exigencias previstas para esa recogida y tratamiento previos al acceso de los datos al proceso (consentimiento, licitud, finalidad, etc.) ha de tener consecuencias en el valor probatorio de los datos en el proceso, sin perjuicio que para su incorporación al proceso y tratamiento por el órgano jurisdiccional no se requiera el consentimiento del interesado. De hecho, no debe perderse de vista, que el propio artículo 236 ter 3 LOPJ deja la puerta abierta a la existencia de estos efectos procesales en cuanto a la validez de los datos personales como prueba, al remitirse expresamente a lo dispuesto en las normas procesales para la validez de la prueba.

De ahí que, pudiera parecer que este artículo prescinde del origen lícito de los datos personales que se puedan usar en un proceso y que solo se preocupa de garantizar que el tratamiento que realice el juzgador, una vez que los datos hayan tenido acceso al proceso, pueda realizarse sin problemas a pesar de que la finalidad de uso jurisdiccional de los datos no haya sido expresamente consentida por el interesado. Y es que, en efecto, asegurar y exigir el carácter lícito de los datos personales desde su origen, sustancialmente que se hayan obtenido y recopilado cumpliendo al menos una de las condiciones previstas en el artículo 6 del Reglamento (UE) 2016/679, no parece ser una preocupación de esta norma. El precepto se limita a habilitar el tratamiento de los datos en el seno de un proceso, aunque esta finalidad no haya sido consentida por el interesado. Y lo único que contiene en relación con la eventual ilicitud de los datos en su origen es la remisión a *"sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba"*, lo que supone que todas las cuestiones relativas a la ilicitud de los datos desde su obtención y recogida deban ventilarse en el seno del momento de admisión de la prueba, conforme a lo dispuesto en las normas procesales. Al respecto, no debe perderse de vista que en la actualidad las normas procesales de los distintos órdenes jurisdiccionales carecen de normas específicas destinadas a regular la validez de los datos personales para su uso en los procesos en aquellos casos en los que los datos puedan tener vicios por no haberse cumplido las exigencias de la normativa de protección de datos en su recogida y posterior tratamiento[49].

49. No debe perderse de vista que el Anteproyecto de LECrim de 2020 recogiendo la necesidad de dar trascendencia procesal, desde el punto de vista la validez probatoria,

Por último, es necesario realizar alguna consideración en relación con la forma de incorporación de los datos personales a los procesos. En concreto, respecto a la distinción que se establece en el artículo 236 ter 3 LOPJ entre que los datos sean facilitados por las partes o recabados a solicitud de los órganos competentes para su incorporación al proceso. Hemos de tener en cuenta que, a pesar de lo que pudiera parecer del tenor del precepto, no resulta indiferente, según la clase de los datos, que sean aportados por las partes del proceso o requeridos por el juzgador.

Así, por ejemplo, la reciente STJUE (Gran Sala) de 5 de abril de 2022, en el asunto C 140/20 (Caso Commissioner of An Garda Síochána y otros) ha indicado que el acceso a los datos conservados por los proveedores de servicios de comunicaciones electrónicas solamente puede realizarse con el control previo realizado por órgano independiente ("*bien por un órgano jurisdiccional, bien por un órgano administrativo independiente*")[50]. De manera que la aportación directa por las partes de esa clase de datos sin haber sido requeridos por el juez tras un previo control podría vulnerar el derecho a la protección de datos. Por ello, en los casos de aportación de los datos por las partes el juzgador deberá controlar y verificar que el litigante esté habilitado para, de conformidad con las exigencias de la normativa de protección de datos, para poder aportar esa información personal. Este concreto control debe extenderse a comprobar que los datos se han recopilado y tratado lícitamente, de acuerdo a las previsiones del artículo 6 Reglamento (UE) 2016/679.

