eman ta zabal zazu

Universidad del País Vasco
Euskal Herriko Unibertsitatea

ZUZENBIDE FAKULTATEA
FACULTAD DE DERECHO

CONSERVACIÓN Y CESIÓN DE DATOS PERSONALES PARA LA PERSECUCIÓN DE DELITOS Y LA INTERSECCIÓN DE LOS OPERADORES DE SERVICIOS DE TELECOMUNICACIONES

TRABAJO DE FIN DE GRADO

CURSO ACADÉMICO 2023/2024

GRADO EN DERECHO

DONOSTIA - SAN SEBASTIÁN

Trabajo realizado por: Anielka Fabiola Pérez Obando

Dirigido por: Jose Francisco Etxeberria Guridi

RESUMEN.

La conservación y cesión de datos personales en el ámbito de la persecución de delitos plantea desafíos legales y éticos, especialmente en la intersección con los operadores de servicios de telecomunicaciones. Este estudio analiza el marco normativo vigente, evaluando la adecuación y eficacia de las leyes actuales para garantizar tanto la protección de la privacidad como la cooperación en las investigaciones criminales. Se examinan casos de estudio relevantes y ejemplos prácticos para ilustrar los problemas y dilemas asociados con esta temática. Esta investigación ofrece una comprensión de cómo interactúan los operadores de servicios de telecomunicaciones con la investigación criminal, resaltando la necesidad de lograr un equilibrio entre preservar la privacidad y garantizar la seguridad pública.

PALABRAS CLAVES: privacidad, derecho a la protección de datos, conservación de datos, cesión de datos, investigación criminal.

ABSTRACT.

The retention and transfer of personal data in the field of crime prosecution raise legal and ethical challenges, especially at the intersection with telecommunications service operators. This study analyses the current regulatory framework, evaluating the adequacy and effectiveness of current laws to ensure both privacy protection and cooperation in criminal investigations. Relevant case studies and practical examples are examined to illustrate the problems and dilemmas associated with this topic. This research offers an understanding of how telecommunications service operators interact with criminal investigation, highlighting the need to strike a balance between preserving privacy and ensuring public security.

KEYWORDS: privacy, right to data protection, data retention, data transfer, criminal investigation.

LABURPENA.

Delituen jarraipenaren esparruan datu pertsonalen kontserbazioa eta transmisioa erronka juridiko eta etikoak planteatzen ditu, batez ere telekomunikazio zerbitzuen operatzaileen arteko elkargunean. Ikerketa hau oraingo arauen markoari buruzko aztertzen du, legeak gaur egun zehazten dutenak, pribatutasunaren babesa eta krimen-ikerketen arteko lankidetza bermatzeko legeak neurtzen ditu. Gaia erakutsi ahal izateko, aztertu dira gaiarekin lotutako adibide garrantzitsua eta praktikoak. Ikerketa honek telekomunikazio zerbitzuen operatzaileek nola elkarreratzen duten krimen-ikerketa, pribatutasuna zaintzearen eta segurtasun publikoa bermatzearen arteko oreka lortzeko beharraz azaltzen du.

GAKO HITZAK: pribatutasuna, datuen babeserako eskubidea, datuen kontserbazioa, datuen lagapena, ikerketa kriminala.

ÍNDICE

LISTADO DE ABREVIATURAS UTILIZADAS

AEPD	Agencia Española de Protección de Datos
CE	Constitución Española
CDFUE	Carta de los Derechos Fundamentales de la Unión Europea
CP	Código Penal
Derechos ARCO	Derechos de acceso, rectificación, cancelación y oposición
DOUE	Diario Oficial de la Unión Europea
DUE	Derecho de la Unión Europea
LCDCE	Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones
LECrim	Ley de Enjuiciamiento Criminal
LGT	Ley General de Telecomunicaciones
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
LOPJ	Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial
LORTAD	Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal
LSSICE	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
RGPD	Reglamento General de Protección de Datos
STC	Sentencia del Tribunal Constitucional
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos

STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
STS	Sentencia del Tribunal Supremo
TUE	Tratado de la Unión Europea
UE	Unión Europea

1. INTRODUCCIÓN

1.1 Contextualización del tema

En la era de la información, los datos personales se han convertido en uno de los recursos más valiosos y, a su vez, más sensibles. La capacidad de rastrear y analizar la información generada por los usuarios de servicios de telecomunicaciones ha abierto nuevas posibilidades en la lucha contra el crimen, permitiendo a las autoridades identificar y perseguir actividades delictivas con mayor eficacia.

La Directiva 2006/24/CE sobre la conservación de datos, aunque derogada por el Tribunal de Justicia de la Unión Europea en 2014, marcó un hito al establecer la obligación de los proveedores de servicios de telecomunicaciones de almacenar datos de tráfico y localización. Esta derogación se basó en que esta Directiva infringía derechos fundamentales, como el derecho al respeto de la vida privada y la protección de datos personales, consagrados en los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea.

Este fallo marcó un punto de inflexión, obligando a los Estados miembros y a los proveedores de servicios de telecomunicaciones a revisar y adaptar sus prácticas y legislaciones en materia de conservación de datos. La jurisprudencia del Tribunal de Justicia de la Unión Europea ha seguido evolucionando, enfatizando la necesidad de protecciones sólidas y un enfoque más específico de los derechos humanos.

El presente Trabajo Final de Grado (TFG) se centra en analizar la conservación y cesión de datos personales por parte de los operadores de servicios de telecomunicaciones con fines de investigación criminal debido a que esta cuestión adquiere una relevancia excepcional a medida que se intensifica la lucha contra el crimen y las autoridades encargadas de hacer cumplir la ley recurren cada vez más a la tecnología para obtener información crucial en sus investigaciones.

1.2 Objetivos del trabajo

El principal objetivo de este trabajo es analizar la legislación europea y nacional vigente en materia de conservación y cesión de datos personales en el ámbito de la persecución de delitos. Este análisis incluirá un estudio de cómo las leyes actuales regulan

la conservación de datos por parte de los proveedores de servicios de telecomunicaciones y la cesión de estos datos a las autoridades competentes.

Además, se llevará a cabo un estudio de la jurisprudencia del Tribunal de Justicia de la Unión Europea. Se revisarán los fallos más relevantes en relación con la conservación y cesión de datos personales con el fin de evaluar su impacto y las interpretaciones jurídicas derivadas de estos fallos. Esta revisión permitirá comprender mejor cómo las decisiones del Tribunal influyen en la aplicación y evolución de la legislación europea en este ámbito.

Finalmente, se evaluará el papel de los proveedores de servicios de telecomunicaciones en el contexto de la conservación y cesión de datos personales. Se analizarán las responsabilidades y obligaciones de estos proveedores, así como los desafíos que enfrentan en la implementación de las normativas vigentes.

1.3 Justificación de la investigación

El fundamento de este TFG radica en la importancia crucial de comprender y equilibrar dos intereses aparentemente contrapuestos: la seguridad pública y la privacidad individual. La capacidad de las autoridades para acceder a datos personales puede ser fundamental para la prevención y persecución eficaz de delitos, incluyendo el terrorismo y la delincuencia organizada. Sin embargo, esta capacidad debe equilibrarse con salvaguardias robustas para proteger los derechos fundamentales de los individuos.

El estudio de la jurisprudencia del Tribunal de Justicia de la Unión Europea es particularmente relevante, ya que sus decisiones no sólo afectan a la interpretación de las leyes dentro de la Unión Europea, sino que también influyen en las políticas de privacidad y seguridad a nivel global. Este análisis es necesario para identificar tendencias y desafíos en la legislación y su aplicación práctica, proporcionando así una base sólida para futuras recomendaciones.

1.4 Metodología utilizada

Para alcanzar los objetivos propuestos se realiza una revisión general de la legislación española y europea relevante, así como un análisis crítico de la jurisprudencia y estudios de casos relacionados con la colaboración entre las compañías de telecomunicaciones y las autoridades encargadas de hacer cumplir la ley. Además, se

recopila y analiza literatura científica y fuentes especializadas para obtener una comprensión completa y actualizada de cada tema.

2. DERECHO A LA PROTECCIÓN DE DATOS COMO DERECHO FUNDAMENTAL EN LA ERA DE LA CONSERVACIÓN Y CESIÓN DE DATOS PERSONALES

2.1 Definición y alcance del derecho a la protección de datos

El derecho a la protección de datos se ha convertido en un tema fundamental en la era digital, donde la conservación y cesión de datos se ha vuelto ubicua. Este derecho surge del derecho más amplio a la privacidad y abarca el control que tienen las personas sobre la información sobre sí mismas.

La vida privada es un aspecto crucial en esta discusión. Se refiere al ámbito de la vida de una persona que está protegida de interferencias indebidas por parte de otros individuos, organizaciones o entidades gubernamentales. En este contexto, la protección de datos se vincula estrechamente con la preservación de la vida privada, ya que los datos personales son componentes fundamentales de la misma.

El derecho a la protección de datos personales ha adquirido una relevancia significativa como un derecho fundamental, tanto a nivel nacional como internacional. Este reconocimiento y alcance están respaldados por diversos instrumentos legales, tanto en Europa como en España, que garantizan la salvaguardia de la privacidad y la autonomía de las personas en relación con el tratamiento de sus datos personales.

En el ámbito europeo, este derecho, aunque no está explícitamente mencionado en el artículo 8 del Convenio Europeo de Derechos Humanos[1] (en lo sucesivo, CEDH), se considera implícito en el derecho al respeto de la vida privada y familiar, y, por consiguiente, sirve como uno de los marcos fundamentales para la protección y el desarrollo de los derechos humanos y las libertades fundamentales.[2]

El Tribunal Europeo de Derecho Humanos (en adelante, TEDH) ha reiterado en varias ocasiones su posición sobre la protección de datos personales, afirmando que esta

[1] Cfr. Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales firmado en Roma el 4 de noviembre de 1950.
[2] Vid. SOBRINO GARCÍA, I. (2019). "Protección de datos y privacidad. Estudio comparado del concepto y desarrollo entre la Unión Europea y Estados Unidos". Revista de Derecho UNED, núm. 25, p. 691.

cuestión se encuentra intrínsecamente ligada al derecho a la vida privada y familiar consagrado en el artículo 8 del CEDH. A través de sus sentencias, el TEDH ha enfatizado que la protección de la información personal no sólo protege la privacidad de las personas, sino que también garantiza el pleno ejercicio de sus derechos fundamentales en una sociedad democrática. Por lo tanto, al reconocer la estrecha relación entre la protección de datos y la vida privada, el Tribunal ha contribuido significativamente a fortalecer el marco legal que promueve la dignidad humana y el respeto a la autonomía individual en el ámbito digital y más allá.[3]

La Carta de los Derechos Fundamentales de la Unión Europea[4] (de ahora en adelante, CDFUE) afirma en su artículo 8 la importancia de salvaguardar la información personal de los individuos. De manera similar, el Tratado de Funcionamiento de la Unión Europea[5] (en adelante, TFUE), en su artículo 16, respalda y asegura esta prerrogativa, definiendo las responsabilidades de la Unión Europea (en lo sucesivo, UE) y los países que la conforman en materia de protección de datos personales.

En el ámbito nacional, la Constitución Española de 1978[6] (más adelante, CE), en su artículo 18.4, no hace referencia expresamente a la protección de datos personales, pero sí implícitamente a la protección contra amenazas contra la dignidad, identidad, libertad y privacidad de las personas, un marco que se ha desarrollado a través de diversas leyes orgánicas y reglamentos específicos. La Ley Orgánica 5/1992[7] (seguidamente, LORTAD), aunque posteriormente fue derogada, se trataba del primer intento legislativo de regular el tratamiento automatizado de datos personales en España. La Ley Orgánica de Protección de Datos de Carácter Personal[8] (desde ahora, LOPD) la sustituyó para transponer la Directiva 95/46/CE[9], que establecía normas para la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre

[3] Cfr. STEDH 28341/1995, de 4 de mayo de 2000, Caso Rotaru vs. Rumania, ap. 43.

[4] Carta de los Derechos Fundamentales de la Unión Europea. *DOUE, C202/389*, de 7 de junio de 2016.

[5] Tratado de Funcionamiento de la Unión Europea. *DOUE, C202/1*, de 7 de junio de 2017.

[6] Constitución Española. *BOE, núm. 311*, de 29 de diciembre de 1978.

[7] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. *BOE, núm. 262*, de 31 de octubre de 1992.

[8] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *BOE, núm. 298*, de 14 de diciembre de 1999.

[9] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *DOUE, L 281*, de 23 de noviembre de 1995.

circulación de estos. El Reglamento de desarrollo de la LOPD[10] detalla las medidas y procedimientos de la implementación de la LOPD. Con la entrada en vigor del Reglamento (UE) 2016/679 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 (más adelante, RGDP)[11], aplicable desde el 25 de mayo de 2018, se establecieron normas uniformes en toda la Unión Europea (en adelante, UE) para la protección de datos personales. Finalmente, la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales[12] (en lo sucesivo, LOPDGDD) alinea la legislación española con el RGPD y profundiza en este derecho, definiendo los principios y directrices para el manejo de la información personal en España y los derechos de los individuos en cuanto a su protección.[13]

El Tribunal Constitucional (en adelante, TC) ha establecido con claridad la autonomía del derecho fundamental a la protección de datos en relación con el derecho a la intimidad, destacando sus distintas funciones y alcances. Según el TC en la sentencia 292/2000[14], el derecho a la intimidad protege la vida personal y familiar de cualquier intrusión no deseada, excluyendo ciertos datos del conocimiento ajeno y salvaguardando la privacidad frente a la publicidad no deseada. En contraste, el derecho a la protección de datos tiene un alcance más amplio y específico, otorgando a la persona un control efectivo sobre sus datos personales mediante la regulación de su recopilación, uso y destino para prevenir el tráfico ilegal y garantizar el respeto a la dignidad y los derechos individuales. Este derecho abarca no sólo los datos íntimos, sino cualquier tipo de información personal que pueda afectar los derechos de la persona, sean o no fundamentales, permitiendo al titular ejercer facultades como el consentimiento previo para la recopilación y uso de datos, el derecho a ser informado sobre el destino y uso de

[10] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. *BOE, núm. 17*, de 19 de enero de 2008.

[11] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. *DOUE, L 119/1*, de 4 de mayo de 2016.

[12] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *BOE, núm. 294*, de 06 de diciembre de 2018.