En conclusión, por tanto, se constata que la habilitación del artículo 236 ter 3 de la LOPJ, para el tratamiento de los datos con fines jurisdiccionales, lo único que hace es exonerar la necesidad del consentimiento del interesado para el uso de los datos para una finalidad diversa de la que fueron obtenidos, pero no convalida, ni subsana los posibles defectos o vicios

---

al respeto y cumplimiento de las exigencias y requisitos derivados de la protección de datos personales, ha previsto en su artículo 520. 2 que "*Únicamente serán válidos aquellos datos relevantes para la investigación cuya obtención, tratamiento e incorporación se realice con sujeción a lo dispuesto en esta ley y en la normativa reguladora del tratamiento de datos personales para fines de prevención, investigación y enjuiciamiento de infracciones penales*". Es decir, no hay la menor duda que la necesidad de respetar las exigencias de la protección de datos en la obtención y tratamiento de las pruebas ha de ser un requisito imprescindible para la validez probatoria de las fuentes de prueba obtenidas, resultando su incumplimiento una causa de exclusión probatoria al amparo de la previsión contenida en el artículo 11.1 LOPJ.

50. Un análisis detallado de esta Sentencia en RODRÍGUEZ LAINZ "La evolución de la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de conservación indiscriminada de datos de comunicaciones electrónicas en la STJUE del Caso G. D. y Comissioner an Garda Síochána" en *Diario La Ley*, n.º 10058, 28 de abril de 2022, 22 pp.

de licitud que pudieran existir en la recogida e inicial tratamiento de los mismos. Es decir, la excepción que supone este precepto al principio de limitación de la finalidad en relación con el tratamiento jurisdiccional de los datos personales que se usen en un proceso como fuentes de prueba en modo alguno convalidará o subsanará los defectos de licitud que puedan gravar a los datos en su recogida y en su inicial tratamiento.

Por todo ello, la licitud del tratamiento de los datos personales de un interesado resulta una exigencia esencial para el respeto del derecho a la protección de datos de la persona titular de los mismos, de ahí que, si la recogida y uso de los datos no reúne los requisitos legalmente previstos, sustancialmente la necesidad de consentimiento del interesado, el resultado será que el tratamiento de los datos se realizará vulnerando el derecho fundamental a la protección de datos y en ciertos casos, que se concretaran más adelante en este trabajo, determinará la posibilidad de su exclusión como fuente de prueba en los procesos jurisdiccionales.

2.3. El problema de la finalidad del tratamiento de los datos personales por los particulares para su uso con fines penales

El segundo de los principios, previstos en el artículo 5 del Reglamento (UE) 679/2016, que han de presidir el tratamiento de los datos personales es el principio de limitación de la finalidad[51], según el cual: *"los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines"* (artículo 5.1.b). Este principio resulta de especial importancia en relación con el uso de datos personales en los procesos, ya que, en principio, la necesidad de una finalidad específica y concreta en el momento de la recogida y tratamiento de los datos obliga al responsable a comunicársela al interesado en el momento de obtener su consentimiento, como hemos podido ver en el anterior apartado. Por tanto, la vulneración del principio de limitación de la finalidad supone una infracción del derecho a la protección de datos por implicar la realización de algún tratamiento de los datos que no cumpla con este fundamental principio del artículo 5 del Reglamento (UE) 2016/679.

En un análisis del alcance del principio de limitación de finalidad se puede comprobar que, a efectos de la licitud de un tratamiento para un fin distinto de aquel para el que se recogieron los datos, en la regulación se

51. El artículo 4.1.3 del Reglamento (UE) 679/2016 define la limitación del tratamiento como "*el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro*".

prevén dos circunstancias que habilitan la posibilidad de un tratamiento para fines diversos: de un lado, aquellos casos en los que exista un consentimiento del interesado para unas finalidades distintas, y de otro lado, los casos en los que de acuerdo con el Derecho de la Unión o de los Estados miembros el tratamiento para finalidades distintas constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar alguno de los objetivos indicados en el artículo 23, apartado 1 del Reglamento (UE) 2016/679. De entre los objetivos que se recogen en el indicado precepto destacan, por su posible relación con el tratamiento de los datos personales para su uso en los procesos, los dos siguientes: (i) la protección de la independencia judicial y de los procedimientos judiciales; (ii) la protección del interesado o de los derechos y libertades de otros.

De modo que, fuera de estas dos habilitaciones para un tratamiento con finalidades distintas a aquellas para las que se recogieron los datos, el responsable del tratamiento deberá determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales (artículo 6.4).

La compatibilidad entre los fines deberá ser apreciada por el particular responsable del tratamiento atendiendo, entre otros, a los siguientes criterios: (i) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto; (ii) el contexto en que se hayan recogido los datos personales; (iii) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales; (iv) las posibles consecuencias para los interesados del tratamiento ulterior previsto; (v) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

Sin embargo, en mi opinión este juicio de compatibilidad previsto en la norma no resultará efectivo en el supuesto que estamos analizando, pues no se debe de olvidar que nos encontramos antes un tratamiento para un fin penal, su uso como prueba en un proceso penal, de datos obtenidos y recopilados por el particular para fines diversos de los penales.

Por ello, dadas las dos posibilidades previstas en la norma para el tratamiento de datos con una finalidad distinta de aquella para la que fueron recopilados y conservados, resulta claro que el uso de los datos como fuente de prueba en un proceso solo podrá producirse siempre que el interesado lo haya consentido o una norma con rango de ley lo haya autorizado para la salvaguarda de alguno de los objetivos del artículo 23 del Reglamento (UE) 2016/679.

En definitiva, a modo de conclusión, debe destacarse que el principio de finalidad en el tratamiento condiciona las posibilidades de uso de

los datos personales, y que consecuentemente, salvo las dos excepciones previstas en el RGDP[52], el tratamiento para una finalidad distinta de que aquellas para las que se recogieron y se autorizó su tratamiento por el titular de los datos, supondrá que el uso no resultará lícito por adecuarse a las exigencias previstas en el artículo 6.4 Reglamento (UE) 2016/679.

3. EXCLUSIÓN PROBATORIA DE DATOS PERSONALES TRATADOS POR LOS PARTICULARES EN EL PROCESO PENAL

La última de las cuestiones que deben abordarse es la relativa al régimen jurídico procesal que se aplica a los datos de personales cuando son usados o se pretende su empleo como fuentes de prueba en el seno de un proceso penal por parte de los particulares sin haber realizado un tratamiento lícito de los mismos.

Como se ha indicado en el epígrafe anterior la actual regulación contenida en el artículo 236 ter 3 LOPJ recoge una general habilitación legal para el tratamiento de datos personales en el seno de los procesos dentro de la actividad jurisdiccional. En concreto, está previsto que no sea necesario el consentimiento del interesado para que sus datos personales puedan ser tratados con finalidad jurisdiccional en el seno de un proceso. Dicho, en otros términos, la norma excepciona la necesidad de consentimiento expreso para un tratamiento con una finalidad distinta de aquella para la que fueron recopilados, esto es, para su tratamiento con una finalidad jurisdiccional.

Esta previsión habilitante del cambio de finalidad en el tratamiento de los datos respecto a la que determinó su recogida y conservación no puede ocultar, ni convalidar, los vicios o defectos en los que se haya podido incurrir en el momento de la recogida de los datos. En efecto, si en la obtención y recogida de los datos, o incluso posteriormente en la cesión de los mismos a un tercero, no se han respetado las exigencias previstas en el artículo 6 del Reglamento (UE) 2016/679 para la licitud del tratamiento, los datos se habrán obtenido y usado con vulneración del derecho a la protección de datos personales del interesado. Y esta vulneración del derecho a la protección de datos en la obtención de la fuente de prueba, en este caso los datos, ha de tener necesariamente reflejo en el proceso,

52. Que expresamente se haya aceptado y consentido por el titular el cambio de finalidad en su tratamiento o que, de acuerdo con el Derecho de la Unión o de los Estados miembros el tratamiento para finalidades distintas constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar alguno de los objetivos indicados en el artículo 23, apartado 1 del Reglamento (UE) 679/2016.

en particular en el examen de la validez de la prueba que debe hacer el juzgador penal[53].

En el examen de la validez de los datos como fuente de prueba en los procesos penales el juez o el tribunal deben apreciar si concurre una causa de exclusión probatoria[54]. En concreto, deben apreciar si procede la exclusión probatoria de los datos obtenidos por particulares con vulneración del derecho fundamental a la protección de datos por aplicación de lo previsto en el artículo 11.1 LOPJ[55]. En este sentido, no hay duda de que los datos obtenidos y tratados sin las exigencias del artículo 6 del Reglamento (UE) 2016/679 no son objeto de un tratamiento lícito, y en consecuencia se vulnera el derecho fundamental a la protección de datos del artículo 18.4 CE. Por ello, los datos que se consigan como consecuencia de un tratamiento ilícito deben ser excluidos del proceso y no pueden constituir una fuente de prueba legítima por haber sido obtenidos con vulneración o violación de un derecho fundamental[56].