[13] Vid. PÉREZ ESTRADA, M. J. (2019). "La protección de datos personales en el registro de dispositivos de almacenamiento masivo de información". Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, pp. 1301-1302. Véase en https://doi.org/10.22197/rbdpp.v5i3.253

[14] Cfr. STC (Pleno) 292/2000, de 30 de noviembre de 2010.

estos, y el derecho a acceder, rectificar y cancelar dicha información. En suma, el derecho a la protección de datos se distingue por el hecho de que otorga a los individuos un control activo sobre sus datos personales imponiendo obligaciones legales a terceros, diferenciándose significativamente del derecho a la intimidad, que se orienta más a proteger el ámbito de la vida personal frente a intrusiones.[15]

Aunque el derecho fundamental a la protección de datos personales tiene una gran relevancia, no es absoluto y puede verse limitado en determinadas circunstancias, tal y como prevé la CE y la jurisprudencia del TC. El artículo 10.1 de la CE señala que los derechos fundamentales deben ejercerse en el marco del orden público y la paz social, lo que implica que estos derechos puedan ser restringidos en aras de mantener la seguridad pública. Además, el TC reconoce que este derecho pueda limitarse para la investigación, persecución y sanción de los delitos[16], siempre que se respete su contenido esencial y se garantice su proporcionalidad. Asimismo, cualquier limitación debe ser compatible con otros derechos fundamentales y bienes jurídicos protegidos constitucionalmente[17], lo que implica un equilibrio entre ellos para evitar vulneraciones desproporcionadas.[18] Del mismo modo, en el contexto de la actividad procesal es posible vulnerar legítimamente derechos fundamentales no absolutos, como el derecho a la intimidad y el secreto de las comunicaciones, siempre que existan garantías como la intervención judicial, motivación y proporcionalidad.[19]

En consecuencia, es evidente que este derecho puede estar sujeto a límites, debiendo cumplir dos requisitos fundamentales para cualquier intervención estatal: en primer lugar, debe tener un fin constitucionalmente legítimo o dirigirse a proteger un bien relevante

---

[15] Vid. ESPARZA LEIBAR, I. (2018). "Protección de datos de carácter personal y proceso penal". En ETXEBARRIA ESTANKONA, K., ORDEÑANA GEZURAGA, I., y OTAZUA ZABALA, G. (Dirs), *Justicia con ojos de mujer. Cuestiones procesales controvertidas*, Editorial Tirant lo Blanch, pp. 931-932.

[16] Esta premisa es rememorada por la STC (Pleno) 292/2000, de 30 de noviembre de 2010 en su FJ 9: "En cuanto a los límites de este derecho fundamental no estará de más recordar que la Constitución menciona en el art. 105 b) que la ley regulará el acceso a los archivos y registros administrativos "salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas" (en relación con el art. 8.1 y 18.1 y 4 CE) …".

[17] Así lo refleja la STC (Pleno) 292/2000, de 30 de noviembre de 2010 en su FJ 11: "...este Tribunal ha declarado que el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución…".

[18] Vid. PÉREZ ESTRADA, M. J. (2019). "La protección de datos personales…", *op. cit.,* p. 1303.

[19] Vid. ESPARZA LEIBAR, I. (2018). "Protección de datos…", *op., cit.,* p. 932.

según la CE y, en segundo lugar, toda intervención estatal en este ámbito debe estar respaldada por una habilitación legal, es decir, debe estar definida por ley. Para garantizar el principio de seguridad jurídica, la ley que establece los límites al derecho a la protección de datos debe cumplir con dos exigencias principales: previsibilidad y certeza. Esto implica que las medidas restrictivas deben ser previsibles, permitiendo a los individuos anticipar las circunstancias en las que su derecho puede ser limitado. Además, estas medidas deben ser claras y específicas, proporcionando garantías mínimas adecuadas para asegurar que el límite al derecho no menoscabe su contenido esencial.[20]

En el ámbito del derecho procesal penal, el derecho a la protección de datos adquiere una significativa relevancia, ya que se debe armonizar la efectividad de las investigaciones criminales con el respeto a la intimidad y privacidad de los individuos. Es esencial que las transferencias de datos personales por los operadores de servicios de telecomunicaciones a las autoridades para fines de investigación criminal se realicen dentro de los límites legales, asegurando el pleno respeto a los derechos fundamentales de las personas afectadas. Este proceso debe llevarse a cabo bajo la supervisión de las autoridades competentes y conforme a los procedimientos establecidos por la ley.

2.2 Importancia de la protección de datos en la sociedad actual

En la era digital moderna, el derecho a la protección de datos personales emerge como un pilar fundamental para salvaguardar la privacidad y la autonomía individual en un mundo cada vez más interconectado. Este derecho, consagrado en numerosos marcos legales nacionales e internacionales, reconoce la importancia de resguardar la información personal de los individuos frente a posibles abusos por parte de entidades públicas y privadas.

En la sociedad actual, caracterizada por los vertiginosos avances de la tecnología y la omnipresencia de los medios digitales, la protección de datos es de suma importancia. El crecimiento exponencial de la recopilación, almacenamiento y procesamiento de información personal, facilitado por la digitalización y la interconexión de sistemas, plantea nuevos desafíos de seguridad y privacidad.

[20] Vid. PIÑAR MAÑAS, J. L. (2020). "Derecho e innovación. Privacidad y otros derechos en la sociedad digital". En CASAS BAAMONDE, M. E. (Coord), *El derecho a la protección de datos personales en la sociedad digital*, Fundación Ramón Areces, p. 49.

Los datos personales se han convertido en un recurso invaluable para muchas entidades, desde empresas y organizaciones gubernamentales hasta plataformas de redes sociales y proveedores de servicios en línea. Esta gran cantidad de datos, desde información básica como nombres y direcciones hasta detalles más sensibles como preferencias personales e historiales médicos, representa un poderoso potencial para el análisis, la segmentación y la manipulación.

En este contexto, la protección de datos surge como un escudo protector contra posibles abusos y violaciones de la privacidad. Garantizar la confidencialidad, integridad y disponibilidad de la información personal se convierte en una prioridad tanto para los individuos como para las instituciones encargadas de regular y supervisar el uso de los datos.

La importancia de la protección de datos en la sociedad actual radica en su capacidad para preservar la dignidad humana, el libre desarrollo de la personalidad y otros derechos fundamentales consagrados en la legislación nacional e internacional. Al salvaguardar la privacidad y la autonomía de los individuos, se promueve una sociedad más justa, equitativa y democrática, donde los ciudadanos puedan ejercer plenamente su libertad y autonomía sin temor a la vigilancia indebida o la manipulación injusta.

Finalmente, la protección de datos no sólo se erige como un derecho fundamental en la era de la conservación y cesión de datos personales, sino también como un pilar esencial para el desarrollo sostenible y ético de la sociedad digital del siglo XXI. Su aplicación efectiva requiere un enfoque multidimensional que engloba desde el desarrollo de políticas y regulaciones hasta la implementación de medidas técnicas y educativas para promover una cultura de privacidad y seguridad en línea.

3. MARCO JURÍDICO SOBRE PROTECCIÓN DE DATOS: SALVAGUARDIAS DE LA CONSERVACIÓN Y CESIÓN DE DATOS

3.1 Legislación europea

La normativa europea en materia de protección de datos está diseñada para garantizar la seguridad y la privacidad de los datos personales de los ciudadanos de la UE. Las principales legislaciones incluyen el Reglamento general de protección de datos, la Directiva *ePrivacy,* la Directiva sobre la conservación de datos y la Directiva de protección de datos en el ámbito penal.

Antes de adentrarnos en los detalles de estas normativas y sus implicaciones, es importante mencionar la Directiva (UE) 2023/1544[21], que debe estar transpuesta a la legislación nacional a más tardar el 18 de febrero de 2026, y el Reglamento (UE) 2023/1543[22], que será aplicable a partir del 18 de agosto de 2026. Estos dos instrumentos legales están interconectados y forman parte del marco legal establecido por la UE para regular la obtención y conservación de pruebas electrónicas en procesos penales. Por un lado, esta Directiva establece normas armonizadas con el fin de recabar pruebas electrónicas en procesos penales. Por otro lado, este Reglamento introduce órdenes europeas de producción y conservación para la obtención de pruebas electrónicas de manera eficiente, garantizando al mismo tiempo el respeto de los derechos fundamentales.

3.1.1 Reglamento General de Protección de Datos

La principal normativa europea en materia de protección de datos es el RGPD. Este Reglamento tiene como objetivo principal fortalecer y unificar la protección de los datos personales de los individuos dentro de la UE, así como regular el flujo de datos personales fuera de la UE.

El RGPD establece una serie de principios para el tratamiento de datos personales que deben ser cumplidos por aquellos que procesan dichos datos, los cuales incluyen: el principio de licitud, lealtad y transparencia, en los que los datos deben procesarse de manera lícita, leal y transparente para el interesado; el principio de limitación de la finalidad, que exige que los datos se recopilen para fines específicos, explícitos y legítimos, sin ser tratados de forma incompatible con esos fines; el principio de minimización de datos, que exige que los datos sean adecuados, pertinentes y limitados a lo necesario para los fines para los que son tratados; el principio de exactitud, que establece que los datos deben ser exactos y actualizados, con medidas para rectificar o suprimir los datos inexactos; el principio de limitación del plazo de conservación, que indica que los datos deben conservarse durante el tiempo necesario para los fines del tratamiento; y el principio de integridad y confidencialidad, que garantiza una seguridad

[21] Directiva (UE) 2023/1544 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales. *DOUE, L 191/181,* de 28 de julio de 2023.

[22] Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales. *DOUE, L 191/118,* de 28 de julio de 2023.

adecuada en el tratamiento de los datos, protegiéndolos contra el acceso no autorizado o ilícito, pérdida, destrucción o daño por accidente, mediante medidas técnicas u organizativas apropiadas (artículo 5).

Además, el RGPD reconoce ciertos derechos a aquellas personas cuyos datos son tratados. Estos derechos incluyen el derecho de acceso, mediante el cual los individuos pueden obtener del responsable del tratamiento la confirmación sobre si se están procesando o no datos personales que les conciernen, y en tal caso, acceso a dichos datos y a cierta información adicional; el derecho de rectificación que permite a los individuos obtener la corrección de los datos personales inexactos que les conciernen; el derecho de supresión, también conocido como "derecho al olvido", otorga a los individuos el derecho a obtener del responsable del tratamiento la eliminación de los datos personales que les conciernen en determinadas circunstancias; el derecho de oposición, que permite que los individuos oponerse en cualquier momento, por motivos relacionados con su situación particular, al tratamiento de los datos personales que les conciernen; y el derecho a la portabilidad de datos, que establece que los individuos tienen derecho a recibir datos personales que les conciernen en un formato estructurado, de uso común y lectura mecánica, y a transmitir estos datos a otro responsable del tratamiento sin interferencia por parte del responsable al que los proporcionó (artículos 15 al 21).

En relación con la conservación de datos, el RGPD estipula que los datos personales deben conservarse de forma que no se pueda identificar a los interesados durante más tiempo del necesario. Esto implica que los datos sólo podrán conservarse durante el plazo necesario para la finalidad perseguida y, una vez transcurrido este plazo, durante los períodos legales de prescripción. Aunque el RGPD no específica plazos concretos, se requiere que los períodos de conservación sean estrictamente necesarios para cumplir con la finalidad para la que se recopilaron los datos personales (artículo 5.1.e).

En torno a la cesión de datos, el RGPD hace una distinción entre la transferencia de datos personales a terceros dentro y fuera de la UE. Las transferencias de datos dentro de la UE generalmente están permitidas sin restricciones adicionales, siempre que se respeten los principios de protección de datos del RGPD. Sin embargo, las transferencias de datos a terceros países fuera de la UE están sujetas a restricciones específicas para garantizar un nivel adecuado de protección de datos, como las Cláusulas Contractuales Estándar o los Mecanismos de Certificación. Además, la Decisión de Adecuación de la

Comisión Europea puede permitir transferencias a países que se considere que tienen un nivel adecuado de protección de datos (artículos 42 al 49).

En España, el RGPD se ha implementado a través de la LOPDGDD. Esta ley, como veremos más adelante, complementa y desarrolla las disposiciones del RGPD y establece reglas específicas para la protección de datos en el ámbito nacional.

3.1.2 Directiva *ePrivacy*

La Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[23] (Directiva sobre la privacidad y las comunicaciones electrónicas), también conocida como la Directiva *ePrivacy*, es una normativa de la UE que regula aspectos específicos de la protección de datos personales y la privacidad en el ámbito de las comunicaciones electrónicas. Esta legislación abarca una serie de disposiciones que buscan salvaguardar la confidencialidad de las comunicaciones y proteger la privacidad de los usuarios de servicios de telecomunicaciones.

La Directiva *ePrivacy* establece medidas para salvaguardar la confidencialidad de las comunicaciones electrónicas, como el correo electrónico y las llamadas telefónicas. Prohíbe cualquier interceptación o vigilancia no autorizada, excepto de determinadas circunstancias y se implementen salvaguardias adecuadas (artículo 5).

En cuanto a la seguridad de los datos, esta Directiva exige que los proveedores de servicios de comunicaciones electrónicas implementen medidas técnicas y organizativas apropiadas. Estas medidas tienen como objetivo garantizar la seguridad de los datos personales tratados, protegiéndolos de accesos no autorizados o cualquier forma de manipulación indebida (artículo 4).

Aunque la Directiva *ePrivacy* no aborda directamente la conservación y cesión de datos en el mismo sentido que el RGPD, si contiene disposiciones que afectan indirectamente a estos aspectos. En cuanto a la conservación de datos, establece que los datos de tráfico deben ser eliminados o anonimizados tan pronto como ya no sean necesarios para la transmisión de comunicaciones, permitiendo su conservación

[23] 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). *DOUE, L 201*, de 31 de julio de 2002.

únicamente para la facturación o los pagos de conexión hasta que se resuelvan las controversias relacionadas. Además, los Estados miembros pueden autorizar la conservación de datos por un período limitado, siempre que sea necesario y proporcionado, para garantizar la seguridad nacional, la defensa, la seguridad pública, o la prevención, investigación, detección y enjuiciamiento de delitos graves. Respecto a la cesión de datos, la Directiva *ePrivacy* garantiza la confidencialidad de las comunicaciones y prohíbe cualquier tipo de interceptación o vigilancia sin el consentimiento del usuario, salvo autorización legal. Asimismo, establece que la cesión de datos a terceros sólo será posible con el consentimiento explícito del usuario o cuando sea necesaria para cumplimiento de una obligación. De manera que los Estados miembros pueden introducir excepciones para la cesión de datos sin consentimiento de los usuarios en casos de protección de la seguridad nacional, la defensa, la seguridad pública, y la prevención, investigación, detección y enjuiciamiento de delitos graves, siempre que estas excepciones sean necesarias, proporcionadas y estén sujetas a salvaguardias adecuadas para proteger los derechos fundamentales (artículos 5, 6 y 15).

3.1.3 Directiva sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones

La Directiva 2006/24/CE sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones[24] (en lo sucesivo, DCD) requería que los datos relacionados con el tráfico y la localización producidos por el uso de dichos servicios fueran almacenados durante un lapso específico para asegurar que estuvieran disponibles para la investigación y procesamiento de delitos graves.

El principal objetivo de la DCD era armonizar las obligaciones de los proveedores de servicios de comunicaciones electrónicas y redes públicas en relación con la conservación de ciertos datos generados o procesados por ellos, con miras a garantizar que esos datos estén disponibles para la investigación, detección y enjuiciamiento de delitos graves (artículo 1.1).

[24] Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. *DOUE, L 105/54,* de 13 de abril de 2006.

La DCD se aplicaba a los proveedores de servicios públicos de comunicaciones electrónicas y a los proveedores de redes públicas de comunicaciones. Esto incluía a operadores de telefonía fija y móvil, proveedores de servicios de Internet, y proveedores de servicios de correo electrónico. Todos estos proveedores estaban obligados a conservar determinados datos generados o procesados como parte de sus servicios.

A su vez, la DCD especificaba ciertos tipos de datos que debían ser conservados, necesarios para rastrear y localizar la fuente, el destino, la fecha, la hora, la duración, el tipo de comunicación y el equipo de comunicación utilizado, así como la localización del equipo de comunicación móvil. Estos datos incluían información sobre el abonado o usuario registrado, el número de teléfono de origen, el nombre y dirección del abonado o usuario registrado, el número marcado y el nombre y dirección del abonado o usuario registrado del número marcado. Además, era obligatorio conservar la fecha y hora de inicio y finalización de la llamada para servicios de telefonía, la fecha y hora de la conexión y desconexión del servicio de acceso a Internet, la información sobre el tipo de servicio de comunicación utilizado (como llamadas de voz o mensajes de textos), los datos de identidad internacional del equipo móvil (IMEI, del inglés *International Mobile Equipment Identity*), el identificador del equipo terminal fijo, el identificador de celda al inicio de la comunicación y los datos de geolocalización de las celdas utilizadas durante la comunicación (artículo 5).

Además, la DCD establecía que los datos debían conservarse por un período mínimo de seis meses y un máximo de dos años a partir de la fecha de la comunicación, siendo facultad de cada Estado miembro determinar el período exacto dentro de este rango (artículo 6).

Asimismo, la DCD estipulaba que sólo las autoridades nacionales competentes podrían acceder a los datos conservados y sólo para fines específicos relacionados con la investigación, detección y enjuiciamiento de delitos graves. Por lo que, el procedimiento para acceder a estos datos debía estar claramente definidos de acuerdo con la legislación nacional de cada Estado miembro, asegurando que dicho acceso estuviera sujeto a salvaguardias adecuadas (artículo 4).

Al mismo tiempo, la DCD incorporaba que los proveedores de servicios estaban obligados a implementar medidas técnicas y organizativas adecuadas para proteger los datos contra la destrucción accidental o ilegal, la pérdida accidental, la alteración, la

divulgación o el acceso no autorizado. Estas medidas debían garantizar que los datos sólo se conservaran durante el período necesario y fueran destruidos al final de este período. Además, los proveedores debían asegurar que los datos se utilizaran para los fines específicos definidos por la directiva y la legislación nacional (artículo 7).

La incorporación de la DCD al marco jurídico español se efectuó mediante la promulgación de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones[25] (en adelante, LCDCE). Dicha legislación dicta las responsabilidades de los operadores de servicios de telecomunicaciones en el país, quienes deben proporcionar a las autoridades competentes acceso a determinados datos de tráfico y localización para su preservación.

3.1.3.1 La invalidez de la Directiva

La DCD fue objeto de muchas críticas y desafíos legales debido a las preocupaciones sobre la privacidad y los derechos fundamentales. Por ello se argumentaba que la conservación masiva de datos infringía los derechos de los individuos relativos a la privacidad y la protección de datos.

La DCD, concebida como respuesta a los atentados terroristas en Madrid (2004) y Londres (2005)[26], con el objetivo de mejorar la seguridad mediante la conservación de datos generados o tratados en relación con los servicios de comunicaciones electrónicas de acceso público. Esta normativa, como se ha mencionado previamente, requería que los proveedores de servicios de comunicaciones conservaran datos de tráfico y localización, así como información de identificación del usuario para facilitar la prevención, investigación, detección y persecución de delitos graves como el terrorismo y la delincuencia organizada.[27]

---

[25] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. *BOE, núm. 251*, de 19 de octubre de 2010.

[26] Según lo establecido en la Declaración sobre la lucha contra el terrorismo, emitida por el Consejo Europeo el 25 de marzo de 2004, y reflejado en el Considerando 8 de la DCD, surgió la necesidad de que el Consejo examinara las medidas para establecer regulaciones sobre la conservación de datos de tráfico de comunicaciones por parte de los proveedores de servicios de telecomunicaciones.

[27] Cfr. STJUE (Gran Sala) de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12. Además, véase SOBRINO GARCÍA, I. (2019). "Protección de datos y privacidad…", *op. cit*., pp. 701-703; LÓPEZ AGUILAR, J. F. (2017). "La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EUUU". UNED, Teoría y Realidad Constitucional, núm. 39, pp. 574-575; ETXEBERRIA GURIDI, J. F. (2015). "La invalidez de la Directiva 2006/24/CE y su repercusión en el ordenamiento español (consecuencias de la STJUE de 8 de abril de 2014". En GÓMEZ COLOMER, J., *El*

La sentencia del TJUE emitida el 8 de abril de 2014, en el caso Digital Rights[28], marcó un hito crucial al declarar la invalidez de la DCD. Esta decisión se basó en la incompatibilidad de la DCD con los derechos fundamentales protegidos por la CDFUE, en particular en los artículos 7 y 8, y los principios establecidos en los artículos 51 a 54 de la misma Carta, especialmente el artículo 52, que establece el principio de proporcionalidad.[29]

Las solicitudes prejudiciales planteadas por la High Court de Irlanda y el Tribunal Constitucional Austriaco pedían al TJUE que examinara la validez de la Directiva en virtud del Tratado de la UE (TUE) y la CDFUE, especialmente en relación con el respecto a la vida privada, la protección de datos personales y la libertad de expresión de comunicación.[30]

El TJUE, en su análisis, determinó que la DCD imponía una injerencia amplia y particularmente grave en los derechos fundamentales al respecto de la vida privada (artículo 7 de la CDFUE) y a la protección de los datos personales (artículo 8 de la CDFUE). Esta conclusión se basó en varios aspectos de la Directiva:

1. Gravedad de la injerencia: En los apartados 65 a 68, el Tribunal sostuvo que la DCD permitía la identificación detallada de las comunicaciones de las personas, incluidas aquellas con las que han estado en contacto, los medios utilizados, la frecuencia y la duración de las comunicaciones, así como la localización de los usuarios. Esta información podría revelar patrones precisos de la vida privada de

---

proceso penal en la encrucijada, Universitat Jaume I, pp. 543-546.; POLO ROCA, A. (2021). "La regulación sobre la conservación de datos en el sector de las comunicaciones electrónicas o telecomunicaciones: estado de la cuestión". IDP. Revista de Internet, Derecho y Política, Nº. 33, pp. 5-7. Véase en http://dx.doi.org/10.7238/idp.v0i33.373811; GONZÁLEZ CANO, M. I. (2019). "Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680". Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, pp. 1343-1346. Véase en https://doi.org/10.22197/rbdpp.v5i3.279

[28] Cfr. STJUE (Gran Sala) de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12.

[29] Vid. SOBRINO GARCÍA, I. (2019). "Protección de datos y privacidad…", *op. cit.*, pp. 701-703; LÓPEZ AGUILAR, J. F. (2017). "La protección de datos personales en la más reciente jurisprudencia del TJUE…", *op. cit.*, pp. 574-575; ETXEBERRIA GURIDI, J. F. (2015). "La invalidez de la Directiva 2006/24/CE…", *op. cit.*, pp. 543-546; POLO ROCA, A. (2021). "La regulación sobre la conservación de datos…", *op. cit.*, pp. 5-7; GONZÁLEZ CANO, M. I. (2019). "Cesión y tratamiento de datos personales en el proceso penal…", *op. cit.*, pp. 1343-1346.

[30] Vid. SOBRINO GARCÍA, I. (2019). "Protección de datos y privacidad…", *op. cit.*, pp. 701-703; LÓPEZ AGUILAR, J. F. (2017). "La protección de datos personales en la más reciente jurisprudencia del TJUE…", *op. cit.*, pp. 574-575; ETXEBERRIA GURIDI, J. F. (2015). "La invalidez de la Directiva 2006/24/CE…", *op. cit.*, pp. 543-546; POLO ROCA, A. (2021). "La regulación sobre la conservación de datos…", *op. cit.*, pp. 5-7; GONZÁLEZ CANO, M. I. (2019). "Cesión y tratamiento de datos personales en el proceso penal…", *op. cit.*, pp. 1343-1346.

los individuos, incluyendo sus hábitos, los lugares visitados y las relaciones sociales (STJUE de 8 de abril de 2014).

2. Falta de criterios claros y objetivos: En los apartados 56 a 62, el TJUE señaló que la Directiva carecía de claridad y precisión para determinar el acceso y uso de los datos por parte de las autoridades nacionales. Esta falta de regulación ha permitido un acceso generalizado sin un control adecuado, lo que generaba una injerencia desproporcionada y sin garantías adecuadas en los derechos fundamentales de los individuos (STJUE de 8 de abril de 2014).

3. Protección y seguridad de los datos: En los apartados 66 y 67, el Tribunal observó que la DCD no garantizaba un nivel suficientemente alto de protección y seguridad para los datos almacenados. No contenía normas claras para asegurar que los datos se trataran de forma segura y que sólo las personas autorizadas tuvieran acceso a ellos, lo que aumentaba el riesgo de abuso y acceso no autorizado (STJUE de 8 de abril de 2014).

4. Proporcionalidad de la medida: En los apartados 51 y 54, el TJUE cuestionó la proporcionalidad de la medida, argumentando que la conservación generalizada de datos no era necesaria para combatir el terrorismo y otros delitos graves. La Directiva era demasiado amplia y no distinguía entre diferentes tipos de datos o personas, afectando indiscriminadamente a todos los usuarios (STJUE de 8 de abril de 2014).

El TJUE concluyó que la DCD no cumplía con los principios de necesidad y proporcionalidad exigidos por el artículo 52 de la CDFUE (STJUE de 8 de abril de 2014). La medida aplicaba de manera indiscriminada a todas las personas, medios de comunicación electrónica y datos susceptibles de tráfico, sin diferenciar ni establecer limitaciones en función del objetivo de seguridad proclamado. Además, no establecía criterios de delimitación del propósito, permitiendo el acceso a los datos personales sólo con el objetivo lícito de prevenir, detectar o reprimir delitos graves. Tampoco contenía ninguna limitación espacial dentro del territorio de la UE y el período de conservación de datos, entre 6 y 24 meses, no estaba justificado en relación con la utilidad específica de los datos a los efectos de la Directiva.

La decisión del TJUE subrayó la importancia de respetar los principios de necesidad y proporcionalidad al legislar sobre la conservación de datos, estableciendo un precedente significativo para la protección de los derechos fundamentales en la legislación de la UE. Además, el fallo del Tribunal dejó claro que cualquier excepción a la confidencialidad de las comunicaciones debe interpretarse de manera restrictiva, subrayando la necesidad de cerrar la brecha de confianza entre la UE y sus ciudadanos en cuanto a la protección de datos personales. De manera que, tras la invalidación de la DCD, cada Estado miembro se vio obligado revisar y ajustar su marco jurídico para cumplir con los principios establecidos por el Tribunal lo que implicó la necesidad de implementar medidas de conservación de datos que fueran proporcionadas, específicas y limitadas, garantizando la protección de los derechos fundamentales de los ciudadanos europeos.[31]

En la normativa española sobre la conservación de datos de comunicaciones electrónicas esta STJUE de 8 de abril de 2014 tuvo un impacto significativo. En este sentido, la normativa española se ha ajustado en respuesta a la sentencia, que busca equilibrar la lucha contra la delincuencia con la protección de los derechos fundamentales. En cuanto a la conservación de datos, se ha mantenido un plazo máximo de 12 meses, pero se han establecido mecanismos más claros para ampliar este plazo a dos años, exigir motivos concretos y limitar los casos en los que puede aplicarse este plazo. Además, se han introducido garantías más sólidas para la destrucción definitiva de los datos una vez concluido el período de conservación. En relación con el acceso o cesión de datos, se han reforzado las restricciones de acceso por parte de autoridades específicas y se ha establecido controles más estrictos, incluyendo una autorización judicial previa detallada y fundamentada. Estas modificaciones buscan cumplir con las exigencias del TJUE y garantizar una mayor protección de los datos personales de los individuos.[32]

En última instancia, la sentencia del TJUE ha planteado desafíos y perspectivas futuras en cuanto al diseño de un nuevo sistema de conservación de datos compatible con la CDFUE. Si bien esta es una oportunidad para encontrar un equilibrio adecuado entre

[31] Vid. SOBRINO GARCÍA, I. (2019). "Protección de datos y privacidad…", *op. cit.*, pp. 701-703; LÓPEZ AGUILAR, J. F. (2017). "La protección de datos personales en la más reciente jurisprudencia del TJUE…", *op. cit.*, pp. 574-575; ETXEBERRIA GURIDI, J. F. (2015). "La invalidez de la Directiva 2006/24/CE…", *op. cit.*, pp. 543-546; POLO ROCA, A. (2021). "La regulación sobre la conservación de datos…", *op. cit.*, pp. 5-7; GONZÁLEZ CANO, M. I. (2019). "Cesión y tratamiento de datos personales en el proceso penal…", *op. cit.*, pp. 1343-1346.

[32] Vid. ETXEBERRIA GURIDI, J. F. (2015). "La invalidez de la Directiva 2006/24/CE…", *op. cit.*, pp. 542-559.

la seguridad pública y la protección de los derechos fundamentales, sigue siendo un desafío complejo para los legisladores europeos. Los futuros marcos legales deberán considerar cuidadosamente las garantías necesarias para proteger los derechos fundamentales y al mismo tiempo permitir la recopilación de datos necesarios para combatir los delitos graves.

3.1.4 Directiva de protección de datos en el ámbito penal

La Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016[33] (en lo sucesivo, Directiva (UE) 2016/680), se refiere a la protección de datos personales en el ámbito de la prevención, investigación, detección y enjuiciamiento de infracciones penales, así como de la ejecución de sanciones penales.

La Directiva (UE) 2016/680 establece normas para proteger los datos personales tratados por las autoridades competentes en el ámbito penal, abarcando en la prevención, investigación, detección o enjuiciamiento de infracciones penales, así como para la aplicación de sanciones penales, incluida la protección y prevención de amenazas a la seguridad pública (artículo 1). Los Estados miembros deben proteger los derechos fundamentales de los individuos, incluido su derecho a la protección de datos, y garantizar que el intercambio de datos dentro de la UE no se limite ni prohíba sin razón justificada. Además, la Directiva permite a los Estados miembros ofrecer mayores garantías para la protección de los derechos del interesado si así lo desean.

Además, La Directiva (UE) 2016/680 instaura una serie de principios fundamentales que los Estados miembros deben garantizar para el tratamiento de los datos personales (artículo 4). En primer lugar, los datos deben ser tratados de manera lícita y leal, cumpliendo con la legislación pertinente y sin infringir los derechos individuales, además de ser recopilados con fines específicos, explícitos y legítimos, asegurando que no se utilicen de manera incompatible con estos objetivos y que sólo se recopilen los datos necesarios. Se permite el tratamiento de datos para fines distintos de los originales, siempre que sea necesario y proporcionado y que el responsable del tratamiento esté autorizado para hacerlo según la legislación vigente. Además, el tratamiento puede incluir

[33] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. *DOUE, L 119/89*, 4 de mayo de 2016.

el archivo en interés público y su uso para fines científicos, estadísticos o históricos, siempre y cuando se apliquen garantías para proteger los derechos de los interesados. Finalmente, el responsable del tratamiento debe demostrar el cumplimiento de estos principios, proporcionando evidencia de que cumple con los estándares de tratamiento de datos, incluyendo la legalidad, la precisión, la seguridad y el respeto de los derechos.

La Directiva (UE) 2016/680 no determina un plazo específico para la conservación de los datos personales (artículo 5). No obstante, establece la importancia de fijar plazos apropiados para la supresión de datos personales o para llevar a cabo revisiones periódicas sobre la necesidad de conservar dichos datos. Esta disposición busca garantizar que los datos personales no se conserven más tiempo del necesario para lograr el propósito para el que fueron recopilados, promoviendo así la gestión responsable de la información personal. Además, se establece que las normas del procedimiento deben asegurar el cumplimiento de estos plazos, lo que implica la implementación de mecanismos efectivos para controlar y asegurar el cumplimiento de los períodos de retención adecuados. Esta disposición refuerza la protección de la privacidad y los derechos de los individuos a la vez que promueve la eficiencia y la transparencia en el manejo de los datos personales por parte de las autoridades competentes en la UE.