Esta consecuencia, la exclusión probatoria de los datos que sean el resultado de un tratamiento ilícito, si bien es clara, precisa y se adecua a la normativa de protección de datos y a la regulación procesal, sin embargo, en la práctica no se suele estimar por parte de los órganos jurisdiccionales penales.

---

53. Ver, sobre esta materia, el trabajo de PÉREZ GIL, J., "Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal" en *Justicia: ¿garantías versus eficiencia?*, Jiménez Conde, F. y Bellido Penadés, R. (dir.), Llopis Nadal, P. y De Luis García, E. (coord.), Tirant lo Blanch, Valencia, 2019, p. 399-441.

54. Hay que ser plenamente consciente que está actividad de valoración probatoria de los datos personales es una tarea compleja, pues no siempre la distinción entre datos personales y datos que no lo son resulta clara cuando se examinan en un concreto proceso. Pues, como señala PÉREZ GIL "*ha de contarse por ello con los llamados 'conjuntos de datos mixtos', en los que se entremezclan datos personales y datos no personales y que representan la mayoría de los conjuntos de datos utilizados en la llamada 'economía de datos'*" (*Cfr. op. cit.*, p. 416).

55. "*En todo tipo de procedimiento se respetarán las reglas de la buena fe. No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales*".

56. "*Si los datos se han obtenido ilícitamente, esto es, vulnerando directa o indirectamente derechos o libertades fundamentales, entre los que hay que entender se encuentra el protegido por el Art. 18.4 CE de que aquí tratamos, su cesión al Juez, lo que incluye también la hecha por un particular, en principio, debe obtener la sanción procesal de la nulidad probatoria (Art. 11.1 LOPJ) –no se puede obtener la verdad a cualquier precio, o al precio de vulnerar derechos fundamentales–, e igualmente podrá conllevar la sanción administrativa (LOPDGDD) o penal (Art. 197. 3 y 7 CP) que corresponda, con la única excepción de que la obtención se haya realizado –sin el consentimiento del titular del derecho afectado y sin orden judicial– en circunstancias de urgencia, esto es, en supuestos de imposibilidad para acudir a solicitar una orden judicial, con riesgo de pérdida de la información, mientras, además de su proporcionalidad, se mantenga la finalidad probatoria*" (*cfr*. VELASCO NÚÑEZ, *op. cit*., p. 140).

Las razones que explican que indebidamente no se excluyan los datos objeto de un tratamiento ilícito son esencialmente: de una parte, una interpretación extensiva y errónea del artículo 236 ter 3 LOPJ, según la cual la no necesidad de consentimiento del interesado para el tratamiento de los datos con finalidad jurisdiccional se interpreta como una habilitación para el uso de datos personales en los procesos sin atender a la licitud de su recopilación y del tratamiento inicial anterior a su entrada en el procedimiento jurisdiccional. Y, de otra parte, que no se distingue adecuadamente entre dos de los principios del artículo 5 del Reglamento (UE) 2016/679 que han de respetarse en el tratamiento de datos personales: el principio de licitud y el principio de limitación de la finalidad. Puesto que se olvida que la posible ilicitud del tratamiento por el que se obtienen los datos no queda subsanada, ni convalidada, por la previsión del artículo 236 ter 3 LOPJ, que lo único que hace es excepcionar la necesidad de consentimiento del interesado para el uso de los datos con una finalidad distinta de la que se recogieron.

Por tanto, aunque el precepto de la LOPJ permita el tratamiento jurisdiccional de los datos sin el consentimiento del interesado, ello no supone que el juzgador no tenga que apreciar la validez probatoria de los datos personales atendiendo a la licitud en el momento de su obtención y en los tratamientos anteriores a su aportación al proceso por parte de los particulares. Y en el caso de que los datos hayan sido obtenidos o tratados sin cumplir con las exigencias del artículo 6 del Reglamento (UE) deberá declarar su nulidad para ser usados como prueba[57].