España se enfrentó a graves consecuencias legales al incumplir el plazo establecido para la transposición de la Directiva (UE) 2016/680, convirtiéndose en el primer caso en que el TJUE[34] impone simultáneamente las dos sanciones previstas en el artículo 260 del TFUE: una multa coercitiva diaria de 89.000 € y una multa a tanto alzado de 15,5 millones de euros. El Tribunal criticó la pasividad de España, rechazando la justificación basada en la inestabilidad política del país durante ese período, y destacó la importancia de la Directiva para garantizar la protección de datos personales, fundamental en la UE. De manera que España fue condenada a pagar más de 20 millones de euros, incluyendo la multa coercitiva y la suma a tanto alzado, por un retraso de casi tres años en la transposición de la Directiva, que finalmente se llevó a cabo con la promulgación de la Ley Orgánica 7/2021 de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de

[34] Vid. STJUE (Sala Octava) de 25 de abril de 2021, asunto C-658/19.

sanciones penales[35] (en adelante, LO 7/2021). Este caso subraya la importancia de que los Estados miembros cumplan con sus obligaciones de transposición de la normativa europea dentro de los plazos establecidos para asegurar un marco jurídico homogéneo y efectivo en toda la UE, y la imposición de sanciones refleja la seriedad con la que se trata el cumplimiento de estas obligaciones, actuando como un poderoso incentivo para evitar futuros retrasos e incumplimientos.[36]

3.2 Legislación nacional

La normativa española sobre protección de datos comprende diversas leyes que abordan diversos aspectos relativos a la conservación y cesión de información personal. A continuación, se detallan las leyes más relevantes.

3.2.1 Ley Orgánica de protección de datos y garantías de los derechos digitales

La LOPDGDD es la principal normativa en España en materia de protección de datos personales. Esta ley complementa y desarrolla el RGPD en el ámbito nacional, estableciendo disposiciones específicas para garantizar la protección de la privacidad y los derechos de los ciudadanos en el entorno digital.

La LOPDGDD se aplica a cualquier tratamiento de datos personales, ya sea completo o parcial, así como al tratamiento no automatizado de datos personales que se encuentran o están destinados a estar en un fichero. Sin embargo, hay excepciones: no se aplican a los tratamientos excluidos por el artículo 2.2 del RGPD, como actividades de seguridad; a los datos de personas fallecidas, salvo las posibles excepciones del artículo 3 de la LOPDGDD; y a los tratamientos regulados por la normativa de protección de materias clasificadas. Los tratamientos no cubiertos directamente por el RGPD, por

[35] 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. *BOE, núm. 126,* de 27 de mayo de 2021.

[36] Vid. RODRÍGUEZ FERNÁNDEZ, R. (2022). "Protección de datos personales: normativa europea y nacional (especial referencia a la normativa de protección de datos en la prevención, detección, investigación y enjuiciamiento de infracciones penales)". La Ley Penal, Nº 157, Sección Legislación aplicada a la práctica, Julio-Agosto 2022, Editorial Wolters Kluwer; MARTÍNEZ VÁZQUEZ, F. (2021). "La nueva Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales". Diario La Ley Penal, Nº 9865, Sección Tribuna, 7 de Junio de 2021, Editorial Wolters Kluwer, p. 5; RODRÍGUEZ AYUSO, J. F. (2021). "Nueva regulación en el tratamiento de datos personales con fines públicos de prevención, detección, investigación, enjuiciamiento y ejecución de sanciones penales: la Ley 7/2021, de 26 de mayo". En PEREIRA PUIGVERT, S., y ORDÓÑEZ PONZ, F. (Dirs), *Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos,* Editorial Aranzadi, p. 655.

afectar actividades fuera del ámbito del Derecho de la UE (en adelante, DUE), se regirán por su legislación específica y supletoriamente por el RGPD y esta ley. Además, el RGPD y la presente ley se aplicarán al tratamiento de datos en procesos judiciales y a la gestión de la Oficina Judicial, sin perjuicio de la Ley Orgánica del Poder Judicial[37] (en lo sucesivo, LOPJ). De manera similar, el RGPD y esta ley se aplicarán al tratamiento de datos del Ministerio Fiscal durante sus procesos y en la gestión de la Oficina Fiscal, sin afectar la Ley del Estatuto Orgánico del Ministerio Fiscal[38], la LOPJ y las normas procesales aplicables (artículo 2).

La LOPDGDD, siguiendo la misma línea que el RGPD, establece varios principios fundamentales para la protección de datos. Estos incluyen el principio de exactitud de los datos, previsto en el artículo 4, establece que la información personal debe ser precisa y actualizada, eximiendo así de responsabilidad a los responsables del tratamiento si han tomado medidas para corregir posibles inexactitudes. El deber de confidencialidad, mencionado en el artículo 5, obliga a todos los responsables y encargados del tratamiento de datos a mantener la confidencialidad incluso después del final de la relación. El consentimiento del afectado, según el artículo 6, debe ser libre, específico, informado e inequívoco, y no puede vincularse a la ejecución de un contrato. En cuanto al tratamiento de datos de menores de edad, el artículo 7 instaura que su consentimiento es válido si tienen más de catorce años, salvo en casos en que la ley exija la asistencia de los titulares de la patria potestad o tutela. El tratamiento de datos por obligación legal, interés público o ejercicio de públicos, de acuerdo con el artículo 8, debe estar respaldado por normativas específicas de la UE o leyes nacionales. Las categorías especiales de datos, según el artículo 9, como la ideología o la orientación sexual, requieren medidas de seguridad adicionales y sólo pueden procesarse en situaciones excepcionales. Por último, el artículo 10 regula el tratamiento de datos de naturaleza penal, restringiendo su uso a casos expresamente autorizados por la ley y limitando su acceso a abogados y procuradores en el ejercicio de sus funciones. Estos principios proporcionan una base sólida para la protección de la privacidad y los derechos digitales en la gestión de datos personales.

Además, la LOPDGDD instaura los derechos de los titulares de los datos que constituyen un aspecto fundamental en la protección de la privacidad y el control sobre

[37] Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. *BOE, núm. 157*, de 02 de julio de 1985.
[38] Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal. *BOE, núm. 11*, de 13 de enero de 1982.

la información personal (artículos 13 a 18). El derecho de acceso brinda a los individuos la posibilidad de confirmar si sus datos personales están siendo tratados y, de ser así, acceder a ellos. A su vez, el derecho de rectificación permite corregir cualquier información personal inexacta que pueda existir. El derecho de supresión, también conocido como derecho al olvido, permite a los individuos solicitar la eliminación de sus datos personales en determinadas circunstancias. Por otro lado, el derecho a la limitación del tratamiento otorga a las personas la facultad de restringir el uso de sus datos en circunstancias específicas. El derecho a la portabilidad de los datos permite a los titulares recibir sus datos personales en un formato estructurado, de uso común y lectura mecánica, facilitando así la transferencia de los datos a otro responsable. Finalmente, el derecho de oposición otorga a los individuos el derecho de oponerse al tratamiento de sus datos personales en ciertas situaciones, proporcionando un mayor control sobre su información. Estos derechos son parte del marco legal que protege los derechos y libertades individuales en el tratamiento de datos.

3.2.2 Ley de conservación de datos en relación con las comunicaciones electrónicas

La Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones[39] (en adelante, LCDCE) es la normativa que tiene como objetivo principal la transposición de la DCD en el ordenamiento jurídico español.

La LCDCE obliga a los proveedores de servicios de comunicaciones electrónicas y redes públicas a almacenar determinados datos generados o tratados en el curso de la prestación de sus servicios (artículos 1 y 2). Así pues, la finalidad de esta ley es apoyar la investigación, detección y persecución de delitos graves, además de garantizar la seguridad nacional, facilitando el acceso de las autoridades competentes a los datos de las comunicaciones electrónicas mantenidas por estos proveedores.

Asimismo, la LCDCE, como examinaremos con mayor profundidad más adelante, establece los tipos de datos que deben conservarse, especificando que incluyen los datos relacionados con el tráfico, la localización y aquellos necesarios para identificar al usuario, excluyendo el contenido de las comunicaciones (artículo 3). En este sentido, es importante destacar que la LCDCE introduce cambios significativos en el concepto de datos, abandonando la noción tradicional de "datos de tráfico" en favor de una definición

[39] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. *BOE, núm. 251,* de 19 de octubre de 2010.

más general y completa. Este cambio se refleja en dos aspectos principales: en primer lugar, la ampliación del concepto de datos incluye los datos de tráfico generados durante la comunicación y los almacenados como datos personales, así como datos adicionales como la localización del usuario y detalles técnicos; y, en segundo lugar, la LCDCE procesa datos de tráfico y datos personales bajo una misma regulación legal, lo que implica que todos los datos, independientemente del tipo de datos, están sujetos a la misma disciplina jurídica. Esto tiene implicaciones legales importantes, ya que los datos recopilados pueden estar sujetos a diferentes regímenes legales dependiendo de sus orígenes, y el acceso a ellos está regulado por disposiciones de la LCDCE o por otras leyes aplicables, como la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal[40] (en lo sucesivo, LECrim) o la LGT.[41]

Según la LCDCE, la duración de la conservación de datos debe oscilar entre un período mínimo de seis meses y un máximo de dos años a partir de la fecha en que se haya realizado la comunicación (artículo 5). Este marco temporal se implementa para garantizar que los datos estén disponibles el tiempo necesario para cumplir con las obligaciones legales y de esta manera facilitar la investigación de posibles delitos, al tiempo que garantiza que los datos no se conservan indefinidamente, lo que puede afectar a la privacidad y los derechos de los usuarios.

El acceso a los datos conservados, como veremos más adelante a detalle, está estrictamente limitado a las autoridades competentes y debe realizarse de acuerdo con los procedimientos legales establecidos, garantizando que dicho acceso sea proporcional y necesario (artículo 6). Este acceso regulado asegura que sólo se utilice cuando sea necesario para la investigación, detección y persecución de delitos graves, así como para la protección de la seguridad nacional. Además, los procedimientos legales existentes están diseñados para proteger los derechos fundamentales y la privacidad de las personas, garantizando que cualquier solicitud de acceso a datos esté sujeta a una estricta revisión judicial. De esta manera, se mantiene un equilibrio entre las necesidades de seguridad

[40] Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica sobre las medidas de investigación limitativas de derechos constitucionales. *BOE, núm. 239*, de 6 de octubre de 2015

[41] Vid. RODRÍGUEZ LAINZ, J. L. (2016). "El secreto de las telecomunicaciones y su interceptación legal: adaptado a la Ley Orgánica 13/2015, de reforma de la Ley de Enjuiciamiento Criminal". Sepín, p. 291.

pública y la protección de las libertades individuales, permitiendo a las autoridades actuar con eficacia y dentro del marco de la ley.

Por otro lado, la LCDCE determina que los proveedores de servicios están obligados a implementar medidas técnicas y organizativas apropiadas para proteger los datos almacenados contra accesos no autorizados, alteraciones, divulgación o destrucción (artículo 8). Estas medidas de seguridad buscan garantizar la integridad y la confidencialidad de la información almacenada, salvaguardando así los derechos y la privacidad de los individuos.

Además, la LCDCE dispone, en los artículos 8.4 y 10, la implementación de mecanismos para velar por el cumplimiento de sus disposiciones, asignando esta responsabilidad a autoridades específicas como la Agencia Española de Protección de Datos (en lo sucesivo, AEPD). Estas entidades tienen la tarea de supervisar las actividades de los proveedores de servicios, asegurándose de que estos cumplan con las obligaciones establecidas en la ley respecto a la conservación de datos. En caso de incumplimiento, la normativa prevé la imposición de sanciones proporcionales a la gravedad de la infracción cometida por los proveedores de servicios, con el fin de garantizar el acatamiento de las disposiciones legales y proteger los derechos de los usuarios. Estas sanciones actúan como un mecanismo disuasorio y correctivo, incentivando el cumplimiento de la normativa establecida y promoviendo así el adecuado tratamiento de los datos por parte de los proveedores de servicios de comunicaciones electrónicas.

Es relevante considerar que esta ley ha sido objeto de controversias por diversas razones: se considera una intrusión significativa en la privacidad, ya que obliga a los proveedores a conservar datos de comunicaciones; la proporcionalidad y necesidad de la medida; la seguridad de los datos, dado el riesgo de acceso no autorizados, filtraciones y ataques cibernéticos, además de la responsabilidad añadida para los proveedores; el impacto de las libertades civiles, ya que puede tener un efecto inhibidor en la libertad de expresión; y, especialmente, sobre la legalidad y constitucionalidad de la ley, cuestionada en su compatibilidad con la legislación de la UE, en concreto tras la invalidez de la Directiva 2006/24/CE por el TJUE, y su enfrentamiento a desafíos legales por vulneración de derechos fundamentales protegidos por la CE y los tratados internacionales.

En cuanto a la legalidad y constitucionalidad de la LCDCE y su alineación con la legislación de la UE, aunque por el momento no hay un pronunciamiento *stricto sensu*

por parte del TC, si existen unas consideraciones por parte del TS. El TS ha establecido que la anulación de una Directiva europea no conlleva automáticamente la invalidez de las leyes nacionales que la hayan transpuesto, enfatizando la autonomía de las legislaciones nacionales siempre que se ajusten al DUE. Además, ha destacado la necesidad de analizar la conformidad de la ley española no sólo con la Directiva anulada, sino también con el DUE en su conjunto, considerando las nuevas exigencias y adaptaciones que se deriven del desarrollo del TJUE. En cuanto a las disposiciones específicas de la LCDCE, se resalta que esta establece un plazo de conservación de datos, con estrictas garantías en su cesión a autoridades judiciales, limitando su tratamiento y cesión únicamente para la detección, investigación y enjuiciamiento de delitos graves, siempre bajo autorización judicial, y garantizando la protección integral de los datos con sanciones por incumplimiento y especificaciones técnicas detalladas. La ley española aborda varias deficiencias señaladas por el TJUE en la Directiva anulada, como la falta de control judicial previos y la ausencia de criterios objetivos para la cesión y uso de los datos, asegurando un sistema de garantías estrictas que protegen los derechos fundamentales. Además, se destaca que la Ley 9/2014[42] y la LOPDGDD complementan la LCDCE, reforzando aún más las garantías en la conservación y cesión de datos. En definitiva, el TS ha determinado que la LCDCE sigue siendo válida y conforme al DUE, al subsanar muchas de las deficiencias que llevaron a la anulación de la DCD, al incluir suficientes garantías para proteger los derechos fundamentales de los individuos, satisfaciendo así las exigencias del TJUE.[43]

En este contexto, es oportuno mencionar el caso C-207/16[44] en el que se presentó una cuestión prejudicial por la Audiencia Provincial de Tarragona ante el TJUE en relación con la LCDCE. Tras la decisión en el caso TELE2 SVERIGE[45], en la que se declaró que el régimen de conservación de datos de Suecia era contrario al DUE, surgió la posibilidad de que el régimen español también fuera considerado incompatible con el DUE. Sin embargo, el TJUE adoptó una interpretación más restrictiva. En lugar de evaluar la legalidad del sistema español de conservación de datos, el Tribunal se centró exclusivamente en aspectos relacionados con el acceso a los datos almacenados. En

[42] Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. *BOE, núm. 114,* de 10 de mayo de 2014.
[43] Cfr. STS (Sala Segunda) 727/2020, de 23 de marzo de 2021. Además, véase el Informe Jurídico de la AEPD, N/REF: 0030/2021.
[44] Cfr. STJUE (Gran Sala), de 2 de octubre de 2018, C-207/16.
[45] Cfr. STJUE (Gran Sala) de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15.

consecuencia, el TJUE ha dejado abierta la posibilidad de interpretación en cuanto a la legalidad de la LCDCE en relación con el DUE. Esta situación pone de relieve la importancia de un escrutinio judicial y legislativo continuo para garantizar que las normativas nacionales se alineen con los estándares europeos en materia de derechos fundamentales.

Como hemos observado, la conservación de datos dentro del marco jurídico europeo es una cuestión de delicado equilibrio entre la protección de la seguridad pública y el respeto a los derechos fundamentales a la privacidad y la protección de datos. La invalidez de la DCD por parte del TJUE ha destacado la urgente necesidad de alcanzar un equilibrio más preciso entre estos intereses contrapuestos. A mi modo de ver, si bien la LCDCE incluye controles judiciales y garantías estrictas en la cesión de datos a autoridades judiciales, no cumple plenamente con los criterios establecidos por el TJUE en relación con la DCD. Aunque esta ley exige la conservación de datos de tráfico y localización durante un año y restringe su uso a la detección, investigación y enjuiciamiento de delitos graves, siempre bajo estrictas garantías y con autorización judicial necesaria, incurre en la generalización al tratar a todas las personas y sin hacer distinciones claras según el objetivo de lucha contra delitos graves. Además, la ley no define claramente qué se entiende por delitos graves, lo cual es necesario para garantizar que la injerencia en la privacidad sea proporcional y necesaria. Esta falta de distinción y especificidad conlleva a una conservación generalizada e indiferenciada de datos, contraviniendo a un requisito fundamental del TJUE, el cual prohíbe que normativas nacionales establezcan una conservación masiva y sin discriminación de datos personales. Por consiguiente, aunque la LCDCE presenta avances significativos en materia de control y proporcionalidad, todavía no cumple con la exigencia del TJUE de evitar una conservación generalizada e indiscriminada de datos.

3.2.3 Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales

La LO 7/2021, si bien tardía y con las graves consecuencias previamente mencionadas, adapta al ordenamiento jurídico español las disposiciones Directiva (UE) 2016/680. Asimismo, complementa la LOPDGDD en materia de prevención, detección, investigación y enjuiciamiento de infracciones penales, así como en la ejecución de

sanciones penales. De manera que, esta ley establece salvaguardias específicas para garantizar el respeto a los derechos fundamentales, como la privacidad y la protección de datos, mientras se llevan a cabo actividades relacionadas con la justicia penal. Por esta razón, es crucial garantizar que cualquier intervención sea mínima y proporcional, y que los datos se manejen y gestionen con el máximo cuidado.[46]

En este sentido, la LO 7/2021 tiene como principal objetivo establecer disposiciones para proteger los datos personales de los individuos en cuanto a su tratamiento por parte de las autoridades competentes con diversos fines, tales como la prevención, detección, investigación y enjuiciamiento de delitos, así como la ejecución de sanciones penales (artículo 1). Además, se incluye la protección y prevención contra amenazas a la seguridad pública. De modo que esta ley busca garantizar que el manejo de esta información se realice de manera adecuada y respetuosa de los derechos de los individuos, en consonancia con los principios de protección de datos personales.

El alcance de esta ley abarca el tratamiento total o parcialmente automatizado de datos personales, así como el tratamiento no automatizado de datos destinados a ficheros, llevado a cabo por autoridades competentes con los fines ya referidos (artículo 2). El tratamiento de datos personales realizado por órganos judiciales y fiscalías, así como dentro de la gestión de la Oficina Judicial y Fiscal, se rige por esta ley, junto con disposiciones específicas de otras leyes pertinentes. No obstante, ciertos tratamientos quedan excluidos de esta ley, como aquellos realizados para fines diferentes a los mencionados, los llevados a cabo por la Administración General del Estado según actividades definidas por el TFUE, los que no están dentro del ámbito del DUE, los sujetos a normativa sobre materias clasificadas, en particular en materia de defensa nacional, y en acciones civiles y procedimientos administrativos no relacionados directamente con los fines penales. Además, la ley no se aplica al tratamiento de datos de personas fallecidas, aunque sus familiares y herederos pueden solicitar el acceso, rectificación o supresión de esos datos.[47]

---

[46] Vid. ESPARZA LEIBAR, I., (2022). "Derecho fundamental a la protección de datos de carácter personal en el ámbito jurisdiccional e Inteligencia Artificial. En especial la LO 7/2021, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales". En CALAZA LÓPEZ, S., y LLORENTE SÁNCHEZ-ARJONA, M. (Dirs), *Inteligencia artificial legal y administración de justicia*, Editorial Aranzadi, p. 196.

[47] Vid. RODRÍGUEZ AYUSO, J. F. (2021). "Nueva regulación en el tratamiento de datos personales…" *op. cit.*, pp. 656-657.

La LO 7/2021 incorpora los principios fundamentales del artículo 5 de la RGPD, asegurando la licitud, lealtad y transparencia en el tratamiento de datos, garantizando que se recolecten de manera legal y transparente. Se establece la limitación de la finalidad, requiriendo que los datos se recopilen únicamente para propósitos específicos y legítimos, y se fomenta la minimización de datos, garantizando que sólo se recojan aquellos estrictamente necesarios. Asimismo, se enfatiza la importancia de mantener la exactitud de los datos, exigiendo que los datos estén actualizados y sean precisos. Se impone un límite explícito al plazo de conservación de los datos, enfatizando que sólo se mantendrán durante el tiempo necesario para cumplir con los fines establecidos. Además, se garantiza la integridad y confidencialidad de los datos, protegiéndolos adecuadamente contra cualquier tratamiento no autorizado. Como novedad, se introduce la obligación de colaboración, que obliga a organismos públicos y a cualquier persona, tanto física como jurídica, a proporcionar datos a autoridades judiciales y policiales cuando sea necesario para la investigación y enjuiciamiento de infracciones penales, reforzando así los mecanismos de aplicación de la ley en este ámbito.[48]

Además, la LO 7/2021 establece aquellas autoridades competentes para llevar a cabo el tratamiento de datos personales de acuerdo con los fines mencionados anteriormente (artículo 4). A tal aspecto, se consideran como autoridades competentes todas las entidades públicas que tengan atribuciones legales para el tratamiento de datos personales con los propósitos mencionados. Esto abarca a las Fuerzas y Cuerpos de Seguridad, Administraciones Penitenciarias, la Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria, el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, y la Comisión de Vigilancia de Actividades de Financiación del Terrorismo. Además, se incluyen las autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal como autoridades competentes.

Esta normativa también realiza una distinción entre "responsable" o "encargado" del tratamiento: por un lado, el término "responsable del tratamiento" o simplemente "responsable" se refiere a la autoridad competente que, ya sea sola o en conjunto con otros, determina los fines y medios del tratamiento de datos personales y, por otro lado,

[48] Vid. RODRÍGUEZ AYUSO, J. F. (2021). "Nueva regulación en el tratamiento de datos personales…" *op. cit.*, pp. 657-658.

el "encargado del tratamiento" o "encargado" se refiere a la persona física o jurídica, autoridad pública, servicio u otro organismo que trata datos personales en nombre y por cuenta del responsable del tratamiento (artículo 5 g y h). De modo que los responsables del tratamiento están obligados a adoptar medidas técnicas y organizativas apropiadas, adaptadas al riesgo que suponen para los derechos y libertades individuales. Paralelamente, los encargados del tratamiento deben ofrecer garantías adecuadas y llevar un registro detallado de todas las actividades del tratamiento que se realizan, lo que incluye la identificación del responsable del tratamiento y los propósitos específicos para los cuales se lleva a cabo dicho tratamiento. Esta documentación no sólo ayuda a garantizar la transparencia y la responsabilidad en el procesamiento de los datos, sino que también facilita la supervisión y el cumplimiento de las regulaciones de protección de datos.[49]

Por otro lado, se determina un marco temporal para la conservación y revisión de datos personales, resaltando los siguientes aspectos: primero, el responsable del tratamiento debe limitar la conservación de datos conforme a los fines indicados; segundo, se impone la obligación de revisar la necesidad de conservar, limitar o eliminar los datos al menos cada tres años, considerando la edad del individuo, la naturaleza de los datos y el estatus de investigaciones o procesos penales, preferiblemente utilizando procesos automatizados; tercero, se instaura un plazo máximo de veinte años para la supresión de los datos, aunque este plazo puede prolongarse en situaciones excepcionales como investigaciones en curso, delitos no prescritos, ejecución de penas pendientes, reincidencia o necesidad de protección de las víctimas (artículo 8). A su vez, es esencial distinguir los datos personales según las diversas categorías de interesados, como sospechosos, condenados, víctimas, entre otros, así como determinar si se basan en hechos objetivos o en apreciaciones subjetivas (artículos 9).[50]

3.3 Regulaciones específicas para los operadores de servicios de telecomunicaciones

Las regulaciones específicas para los operadores de servicios de telecomunicaciones en España están sujetas a varias leyes que han ido evolucionando con el tiempo para adaptarse al panorama tecnológico cambiante y garantizar la protección de

[49] Vid. RODRÍGUEZ AYUSO, J. F. (2021). "Nueva regulación en el tratamiento de datos personales…", *op. cit.*, p. 659.
[50] Vid. MARTÍNEZ VÁZQUEZ, F. (2021). "La nueva Ley Orgánica de protección de datos personales…", *op. cit.*, p. 9.

los derechos de los ciudadanos en el contexto digital. En este sentido, la normativa clave incluye la Ley 32/2003[51] (en adelante, LGT), la cual, si bien ha sido derogada, supuso un paso importante en la regulación del sector de las telecomunicaciones en España. Esta ley sentó las bases para la gestión del espectro radioeléctrico, la prestación de servicios de telecomunicaciones y la protección de los derechos de los usuarios.

Posteriormente, la Ley 9/2014[52] supuso un paso significativo al derogar la LGT y establecer un marco jurídico más actualizado para regular el sector de las telecomunicaciones. Esta ley abordó aspectos como la neutralidad de la red, la protección de competencia y la promoción de la inversión en infraestructuras de telecomunicaciones, entre otros aspectos relacionados.

No obstante, la regulación actual en materia de telecomunicaciones es la Ley 11/2022, de 28 de junio[53]. Esta ley representa la más reciente actualización legislativa del sector de las telecomunicaciones en España y tiene como objetivo adaptar la regulación a los avances tecnológicos y cambios en el mercado de las comunicaciones.

En paralelo, la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico[54] (en adelante, LSSICE), también desempeña un papel relevante en el contexto de las telecomunicaciones. Esta ley establece el marco legal para la prestación de servicios electrónicos, el comercio electrónico y la firma electrónica, entre otros aspectos relacionados con la sociedad de la información.

En lo que respecta a la cesión de datos personales por parte de los operadores de servicios de telecomunicaciones a las autoridades para investigación criminal, estas leyes proporcionan el marco legal dentro del cual deben realizarse dichas cesiones. Es importante señalar que cualquier transferencia de datos personales debe realizarse conforme a los principios de protección de datos establecidos en la legislación española y europea, como por ejemplo la LOPDGDD y el RGPD.

---

[51] Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. *BOE, núm. 264,* de 4 de noviembre de 2003.

[52] Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. *BOE, núm. 114,* de 10 de mayo de 2014.

[53] Ley 11/2022, de 28 de junio, General de Telecomunicaciones. *BOE, núm. 155,* de 29 junio de 2022.

[54] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. *BOE, núm. 166,* 12 de julio de 2002.

4. INTERSECCIÓN ENTRE LA CONSERVACIÓN DE DATOS, LA INVESTIGACIÓN CRIMINAL Y COOPERACIÓN CON LOS OPERADORES DE SERVICIOS DE TELECOMUNICACIONES

4.1 Conservación de datos personales

4.1.1 Definición y finalidad

La conservación de datos personales se refiere al almacenamiento de información de comunicaciones electrónicas que permite identificar de manera directa o indirecta a una persona física durante un período determinado, con el fin de utilizarlos en investigaciones criminales o para garantizar la seguridad nacional.

De esta manera, el objetivo de la conservación de datos personales es permitir a las autoridades competentes acceder a información relevante para la prevención, detección y enjuiciamiento de delitos a través de la cooperación judicial internacional[55]. En este sentido, la retención de datos personales es esencial para la lucha contra el crimen, incluyendo el terrorismo y la delincuencia organizada, al facilitar el acceso a datos que pueden ser considerados necesarios para investigaciones criminales y la seguridad pública. Así pues, la cooperación judicial internacional desempeña un papel importante a la hora de facilitar el intercambio de información entre países para combatir amenazas transnacionales, como el terrorismo, y garantizar la seguridad a nivel global.

4.1.2 Principio de disponibilidad y la libre circulación de datos en relación con la conservación de datos

La conservación de datos personales está estrechamente vinculada al principio de disponibilidad y la libre circulación de datos. Estos principios son fundamentales para garantizar que la información personal sea accesible cuando sea necesario y pueda compartirse y utilizarse de manera segura y eficaz, siempre dentro de los marcos legales establecidos.

El principio de disponibilidad emerge como un modelo innovador en la política criminal europea, cuyo objetivo radica en asegurar que las autoridades de cada Estado miembro de la UE tengan el derecho a acceder y utilizar la información esencial para prevenir, investigar y sancionar delitos. Esta premisa implica que dichas autoridades

[55] Cfr. Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001.

deben contar con acceso a datos relevantes en condiciones equiparables a las de otras jurisdicciones. Este principio se manifiesta en diversas decisiones y directivas de la UE que faciliten el intercambio de información y datos personales entre los Estados miembros, particularmente en la lucha contra el terrorismo y la delincuencia transfronteriza, promoviendo así una mayor cooperación y coordinación entre las autoridades policiales y judiciales de los distintos países de la UE.[56] Asimismo, este principio se refiere a la capacidad de garantizar que los datos personales estén accesibles y utilizables cuando sean necesario para los fines previstos, lo cual implica asegurar la accesibilidad de los datos para las personas autorizadas tanto dentro como fuera de una organización en el momento que se requieran, mantener la integridad de los datos completos y sin alteraciones durante su período de conservación, y proporciona a los sistemas de almacenamiento y gestión de datos la resiliencia necesaria para resistir y recuperarse de incidentes que puedan afectar su disponibilidad, como fallos técnicos o ataques cibernéticos. Por tanto, esta disponibilidad asegura que los datos puedan circular libremente dentro de los límites marcados por la normativa, facilitando su uso legítimo y protegiendo la privacidad y los derechos de los individuos.[57]

La libre circulación de datos personales en la UE, según el RGPD, se concibe como un principio fundamental que permite la transferencia sin restricciones de información personal dentro del territorio comunitario. Este principio, sustentado en el equilibrio entre la protección de los datos personales y otros derechos fundamentales, busca garantizar que las limitaciones a la circulación de datos sean necesarias para salvaguardar los derechos y libertades individuales. Se fomenta así un entorno que promueve la protección de la privacidad de los individuos mientras se facilita el intercambio fluido de información esencial para el funcionamiento eficiente de la sociedad y el mercado interno de la UE, tal como se establece en algunos artículos del RGPD, que definen y regulan la objeción

[56] Vid. GALÁN MUÑOZ, A. (2015). "La protección de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal en la Unión Europea". En COLOMER HERNÁNDEZ, I., *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Editorial Aranzadi, pp. 42-51; PESQUEIRA ZAMORA, M. J. (2020). "Diligencias de investigación, cesión de datos y principio de proporcionalidad". InDret, Núm. 4, pp. 436-437. Véase en https://doi.org/10.31009/InDret.2020.i4.11

[57] Vid. ETXEBERRIA GURIDI, J. F. (2009). "Principio de disponibilidad y protección de datos personales: a la búsqueda del necesario equilibrio en el espacio judicial penal europeo". En Eguzkilore: Cuaderno del Instituto Vasco de Criminología, Nº. 23, pp. 360-361.; RUGGERI, E. (2022). "Principio de disponibilidad y libre circulación de evidencias y datos personales en Europa. Nuevas garantías y nuevos riesgos para los derechos individuales". En COLOMER HERNÁNDEZ, I., CATALINA BENAVENTE, M. Á., y OUBIÑA BARBOLLA, S. (Dirs), *Uso de la información y de los datos personales en los procesos: los cambios en la era digital*, Editorial Aranzadi, pp. 330-335.

pertinente y motivada, las evaluaciones de impacto relativas a la protección de datos y la autoridad de control en materia de protección de datos (Considerando cuarto y artículos 4. 24), 35 y 51).