Las concretas posibilidades de vulneración del derecho a la protección de datos personales en la obtención y tratamiento de los datos que posteriormente vayan a ser incorporados a un proceso penal por parte de los particulares son múltiples. A efectos de una posible clasificación de los casos de vulneración de este derecho fundamental hay que atender a un doble criterio: de un lado, a los vicios, esencialmente a la ilicitud, producidos en el momento de la recogida o recopilación de los datos personales; y de otro lado, a los vicios en los que se pueda haber incurrido en un tratamiento de los datos con anterioridad a su ingreso o aportación a un concreto proceso.

57. Como indica VELASCO NÚÑEZ las cesiones de datos hechas por un particular "*sólo tendrán validez probatoria –ya que no vulnerarán el derecho recogido en el Art. 18.4 CE, que es de protección legal, a través del Reglamento General y las Directivas específicas como la 2016/68013– cuando:*
– estén consentidas por el titular del derecho afectado,
– estén autorizadas por el Juez Instructor,
– o vengan justificadas por circunstancias de urgencia y obedezcan a un fin social o a un interés público" (*cfr. op. cit.*, p. 144).

Por ello, en aplicación de ambos criterios podemos identificar algunas de las vulneraciones de este derecho fundamental que más se dan en la práctica:

(i) Los datos son recopilados por los particulares sin el consentimiento del interesado y sin que concurra ninguna otra de las condiciones previstas en el artículo 6 del Reglamento (UE) 2016/679 para que el tratamiento sea lícito.

El caso más usual en el que se produce una vulneración del derecho a la protección de datos tiene lugar cuando los datos son recogidos, obtenidos o recopilados de forma ilícita por no cumplirse ninguna de las condiciones previstas en el RGPD. En estos supuestos la obtención de los datos, y su posterior tratamiento, no estaría habilitada de acuerdo con la normativa de protección de datos personales, y, en consecuencia, el uso y tratamiento de los mismos sería nulo y deberían ser excluidos como prueba en el proceso penal, por haber sido obtenidos con vulneración del derecho fundamental a la protección de datos.

En relación con estos supuestos se plantea el problema de cómo actuar en aquellos casos en los que los datos se recopilan de canales abiertos[58], es decir de fuentes de acceso libre, sin que la voluntad del titular de los datos haya establecido ninguna clase de exigencia para acceder a los mismos. En principio, cuando los datos se obtienen de canales abiertos puede

58. No debe perderse de vista que el anteproyecto de LECrim de 2020 prevé, de forma a mi juicio poco afortunada, en el artículo 514 ALECrim en relación con la búsqueda y obtención de datos a través de fuentes y canales abiertos por parte de las autoridades competentes que "1. *Para averiguar los delitos o descubrir a los responsables de su comisión, la Policía Judicial, por sí o por orden del Ministerio Fiscal, podrá recabar todas aquellas informaciones relevantes para la investigación que se encuentren disponibles en fuentes abiertas de información, así como los datos relativos al investigado que sean accesibles a través de canales abiertos de comunicación*". De manera que parece reconocer una libertad de obtención y uso de los datos personales que existan en canales abiertos sin necesidad de autorización jurisdiccional, salvo cuando esa recopilación de datos personales de fuentes abiertas "*se realice de forma sistemática y continuada con el objeto de crear un registro histórico de la actividad del investigado en el entorno digital, será necesaria autorización previa del Juez de Garantías*" (artículo 514.2 ALECrim). En todo caso, aunque eventualmente se pudiera aceptar esa libertad de búsqueda de datos por parte de las autoridades competentes en los canales abiertos, hipótesis que resulta más que dudosa desde el punto de la garantía de los derechos fundamentales, en concreto desde el de la protección de datos personales, no puede ocultarse que en la práctica se viene realizando (informes OSINT, etc.). Sin embargo, parece más adecuado sostener que los particulares no estarán habilitados para un tratamiento de datos personales de canales abiertos consistente en su aportación como fuente de prueba al proceso penal, siempre y cuando los datos se hayan recopilado sin el consentimiento del titular y sin que concurra ninguna otra de las condiciones del artículo 6 Reglamento (UE) 2016/679 que permita considerar que con esa actuación se produce un tratamiento lícito.

pensarse que la persona que los recopila y posteriormente los utiliza no está vulnerando el derecho a la protección de datos, pero ello es así solo en el caso que los datos hayan sido subidos o puestos por el titular en el canal abierto[59]. Por el contrario, si los datos no han sido subidos por su titular sino por un tercero, sin autorización o consentimiento del titular de los mismo, resulta evidente que cuando son tomados de la fuente de acceso libre se estará ante una recopilación y tratamiento ilícito, que en caso de resultar finalmente aportado a un proceso penal habrá de determinar la exclusión probatoria de dichos datos personales.

No es fácil mantener otra interpretación, pues hacerlo supondría reconocer que por el simple hecho de que un tercero suba a un canal de acceso libre una determinada información, obtenida sin el consentimiento de su titular, se estaría convalidando y subsanando esa obtención y tratamiento ilícito si se permitiese que tomada la información personal de la fuente de acceso libre ya no se considerase que se ha producido una vulneración del derecho a la protección de datos, que debiera llevar aparejada la exclusión probatoria de la información personal ilícitamente obtenida[60].

(ii) Los datos recopilados lícitamente son cedidos a un tercero sin el necesario consentimiento del interesado y el tercero destinatario los aporta al proceso penal.

Otro de los supuestos de vulneración del derecho a la protección de datos que, con cierta frecuencia, ocurre en la realidad es aquel en el que la recogida y tratamiento inicial de los datos en forma lícita, normalmente por haber sido consentida por el titular de los mismos, deviene en una situación de ilicitud en tratamientos posteriores, toda vez que estos no

59. La Agencia Española de Protección de datos expresamente ha señalado en una reciente resolución de septiembre de 2022 que "*no pueden ser objeto de tratamiento los datos personales obtenidos de una red social o de internet, sin que concurra alguna de las bases de legitimación previstas en el art. 6 del RGPD. Por lo tanto, se considera que estamos ante un tratamiento ilícito de datos personales, ya que en este caso la parte reclamada ni siquiera intentó obtener el consentimiento de los reclamantes para el uso de su imagen, dado que consideró que tenía interés legítimo para su tratamiento*" (Resolución sancionadora en Expediente N.º: EXP202104917).

60. A modo de ejemplo, imaginemos que un dato personal de una persona es subido sin su consentimiento a una página web de una empresa a una sección que es de acceso libre, y de ahí es tomada por un tercero que la aporta a un proceso penal como prueba. La aportación al proceso no requerirá consentimiento del titular de los datos por la prescripción del artículo 236 ter 3 LOPJ, pero el simple hecho de que se haya tomado de una fuente de acceso libre no convalida, ni subsana el vicio de ilicitud que grava la obtención de esos datos y el primer tratamiento de los mismos, consistente en su publicación en la web de la empresa sin el debido consentimiento.

son consentidos, ni aceptados por el titular de los datos[61]. En estos casos, el destinario de los datos que no ha sido autorizado por el titular, al tratar los datos incurre en causa ilicitud por no cumplir con las exigencias del artículo 6 del Reglamento (UE) 679/2012, y por ello cuando aporta los datos al proceso penal incurre en causa de exclusión probatoria por tratarse de evidencias obtenidas y tratadas con vulneración del derecho fundamental a la protección de datos del artículo 18.4 CE[62].

(iii) Los datos recopilados lícitamente son cedidos a un tercero con el consentimiento del interesado, pero el tercero destinario los trata para una finalidad diversa de la consentida, antes de su aportación al proceso penal.

En este caso, aunque la aportación al proceso con la finalidad de tratamiento jurisdiccional de los datos queda habilitada por el artículo 236 ter 3 LOPJ, el tratamiento realizado por el tercero destinatario de los datos cedidos no resulta ajustado a la finalidad para la que se consintió y en consecuencia los datos se considerarán ilícitamente obtenidos[63]. Es decir, en este supuesto la recopilación y el inicial tratamiento de los datos por el responsable ha sido lícita por haber sido consentida por el titular, sin

61. Como señala DELGADO MARTÍN "*Si se trata de datos de los que es titular la propia parte que los aporta, no concurre vulneración alguna del derecho reconocido en el art. 18.4 CE. Los problemas surgen cuando se aportan datos personales de otra parte procesal, o de otra persona que no tiene el estatuto de parte en el procedimiento: en estos casos será necesario el consentimiento del interesado; y ante su ausencia, cabe analizar con detenimiento si la cesión del dato (comunicación como forma de tratamiento) se ha producido de forma ilícita (base jurídica que lo legitima)*" (*cfr*. "Protección de datos personales y prueba en el proceso", en *Diario La Ley*, n.º 9383, 22 marzo 2019, p. 10).