Al fin de cuentas, esta interrelación requiere un delicado equilibrio entre la protección de la privacidad y los derechos individuales, y la necesidad de garantizar la eficacia de la justicia penal y la seguridad pública.

4.1.3 Obligación de conservación de datos

La obligación de conservación de datos se refiere a la retención de datos personales durante un período de tiempo determinado, en cumplimiento de las disposiciones de las leyes y regulaciones de protección de datos.

Según el artículo 4 de la LCDCE, la obligación de conservar datos implica que los operadores deben recopilar y almacenar los datos de tráficos generados durante la prestación de servicios de comunicaciones, asegurándose de que estos datos se conserven de acuerdo con la ley. Además, se establece que los operadores no pueden utilizar o aprovechar los registros generados.

Esta obligación de conservación de datos se extiende a las llamadas fructuosas, definidas como aquellas en las que se realiza una llamada con éxito, pero no hay respuesta por parte del receptor, o en las que hay una intervención por parte del operador u operadores involucrados en la llamada. La conservación de datos de estas llamadas se considera importante en las investigaciones, ya que pueden proporcionar indicios sobre relaciones entre personas investigadas[58].

Este deber de conservación se acompaña con la correlativa obligación de ceder datos a las autoridades competentes, como se establece en los artículos 6 y 7 de la LCDCE.

4.1.4 Clasificación de los datos conservados

La LCDCE, en su artículo 3, determina los tipos de datos que deben ser conservados por los prestadores de servicios de comunicaciones electrónicas disponibles al público.

[58] Vid. RODRÍGUEZ LAINZ, J. L. (2008). "El principio de proporcionalidad en la nueva ley de conservación de datos relativos a las comunicaciones (I)". Diario La Ley, Nº 6859, Sección Doctrina, 14 de enero de 2008, Editorial Wolters Kluwer. p. 10.

Entre los datos que se conservan se encuentran información detallada de los terminales de comunicación, incluidos números de teléfono, direcciones IP y otros identificadores únicos de dispositivos; datos de localización que proporcionan información sobre la ubicación de los usuarios durante las comunicaciones, que van desde información general hasta datos precisos de geolocalización; la identificación de los usuarios involucrados en las comunicaciones, que implica la conservación de nombres, números de identificación personal y datos de registro en servicios de comunicación; información detallada sobre las comunicaciones en sí misma, como la hora y fecha de inicio y fin, la duración y el tipo de comunicación realizada, ya sea una llamada telefónica, un mensaje de texto o cualquier otro medio; y registros de llamadas infructuosas que ofrecen información sobre comunicaciones que no se completaron con éxito, brindando una visión más amplia de los patrones de comunicación (artículo 3). Estos datos son necesarios para una variedad de propósitos, desde la gestión de redes y la optimización de servicios hasta la investigación criminal, pero se conservan sin acceder ni almacenar el contenido real de las comunicaciones, en cumplimiento del derecho al secreto de estas y la protección de la privacidad de los usuarios.[59]

Como puede observarse, la conservación de datos engloba la preservación de una amplia variedad de tipos de datos. En este escenario, surge el debate sobre la conservación de datos de manera generalizada e indiscriminada que puede llevar a vulneraciones de la privacidad y el abuso de la información, ya que acumula grandes volúmenes de datos personales sin un propósito específico, incrementando los riesgos de seguridad y potenciales violaciones de los derechos fundamentales de los individuos.

Bajo esta premisa, este tipo de prácticas abarca la recopilación, uso o divulgación de información de manera excesivamente amplia, genérica o sin discriminación, lo que puede comprometer la privacidad y los derechos de los individuos afectados.

En este sentido, la sentencia emitida por el TJUE en el caso G.D. y Comissioner an Garda Síochána[60], reitera la postura del TJUE respecto a la incompatibilidad del DUE con la conservación generalizada e indiscriminada de datos de tráfico y localización de comunicaciones electrónicas. Esta decisión establece que el artículo 15.1 de la Directiva

[59] Vid. RODRÍGUEZ LAINZ, J. L. (2008). "El principio de proporcionalidad en la nueva ley de conservación de datos…", *op. cit.*, pp. 7-10.
[60] STJUE (Gran Sala) de 5 de abril de 2022, asunto C-140/20.

ePrivacy, en concordancia con los derechos fundamentales recogidos en la Carta de la UE, prohíbe medidas legislativas que impongan una conservación generalizada e indiscriminada de dichos datos con fines de lucha contra la delincuencia grave y la prevención de amenazas graves contra la seguridad pública. No obstante, se abre la posibilidad de establecer criterios de retención selectiva de datos, siempre y cuando sean objetivos, no discriminatorios, limitados a lo estrictamente necesario y permitan vincular los delitos graves con los individuos cuyos datos se conservarán. Además, la sentencia aborda temas como el uso de datos conservados por motivos comerciales en investigaciones de delitos graves, la regulación de las "conservaciones rápidas" (*freezing orders*) y la necesidad de que la autoridad que supervise el acceso a los datos sea independiente. Asimismo, la sentencia introduce unas novedades en relación con los términos de conservación de datos de asignación de IIPP dinámicas, ampliando el concepto de identidad civil para incluir los datos que permitan la identificación de personas involucradas en actos delictivos graves. Esto posibilita la conservación preventiva de datos relacionados con tarjetas de telefonía de prepago. Además, aborda la posibilidad de crear bases de datos sobre asignaciones de IIPP dinámicas en el ámbito de la lucha contra la delincuencia y amenazas graves contra la seguridad pública. En definitiva, la sentencia reafirma la postura del TJUE contra la conservación generalizada e indiscriminada de datos de comunicaciones electrónicas, aunque permite la posibilidad de regímenes de retención selectiva bajo condiciones estrictas, lo que implica la necesidad urgente de adecuar la legislación y jurisprudencia nacional a esta doctrina.[61]

4.1.4 Sujetos obligados

En relación con los sujetos que quedan obligados a conservar los datos, éstos serán los operadores que prestan servicios de comunicaciones electrónicas públicas o exploten redes públicas de comunicaciones, de conformidad con el artículo 2 de la LCDCE.

[61] Vid. RODRÍGUEZ LAINZ, J. L. (2022). "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". Diario La Ley, Nº 10058, Sección Tribuna, 28 de Abril de 2022, Editorial Wolters Kluwer.

El alcance territorial de esta ley se determina según el principio del establecimiento en España o la operación a través de un establecimiento permanente en el territorio nacional, tal como se describe en el artículo 2 de la LSSICE.[62]

4.1.5 Concepto de delitos graves

Los datos se conservan principalmente en el ámbito de la lucha contra el crimen, específicamente para la prevención, detección, investigación y enjuiciamiento de infracciones penales graves. Por ello, la LCDCE establece que su objetivo es regular la obligación de los operadores de conservar los datos generados o tratados en el contexto de la prestación de servicios de comunicaciones electrónicas o redes públicas de comunicación y, además, estipula el deber de proporcionar dichos datos a los agentes autorizados cuando sean solicitados mediante la correspondiente autorización judicial, con el propósito de detectar, investigar y enjuiciar delitos graves contempladas en el Código Penal (en adelante, CP) o en las leyes penales especiales.

En este sentido, la cuestión que surge en torno a la interpretación del término de "delitos graves" es crucial. Sin embargo, la LCDCE no define de manera específica qué se entiende por "delitos graves", pero remite a la legislación penal para su interpretación.

Por consiguiente, desde una interpretación literaria, el artículo 13 del CP considera como "delitos graves" a aquellos que la ley castiga con penas graves y, además, cuando la pena pueda clasificarse tanto como grave o menos grave, se considerará como grave. Correlativamente, en el artículo 33, apartado segundo, del CP se enumeran varios tipos de penas graves, como la prisión permanente revisable, la prisión superior a cinco años, la inhabilitación absoluta, entre otras. Por otro lado, la interceptación de comunicaciones telefónicas y telemáticas y la cesión de datos electrónicos almacenados por prestadores de servicios están relacionadas con investigaciones de delitos específicos, mencionados en el artículo 579 en relación con el artículo 588 ter a de la LECrim, como los delitos dolosos castigados con al menos tres años de presión, delitos cometidos en grupos u organizaciones criminales y delitos de terrorismo, o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

[62] Vid. RODRÍGUEZ LAINZ, J. L. (2008). "El principio de proporcionalidad en la nueva ley de conservación de datos…", *op. cit.*, p. 12.

En este aspecto, la ausencia de una definición específica de "delito grave" por parte del TJUE obliga a los Estados miembros de la UE a determinar qué constituye un delito grave según su propia legislación interna, lo que podría dar lugar a disparidades en la aplicación de estas normas. Además, la normativa exige que el acceso selectivo a los datos conservados no se limite únicamente a la lucha contra la delincuencia grave, estableciendo que los Estados miembros deben definir requisitos materiales y procedimentales específicos, como la identificación concreta de los delitos graves y la duración estrictamente necesaria de la conservación de datos, permitiendo prórrogas sólo si la necesidad persiste. Esta falta de una definición clara plantea problemas prácticos en las investigaciones penales, ya que muchos delitos que no se consideran graves quedan fuera del alcance de la conservación selectiva de datos, lo que implica la recopilación de pruebas necesarias para dichas investigaciones.[63]

Partiendo de esta premisa, cabe mencionar la sentencia del TJUE del 02 de octubre de 2018[64], que resuelve una cuestión prejudicial planteada por la Audiencia Provincial de Tarragona sobre el acceso a datos personales en un caso de robo con violencia de un teléfono móvil. La Policía Judicial solicitó la identificación de usuarios de tarjetas SIM asociadas al código IMEI del móvil robado. El TJUE debía determinar si la gravedad del delito, como criterio para justificar la injerencia en los derechos fundamentales al respeto de la vida privada y la protección de los datos personales (artículos 7 y 8 de la CDFUE), podía basarse sólo en la pena imponible o también en el nivel de lesividad de la conducta delictiva. Además, se cuestionaba si era apropiado establecer un umbral mínimo de pena de tres años para justificar tal injerencia. Finalmente, el TJUE, en su decisión, concluyó que el acceso a datos personales por parte de las autoridades constituye una injerencia en los derechos fundamentales, pero esto no significa necesariamente que se limite a delitos graves, sino también para la prevención y persecución de delitos en general. De esta forma, dicha injerencia puede justificarse para la persecución de delitos en general, lo que flexibiliza la interpretación previa que restringía esta posibilidad a la lucha contra delitos graves.[65]

---

[63] Vid. OROMÍ I VALL-LLOVERA, S. (2021). "El rol de las empresas tecnológicas en la cooperación policial y judicial y en las diligencias de investigación penal". En PEREIRA PUIGVERT, S., y ORDÓÑEZ PONZ, F. (Dirs), *Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos*, Editorial Aranzadi, pp. 827-828.

[64] STJUE (Gran Sala), de 2 de octubre de 2018, C-207/16.

[65] Vid. CABALLERO TRENADO, L. (2018). "Acceso a comunicaciones electrónicas y tratamiento de datos personales: nuevo criterio. Comentario a la STJUE (Gran Sala) C-207/16, de 2 de octubre de 2018,

En definitiva, el TJUE ha determinado que la injerencia grave en los derechos fundamentales sólo puede justificarse cuando se trata con la lucha contra la delincuencia grave, como delitos cometidos en el seno de organizaciones criminales o terrorismo. No obstante, cuando la injerencia no es grave, puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir delitos en general. En consecuencia, el TJUE destaca que la determinación de si un delito es grave no debe basarse únicamente en la pena máxima que se puede imponer, sino también en la naturaleza y el impacto del delito en los bienes jurídicos individuales y colectivos.[66]

4.1.6 Duración de la conservación de datos

Según el artículo 5 de la LCDCE, los datos deben conservarse durante un período de doce meses, computados desde la fecha de la comunicación. Este plazo podrá ampliarse reglamentariamente hasta un máximo de dos años o reducirse hasta un mínimo de seis meses. Esta decisión se considera teniendo en cuenta criterios como los costos del almacenamiento y conservación de datos, así como su relevancia para los fines de investigación, detección y enjuiciamiento de delitos graves, después de consultar a los operadores.

Para acceder a los datos en posesión de los operadores, a la luz del artículo 6 de la LCDCE, siempre será necesario la autorización judicial previa. Además, los agentes facultados para acceder a estos datos serán únicamente las Fuerzas y Cuerpos de Seguridad —mientras desempeñen funciones de policía judicial—, la Dirección Adjunta de Vigilancia Aduanera —mientras desarrollen sus competencias como policía judicial—, y el Centro Nacional de Inteligencia —en el curso de investigaciones de seguridad sobre personas o entidades—, a quienes los operadores deben asignarles los datos almacenados.

sobre acceso de las autoridades nacionales a los datos para la investigación de un delito y umbral de gravedad del delito que puede justificar el acceso a los datos". Revista de Derecho, Empresa y Sociedad (REDS), Nº 13, pp. 363-367; PÉREZ MANZANO, M. (2020). "Protección de datos personales: retos para el sistema penal". En CASAS BAAMONDE, M. E. (Coord), *El derecho a la protección de datos personales en la sociedad digital*, Fundación Ramón Areces, p. 87.

[66] Cfr. STJUE (Gran Sala) de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12; STJUE (Gran Sala) de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15; STJUE (Gran Sala), de 2 de octubre de 2018, C-207/16.

4.2 Cooperación de los operadores de servicios de telecomunicaciones en la investigación criminal

4.2.1 Rol de los operadores de servicios de telecomunicaciones en la investigación criminal

Los operadores de servicios de telecomunicaciones juegan un papel crucial en la investigación criminal, actuando como proveedores de información esencial para el esclarecimiento de delitos. Este rol se fundamenta en el «deber de colaboración» establecido en la LOPDGDD, así como en la LECrim.

En virtud de este deber, los operadores de servicios de telecomunicaciones están obligados a colaborar con las autoridades en la investigación de delitos, facilitando el acceso a datos personales relacionados con las comunicaciones de sus usuarios. Este acceso se lleva a cabo bajo estrictas medidas de seguridad y confidencialidad, garantizando en todo momento el respeto a los derechos fundamentales de los individuos, especialmente en lo que respecta a la privacidad y protección de datos personales.

De este modo, la cooperación entre los operadores de servicios de telecomunicaciones y las autoridades se lleva a cabo mediante la cesión de información relevante, como el número de teléfono de origen y destino, el nombre y dirección del abonado o usuario registrado, el listado de llamadas, la fecha y hora de las comunicaciones, el IMEI del terminal, datos de ubicación y otros metadatos asociados a las comunicaciones electrónicas. Estos datos pueden proporcionar pistas importantes para identificar y procesar a sospechosos, así como reconstruir hechos relacionados con la comisión de un delito.

Desde este punto de vista, el artículo 588 ter e de la LECrim establece un deber de colaboración para facilitar la intercepción de comunicaciones telefónicas y telemáticas, aplicable a cualquier persona o entidad que contribuya a estas comunicaciones. Esta obligación, dentro del marco legal de las medidas de investigación tecnológica, incluye a operadores de redes públicas y prestadores de servicios de la sociedad de la información, así como a otros implicados en las comunicaciones. Los sujetos obligados deben

colaborar con el Juez, el Ministerio Fiscal y la Policía Judicial, proporcionando la información necesaria y guardando secreto sobre las actividades requeridas[67].

Es importante resaltar que la cesión de datos personales por parte de los operadores de servicios de telecomunicaciones debe realizarse conforme con los principios de proporcionalidad y necesidad. Es decir, sólo se cederán aquellos datos que sean absolutamente necesarios para la investigación en curso, evitando cualquier tipo de exceso o abuso en el acceso a la información personal de los usuarios.

Además, los operadores de servicios de telecomunicaciones están sujetos a estrictas obligaciones de secreto profesional y confidencialidad, lo que implica que la información proporcionada se utiliza únicamente para fines específicos de investigaciones criminales y bajo el control de las autoridades competentes. Cualquier uso indebido o divulgación no autorizada de estos datos puede acarrear severas sanciones legales y daños a la reputación de sus servicios.

Por otro lado, es importante señalar que la colaboración entre los operadores de servicios de telecomunicaciones y las autoridades en el ámbito de la investigación criminal no les exime de obtener la correspondiente autorización judicial cuando ésta sea necesaria. Es decir, en los casos en que se requiera la intervención de comunicaciones o el acceso a datos especialmente protegidos, las autoridades competentes deberán obtener previamente una decisión judicial que respalde dicha actuación, garantizando así el debido proceso y el respeto a los derechos fundamentales de los individuos.

En definitiva, el rol de los operadores de servicios de telecomunicaciones en la investigación criminal es fundamental para el esclarecimiento de delitos, pero debe realizarse dentro del marco legal establecido, respetando siempre los derechos fundamentales de los individuos y garantizando la seguridad y confidencialidad de los datos personales cedidos a las autoridades. La colaboración entre ambas partes se basa en los principios de proporcionalidad, necesidad y respeto a la legalidad, siendo esencial para la eficacia del sistema de justicia penal en España.

[67] Circular 2/2019, de 6 de marzo, de la Fiscal General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas. *BOE, núm. 70*, de 22 marzo de 2019.

4.2.2. Cesión de datos personales por los operadores de servicios de telecomunicaciones en la investigación criminal

4.2.2.1 Definición y finalidad

La cesión de datos personales en el ámbito de una investigación criminal se refiere a la transferencia de información sensible por parte de los operadores de servicios de telecomunicaciones a las autoridades competentes con el fin de cooperar en las investigaciones penales. De modo que, esta actividad implica revelar datos a terceros distintos del interesado, como parte de diligencias que permiten a las autoridades acceder a información relevante para esclarecer delitos. Además, la cesión de datos personales en investigaciones criminales debe respetar los principios de proporcionalidad, legalidad y necesidad, garantizando que sólo se compartan los datos que sean absolutamente necesarios para la investigación en curso, respetando los derechos fundamentales de los individuos, como el derecho a la protección de datos personales y la privacidad.

Por tanto, el objetivo principal de la cesión de datos personales en la investigación criminal es facilitar el acceso de las autoridades competentes a información relevante para dilucidar actos delictivos y realizar investigaciones penales de manera efectiva. La operación tiene como objetivo combinar las necesidades de las investigaciones criminales con los derechos de protección de datos personales, permitiendo a las autoridades obtener los documentos y pruebas incriminatorias necesarias para resolver casos penales. La transferencia de datos personales en el marco de una investigación criminal se realiza con la finalidad de contribuir a la prevención y resolución del delito, respetando los derechos fundamentales de las personas interesadas.

La normativa que regula la cesión de datos personales en investigaciones criminales incluye la Directiva (UE) 2016/680, la LO 7/2021, la LCDCE, y la LECrim. Estas leyes establecen criterios para la recogida, cesión, tratamiento, y uso de datos personales en investigaciones criminales, con el objetivo de garantizar la protección de los derechos fundamentales de las personas. Además, estas leyes establecen garantías y principios aplicables a los interesados. como el principio de disponibilidad, el derecho a la información, y los derechos ARCO.

4.2.2.2 Obligación de cesión de datos

El deber de cesión de datos personales en investigaciones criminales en la LCDCE establece que los operadores de servicios de telecomunicaciones tienen la obligación de ceder ciertos datos generados o tratados en la prestación de servicios de comunicaciones electrónicas. Según la LCDCE, los datos almacenados por los operadores de telecomunicaciones sólo pueden ser cedidos de conformidad con lo previsto en la ley y previa autorización judicial.

En consecuencia, la cesión de datos sólo se realizará en formato electrónico únicamente a los agentes facultados, mencionados previamente, y se limitará a la información necesaria para lograr los fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el CP o en las leyes penales especiales.

Los operadores deberán transferir los datos conservados a los agentes autorizados a que se refiere el artículo 3 de la LCDCE, concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial. Dicha resolución judicial determinará, conforme a lo previsto en la LECrim y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes competentes.

4.2.2.3 Procedimiento de la cesión de datos

El artículo 7 de la LCDCE regula el procedimiento de cesión de datos que se debe seguir. De este modo se determina claramente las obligaciones y condiciones bajo las cuales los operadores deben ceder los datos conservados a agentes facultados, siempre sujeto a una resolución judicial. Esto es esencial para garantizar que el proceso se lleve a cabo de manera legal y justa, protegiendo tanto los derechos de los individuos como las necesidades de la investigación.

En primer lugar, establece la obligación de cesión de datos por parte de los operadores. Estos están obligados a ceder los datos conservados que permitan identificar a personas a los agentes facultados. Esta obligación es independiente de la decisión judicial, lo que significa que la cesión debe realizarse siempre que se cumplan las condiciones especificadas, garantizando así la necesaria cooperación en las investigaciones pertinentes.

Seguidamente, el artículo aborda la resolución judicial necesaria para la cesión de datos. La cesión de datos debe estar determinada por una resolución judicial y se hace referencia a la LECrim para determinar los datos que deben ser cedidos. Además, esta resolución debe adherirse estrictamente a los principios de necesidad y proporcionalidad, asegurando que solo se cedan los datos imprescindibles para la investigación.

Finalmente, se detalla el plazo de ejecución para la cesión de datos. La decisión judicial determinará el plazo dentro del cual debe realizarse la cesión de datos, teniendo en cuenta la urgencia y los efectos de la investigación, así como la naturaleza y complejidad técnica de la operación. A falta de plazo específico en la orden, la cesión debe realizarse en el plazo de 72 horas a partir de las 8:00 horas del día natural siguiente a la recepción de la decisión por parte del sujeto obligado. Esta disposición garantiza que la cesión de datos se realice de manera oportuna, facilitando así el avance efectivo de las investigaciones.

La disposición final cuarta de la ley detalla el formato electrónico en el que deberán proporcionar los datos conservados, estableciendo que será determinado por Orden[68] conjunta de los ministros correspondientes.

En síntesis, el procedimiento de cesión de datos establecido por la LCDCE tiene como objetivo garantizar la legalidad, proporcionalidad y eficacia en la obtención y utilización de información sensible para fines de investigación y enjuiciamiento penal.

4.2.2.4 Uso de datos obtenidos en un procedimiento penal para otros procedimientos

En el ámbito del derecho procesal penal español, uno de los temas que suscita especial interés y debate es la utilización de datos obtenidos durante un procedimiento penal para otros procedimientos. Esta cuestión plantea interrogantes sobre la protección de la privacidad y los derechos fundamentales de los individuos involucrados en procesos judiciales, así como los límites y alcances de la utilización de dicha información en distintos contextos legales.

Las normativas europeas regulan la posibilidad de utilizar información obtenida en un proceso penal para otros procesos. Estas normativas establecen condiciones

[68] Vid. Orden PRE/199/2013, de 29 de enero, por la que se define el formato de entrega de los datos conservados por los operadores de servicios de comunicaciones electrónicas o de redes públicas de comunicaciones a los agentes facultados.

específicas que deben cumplirse para garantizar el tratamiento legal y ético de datos personales en el ámbito de la cooperación judicial y policial en materia penal.

En un principio, se destaca el Convenio de asistencia judicial penal entre los Estados miembros de la UE[69] que aborda la transferencia de datos entre autoridades competentes de los Estados miembros. Reconoce la posibilidad de utilizar la información obtenida de esta transferencia para otros procedimientos judiciales o administrativos directamente relacionados con el procedimiento original. Además, permite su uso para prevenir una amenaza inmediata o grave a la seguridad pública, aunque en estos casos se podrá requerir autorización previa.[70]

La Decisión Marco 2008/977/JAI[71] del Consejo amplía esta posibilidad y normaliza su tratamiento legal en todos los Estados miembros de la UE, al tiempo que establece criterios específicos para el tratamiento de datos personales en el ámbito de la cooperación penal. Se establecen los principios como la licitud, la proporcionalidad y la finalidad del tratamiento de los datos, así como el respeto de los derechos de rectificación, supresión y bloqueo de datos.[72]

La Directiva sobre protección de datos en el ámbito penal sigue esta misma línea y establece un régimen común para garantizar el intercambio de información entre las autoridades encargadas de la seguridad nacional y la lucha contra la delincuencia. Se reconoce que el uso de esta información debe cumplir con los principios de licitud, necesidad y proporcionalidad, así como las disposiciones establecidas en el derecho nacional y el RGPD.[73]

En pocas palabras, la normativa europea proporciona un marco legal para el uso de la información obtenida en un proceso penal para otros procedimientos, pero este uso está

[69] Vid. Convenio de asistencia judicial en materia penal entre los Estados miembros de la Unión Europea, hecho en Bruselas el 29 de mayo de 2000.
[70] Vid. RODRÍGUEZ LAINZ, J. L. (2019). "La transferencia de datos obtenidos en el curso de una medida de investigación tecnológica a la luz de la Directiva (UE) 2016/680". En COLOMER HERNÁNDEZ, I., OUBIÑA BARBOLLA, S., y CATALINA BENAVENTE, M. Á. (Dirs), *Uso y Cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios,* Editorial Aranzadi, pp. 341-342.
[71] Cfr. Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.
[72] Vid. RODRÍGUEZ LAINZ, J. L. (2019). "La transferencia de datos obtenidos en el curso de una medida de investigación tecnológica…", *op. cit.,* pp. 342-344.
[73]Vid. RODRÍGUEZ LAINZ, J. L. (2019). "La transferencia de datos obtenidos en el curso de una medida de investigación tecnológica…", *op. cit.,* pp. 344-447.

sujeto a condiciones específicas y principios fundamentales, como la licitud, necesidad y proporcionalidad del tratamiento de datos.

4.2.2.4.1 Uso de datos obtenidos en un proceso penal para otro proceso penal o iniciar una nueva causa penal

En el ámbito penal, la información y las pruebas obtenidas en un proceso penal pueden ser utilizadas en otros procesos penales, incluyendo la apertura de un nuevo proceso penal. Esto se fundamenta en la búsqueda de la verdad y la justicia, siempre que se respeten los derechos fundamentales de las partes involucradas.

La práctica de utilizar información derivada de investigaciones penales para iniciar nuevas causas penales está ampliamente aceptada en el marco jurídico español, aunque sujeta a ciertas restricciones para salvaguardar los derechos fundamentales. La LECrim establece los fundamentos de esta cesión de datos, especialmente a través de disposiciones que regulan el procesamiento de información incidental descubierta durante indagaciones penales. En este sentido, el artículo 262 de la LECrim obliga a las autoridades judiciales a comunicar cualquier noticia de un delito descubierto en el curso de sus funciones, sin excepción alguna. Además, el artículo 17 de la LECrim exige la separación de investigaciones para hechos no relacionados con criterios de conexidad definidos, con el objetivo de agilizar los procedimientos. La flexibilidad del sistema legal español también se refleja en disposiciones como los artículos 624 y 760 de la LECrim y el artículo 28 de la Ley Orgánica del Tribunal del Jurado[74], que permite cambiar el procedimiento judicial si se determina que el hecho investigado corresponde a un cauce procesal distinto. No obstante, el uso de estos datos está sujeto a principios rectores como la proporcionalidad y la necesidad, en línea con el CEDH y la jurisprudencia europea y nacional. Además, la transmisión de datos se justifica principalmente en casos de delitos graves como terrorismo, delincuencia organizada, trata de personas, abusos sexuales contra menores, ataques a la integridad de los mercados financieros y delitos contra los derechos fundamentales, incluida la seguridad nacional. En definitiva, se busca garantizar que, al emplear información obtenida en investigaciones penales para iniciar nuevos procesos

[74] Ley Orgánica 5/1995, de 22 de mayo, del Tribunal del Jurado. *BOE, núm. 122*, de 23 de mayo de 1995.

penales, se respeten los principios de proporcionalidad y los derechos individuales, evaluando cuidadosamente cada caso específico.[75]

En síntesis, la cesión de datos para iniciar una nueva causa penal está amparada por la legislación española, pero su ejecución debe garantizar el respeto de los derechos fundamentales y cumplir con los requisitos legales establecidos.

4.2.2.4.2 Uso de datos obtenidos en un proceso penal para un proceso administrativo

Los datos obtenidos en un proceso penal también pueden ser utilizados en procedimientos administrativos, pero este uso está sujeto a restricciones legales específicas destinadas a proteger la privacidad y los derechos fundamentales de los individuos.

La jurisprudencia del TC y del TJUE ha establecido criterios claros en este ámbito. La sentencia 17/2013[76] del TC destacó que la transferencia de datos entre procedimientos penales y administrativos requiere una expresa previsión legal. Este principio fue reafirmado en la sentencia 67/2020[77], que permite la utilización de datos contables obtenidos en el registro de un despacho de abogados para la elaboración de un expediente de liquidación tributaria, siempre que se respetara el control jurisdiccional de dichos datos. Este control es un requisito también señalado por la jurisprudencia del TJUE, como en el caso TELE2 SVERIGE AB[78], que destaca la necesidad de una supervisión estricta para proteger los derechos fundamentales del tratamiento. En este sentido, la reciente sentencia del TJUE, en el caso ENDEMOL SHINE FINLAND OY[79], refuerza la legitimidad de la cesión de datos, siempre que cuente con respaldo legal y esté sujeta a supervisión judicial en el ámbito administrativo. [80]

El marco legal actual se encuentra principalmente en la LO 7/2021, la cual extiende su ámbito de aplicación más allá de la prevención y sanción de infracciones penales,

---

[75] Vid. RODRÍGUEZ LAINZ, J. L. (2024). "El ordenamiento jurídico español frente a la nueva doctrina del TJUE sobre utilización de datos obtenidos en el curso de una investigación criminal en otros procedimientos penales o administrativos (1)". Diario La Ley, Nº 10478, Sección Tribuna, 4 de Abril de 2024, Editorial Wolters Kluwer, pp. 13-16.