62. Por ejemplo, pensemos en el supuesto de un paciente que consiente que una serie de pruebas diagnósticas le sean realizadas en un centro médico y que los resultados de las mismas, que no olvidemos forman parte de las categorías especiales de datos previstos en el artículo 13. 1 LO 7/2021, sean tratados por el personal sanitario a efectos terapéuticos. Y posteriormente esos datos sanitarios son cedidos por el hospital de forma expresa a uno de los médicos que ha tratado al paciente que los utiliza como fuente de prueba de descargo en un proceso penal en el que está siendo investigado por un delito de homicidio imprudente de otro paciente.

63. Un ejemplo puede ser el siguiente: una persona consiente que su historial crediticio (saldo de sus cuentas, deudas que le gravan, etc.) sea cedido por su entidad financiera a una cooperativa de viviendas para que sean usados para decidir si le admiten como cooperativista o no. El presidente de la cooperativa es acusador particular en un proceso contra un tercero ajeno a la cooperativa por un delito societario y procede a aportar los datos bancarios del cooperativista, que fueron aportados exclusivamente para decidir su admisión en la cooperativa. La aportación será posible al amparo del artículo 236 ter 3 LOPJ sin necesidad del consentimiento, pero ese dato podrá ser excluido de su uso como fuente de prueba si cuando se consintió la cesión de esos datos no se autorizó su uso para un proceso un proceso penal, sino exclusivamente para su admisión en el seno de la cooperativa.

embargo, la posterior cesión a un tercero no ha sido consentida, lo que determina que en consecuencia el tratamiento por ese tercero no sea lícito y cuando los aporte al proceso al amparo de la habilitación legal no estará convalidado, ni subsanado, el vicio de nulidad que grava su obtención y tratamiento, debiendo el juzgador acordar su exclusión probatoria en aplicación de la previsión del artículo 11.1 LOPJ.

(iv) Los datos recopilados lícitamente son comunicados por el responsable del tratamiento a un tercero para la prestación de un servicio y el tercero los aporta al proceso penal sin que el titular de los datos los sepa y lo haya consentido.

En estos casos hay que tener presente que nos encontramos en supuestos de comunicación de los datos, que no cesión de los mismos[64], en los que la persona que los ha recibido los trata y los usa sin el debido consentimiento por parte de su titular, dado que recibe los datos de un tercero que fue el que legítimamente los recogió y los trató con el consentimiento del titular de los mismos. De manera que la persona a la que se comunican los datos sin haber sido objeto de autorización por parte del titular, cuando trata esos datos lo está haciendo de forma ilícita, si no cuenta con el consentimiento del titular o si no concurre alguna otra de las condiciones del artículo 6 del RGPD. Y, en consecuencia, a pesar de que pueda aportarlos a un proceso sin el consentimiento del titular gracias a la habilitación legal del artículo 236 ter 3 LOPJ, no hay duda de que, para aceptar esos datos como fuente de prueba, el tribunal deberá comprobar la licitud en la obtención y tratamiento de los datos, al margen de la aportación al procedimiento jurisdiccional, y en su caso acordar la exclusión probatoria de los mismos por vulneración del derecho fundamental a la protección de datos.

64. Sobre esta distinción ARJONA GUAJARDO-FAJARDO señala que "*hay que distinguir entre ceder datos a un tercero, y proporcionar a un tercero acceso a determinada información en orden a posibilitarle que preste un servicio. No todo acto de comunicación de datos a un tercero implica cesión de datos. Hay cesión de datos si el tercero que recibe los datos puede utilizarlos para sus propios fines, decidiendo el objeto y finalidad del tratamiento (v.gr., se vende la base de datos que uno tiene a un tercero, para que se sirva de ella en orden a enviar publicidad de sus propios productos). Hay simple acceso a datos cuando el tercero recibe los datos para realizar determinadas operaciones y prestar con ello un servicio a quien se los ha facilitado, pero no puede decidir sobre su finalidad (v.gr., una empresa pide a un abogado asesoramiento laboral, y para ello le traslada los datos de sus trabajadores; o encarga la gestión de nóminas a un gestor externo, para lo cual le comunica los datos de los trabajadores*)" (*Cfr. op. cit.*, p. 706).