[76] Cfr. STC (Pleno) 17/2013, de 31 de enero de 2013.

[77] Cfr. STC (Sala Segunda) 67/2020, de 29 de junio de 2020.

[78] Cfr. STJUE (Gran Sala) de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15.

[79] Cfr. STJUE (Sala Sexta) de 7 de marzo de 2024, asunto C-740/22.

[80] Vid. RODRÍGUEZ LAINZ, J. L. (2024). "El ordenamiento jurídico español frente a la nueva doctrina del TJUE…", *op. cit.*, p. 16.

incluyendo la protección frente a amenazas contra la seguridad pública. No obstante, esta ley también hace referencia al marco jurídico específico de la LOPJ y al Estatuto Orgánico del Ministerio Fiscal en cuanto al tratamiento de datos bajo su competencia. Estas normativas limitan explícitamente la cesión de datos al Consejo General del Poder Judicial y al Ministerio de Justicia dentro de sus competencias de control e inspección. Por otra parte, la LO 7/2021, en su artículo 2.3 e), excluye de su ámbito de aplicación el tratamiento de datos en procedimientos administrativos que no tengan un objeto directo relacionado con la prevención o sanción de infracciones penales. Esto significa que cualquier cesión de datos de un procedimiento penal a uno administrativo debe estar respaldado por una normativa específica y debe cumplir con el RGPD.[81]

Actualmente, son escasas las normas administrativas que permiten claramente la cesión de datos obtenidos en procedimientos penales. Una excepción notable es la Ley General Tributaria[82], cuyo artículo 94.3 permite la transferencia de datos bajo determinadas condiciones. La Ley del Procedimiento Administrativo Común[83] ha suprimido muchas disposiciones que permitían esta transferencia, limitando significativamente esta posibilidad. Sin embargo, algunas normativas sectoriales específicas, como las relacionadas con el tráfico o la lucha contra el dopaje, mantienen cierta coordinación entre las autoridades judiciales y administrativas.[84]

En suma, la cesión de datos para procedimientos administrativos en España se rige por requisitos legales y principios fundamentales, como la proporcionalidad y el respeto a los derechos fundamentales, y debe cumplir con la normativa vigente en materia de protección de datos, garantizando la transparencia y la licitud en su ejecución.

Adicionalmente, la jurisprudencia del TEDH ha abordado esta cuestión a través de casos como LAMBERT v. Francia (1998)[85], MATHERON v. Francia (2005)[86], y M.N y otros v. San Marino (2015)[87], donde se resalta la importancia de que los ordenamientos

[81] Vid. RODRÍGUEZ LAINZ, J. L. (2024). "El ordenamiento jurídico español frente a la nueva doctrina del TJUE…", *op. cit.*, pp. 16-17.
[82] Ley 58/2003, de 17 de diciembre, General Tributaria. *BOE, núm. 302*, de 18 de diciembre de 2003.
[83] Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. *BOE, núm. 236*, de 02 de octubre de 2015.
[84] Vid. RODRÍGUEZ LAINZ, J. L. (2024). "El ordenamiento jurídico español frente a la nueva doctrina del TJUE…", *op. cit.*, p. 17.
[85] Cfr. STEDH 23618/94, de 24 de agosto de 1998, Caso LAMBERT v. Francia.
[86] Cfr. STEDH (Sección 4ª) 57752/00, de 29 de marzo de 2005, Caso MATHERON v. Francia.
[87] Cfr. STEDH (Sección 3ª) 28005/12, de 7 de julio de 2015, Caso M.N y otros v. San Marino.

nacionales establezcan mecanismos para impugnar la legitimidad de la cesión de datos derivados de las investigaciones criminales. La decisión del caso VERSINI-CAMPINCHI y CRASNIANKI v. Francia (2016)[88] marcó un punto de inflexión al ampliar el ámbito de protección de la privacidad al incluir el uso de información obtenida en procedimientos penales en contextos administrativos, enfatizando la necesidad de garantías y la posibilidad de impugnar dicha utilización. Posteriormente, el caso TERRAZZONI v. Francia (2017)[89] extiende este análisis a la cesión de información obtenida en investigaciones criminales para procedimientos disciplinarios, afirmando su legitimidad siempre y cuando se respeten las garantías procesales y esté justificada en un interés general. En el caso ADOMAITIS v. Lituania (2022)[90] se introduce el elemento de proporcionalidad, argumentando que el uso de información debe ser justificado por un interés público imperioso. Por último, en los casos SHIPS WASTE OIL COLLECTOR B.V v. Holanda, BURANDO HOLDING B.V y PORT INVEST B.V v. Holanda, JANSSEN DE JONG GROEP B.V. y otros v. Holanda (2023)[91] se subraya la importancia de respaldar la cesión de datos con una base legal y que sea proporcional a la finalidad perseguida, en este caso, como la protección del orden público y económico. En definitiva, la jurisprudencia del TEDH establece que la cesión de datos obtenidos en el marco de procedimientos penales para otros fines debe cumplir con criterios de legalidad, proporcionalidad y salvaguardias adecuadas para proteger los derechos individuales, en consonancia con fines legítimos de interés público.[92]

5. CONCLUSIONES

El presente estudio ha proporcionado una visión que abarca múltiples aspectos sobre la compleja intersección entre la protección de datos, la investigación criminal y la cooperación con los operadores de servicios de telecomunicaciones. Los avances tecnológicos en el ámbito de telecomunicaciones presentan desafíos significativos para el marco jurídico, impulsando constantes adaptaciones normativas que, si bien intentan

[88] Cfr. STEDH (Sección 5ª) 49176/11, de 16 de junio de 2016, Caso VERSINI-CAMPINCHI y CRASNIANKI v. Francia.
[89] Cfr. STEDH (Sección 5ª) 33242/12, de 29 de junio de 2017, Caso TERRAZZONI v. Francia.
[90] Cfr. STEDH (Sección 2ª) 14833/18, de 18 de enero de 2022, Caso ADOMAITIS v. Lituania.
[91] Cfr. STEDH (Sección 5ª) 2800/16, de 16 de mayo de 2023, Casos SHIPS WASTE OIL COLLECTOR B.V v. Holanda, BURANDO HOLDING B.V y PORT INVEST B.V v. Holanda, JANSSEN DE JONG GROEP B.V. y otros v. Holanda.
[92] Vid. RODRÍGUEZ LAINZ, J. L. (2024). "El ordenamiento jurídico español frente a la nueva doctrina del TJUE…", *op. cit.*, pp. 3-13.

adecuarse a la era digital, aún enfrentan dificultades para garantizar una protección íntegra de los derechos fundamentales que interfiere con estos.

Desde este punto de vista, el derecho a la protección de datos emerge como un derecho fundamental autónomo, distinto del derecho a la intimidad, conforme al artículo 18.4 de la CE y respaldado por la CEDH y la CDFUE. En el contexto de la persecución de delitos, la conservación y cesión de datos por parte de los operadores de servicios de telecomunicaciones se encuentran en una encrucijada crítica entre la necesidad de la seguridad pública y la protección de los derechos fundamentales.

La normativa de la UE y la legislación nacional española han evolucionado para dar cabida a esta intersección. La Directiva 2006/24/CE, que inicialmente regulaba la conservación de datos, fue invalidada por el TJUE debido a su incompatibilidad con los derechos fundamentales de los artículos 7 y 8 de la CDFUE, y por no respetar el principio de proporcionalidad del artículo 52 de la Carta. Principalmente, se criticó la falta de proporcionalidad y la ausencia de criterios objetivos y control judicial previo, lo que resultaba en una conservación generalizada e indiscriminada de datos.

La Ley 25/2007, de 18 de octubre, responde a estas deficiencias al establecer un sistema de salvaguardias estrictas, que incluye la obligación de control judicial previo y criterios objetivos para la cesión y el uso de datos. Esta ley garantiza que la conservación y cesión de datos se realicen en condiciones que respeten adecuadamente los derechos fundamentales, en particular el derecho a la privacidad y a la protección de datos personales.

Ahora bien, persiste un debate sobre la conservación generalizada e indiscriminada de datos personales, práctica que puede comprometer la privacidad y facilitar el abuso de información. El TJUE ha declarado que esta conservación indiscriminada es incompatible con el DUE, permitiendo únicamente la retención selectiva de datos de tráfico y localización bajo ciertas condiciones, por lo que garantizar que no se produzca una conservación indiscriminada sigue siendo una tarea compleja. Esta problemática pone de relieve la necesidad de establecer límites claros y objetivos en cuanto al acceso y almacenamiento de datos, evitando así posibles vulneraciones de la privacidad y de los derechos fundamentales de los ciudadanos.

La interpretación de “delitos graves” es fundamental, ya que se trata de un criterio esencial para la conservación de datos con fines de prevención, detección e investigación criminal. Sin embargo, presenta desafíos debido a que la Ley 25/2007, de 18 de octubre, no define este término explícitamente, remitiéndose a la legislación penal para su interpretación. Además, no existe una definición concreta por la normativa europea. Ahora bien, el TJUE ha indicado que sólo se justifica una injerencia grave en los derechos fundamentales para combatir delitos graves, como el terrorismo y los delitos cometidos por organizaciones criminales, pero sugiere que la gravedad del delito debe evaluarse no sólo por una determinada pena, sino también por su naturaleza y su impacto en los bienes jurídicos individuales y colectivos.

La jurisprudencia tanto europea como española respalda la utilización de datos obtenidos en procedimiento penales en otros ámbitos legales, como procedimientos administrativos e incluso en la apertura de una nueva causa penal. En este aspecto, la jurisprudencia del TEDH subraya que la cesión de datos obtenidos en procedimientos penales para otros fines debe cumplir con criterios de legalidad, proporcionalidad y garantías adecuadas para proteger los derechos individuales, alineándose con fines legítimos de interés público. Esta perspectiva refuerza la necesidad de lograr un equilibrio entre la eficacia en la persecución de delitos y la protección de derechos fundamentales, asegurando que las medidas adoptadas sean estrictamente necesarias y proporcionadas a los objetivos perseguidos.

En conclusión, la protección de datos personales en el contexto de la persecución de delitos requiere un delicado equilibrio entre las necesidades de seguridad y el respeto a los derechos fundamentales. La legislación vigente, tanto a nivel de la UE como nacional, establece un marco jurídico destinado a proteger estos derechos mediante la implementación de controles judiciales y criterios estrictos para la conservación y cesión de datos. La jurisprudencia del TJUE y el TEDH refuerza este enfoque, enfatizando la importancia de la proporcionalidad y la necesidad de criterios objetivos en la conservación de datos y cesión de datos personales, especialmente en relación con delitos graves. Es esencial la continua adaptación de la normativa y su interpretación por los tribunales para enfrentar los desafíos en la intersección entre la protección de datos y la persecución de delitos en la era digital.

Este estudio destaca la imperiosa necesidad de promover un enfoque integral que concilie la seguridad pública con el respeto a la privacidad y los derechos individuales. Solo a través de un equilibrio adecuado entre estos aspectos, basado en el imperativo ético de proteger la dignidad y la libertad de los ciudadanos, podremos construir una sociedad justa y democrática en la era digital, donde la tecnología y la ley converjan en armonía para el bienestar común.

6. BIBLIOGRAFÍA

6.1 General: manuales, publicaciones y revistas

CABALLERO TRENADO, L. (2018). "Acceso a comunicaciones electrónicas y tratamiento de datos personales: nuevo criterio. Comentario a la STJUE (Gran Sala) C-207/16, de 2 de octubre de 2018, sobre acceso de las autoridades nacionales a los datos para la investigación de un delito y umbral de gravedad del delito que puede justificar el acceso a los datos". Revista de Derecho, Empresa y Sociedad (REDS), Nº 13, pp. 363-367.

ESPARZA LEIBAR, I. (2018). "Protección de datos de carácter personal y proceso penal". En ETXEBARRIA ESTANKONA, K., ORDEÑANA GEZURAGA, I., y OTAZUA ZABALA, G. (Dirs), *Justicia con ojos de mujer: Cuestiones procesales controvertidas,* Editorial Tirant lo Blanch, pp. 931-932.

ESPARZA LEIBAR, I., (2022). "Derecho fundamental a la protección de datos de carácter personal en el ámbito jurisdiccional e Inteligencia Artificial. En especial la LO 7/2021, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales". En CALAZA LÓPEZ, S., y LLORENTE SÁNCHEZ-ARJONA, M. (Dirs), *Inteligencia artificial legal y administración de justicia,* Editorial Aranzadi, p. 196.

ETXEBERRIA GURIDI, J. F. (2009). "Principio de disponibilidad y protección de datos personales: a la búsqueda del necesario equilibrio en el espacio judicial penal europeo". En Eguzkilore: Cuaderno del Instituto Vasco de Criminología, Nº. 23, pp. 360-361.

ETXEBERRIA GURIDI, J. F. (2015). "La invalidez de la Directiva 2006/24/CE y su repercusión en el ordenamiento español (consecuencias de la STJUE de 8 de abril de 2014)". En GÓMEZ COLOMER, J., *El proceso penal en la encrucijada,* Universitat Jaume I, pp. 543-546.

GALÁN MUÑOZ, A. (2015). "La protección de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal en la Unión Europea". En COLOMER HERNÁNDEZ, I. (Dir), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea,* Editorial Aranzadi, pp. 42-51.

GONZÁLEZ CANO, M. I. (2019). "Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680". Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, pp. 1343-1346. Véase en https://doi.org/10.22197/rbdpp.v5i3.279

LÓPEZ AGUILAR, J. F. (2017). "La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EEUU". UNED, Teoría y Realidad Constitucional, núm. 39, pp. 574-575.

MARTÍNEZ VÁZQUEZ, F. (2021). "La nueva Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales". Diario La Ley Penal, Nº 9865, Sección Tribuna, 7 de Junio de 2021, Editorial Wolters Kluwer, p. 5.

PÉREZ ESTRADA, M. J. (2019). "La protección de datos personales en el registro de dispositivos de almacenamiento masivo de información". Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, pp. 1301-1302. Véase en https://doi.org/10.22197/rbdpp.v5i3.253

PÉREZ MANZANO, M. (2020). "Protección de datos personales: retos para el sistema penal". En CASAS BAAMONDE, M. E. (Coord), *El derecho a la protección de datos personales en la sociedad digital,* Fundación Ramón Areces, p. 87.

PESQUEIRA ZAMORA, M. J. (2020). "Diligencias de investigación, cesión de datos y principio de proporcionalidad". InDret, núm. 4, pp. 436-437. Véase en https://doi.org/10.31009/InDret.2020.i4.11

PIÑAR MAÑAS, J. L. (2020). "Derecho e innovación. Privacidad y otros derechos en la sociedad digital". En CASAS BAAMONDE, M. E. (Coord), *El derecho a la protección de datos personales en la sociedad digital*, Fundación Ramón Areces, p. 49.

POLO ROCA, A. (2021). "La regulación sobre la conservación de datos en el sector de las comunicaciones electrónicas o telecomunicaciones: estado de la cuestión". IDP. Revista de Internet, Derecho y Política, Nº. 33, pp. 5-7. Véase en http://dx.doi.org/10.7238/idp.v0i33.373811.

OROMÍ I VALL-LLOVERA, S. (2021). "El rol de las empresas tecnológicas en la cooperación policial y judicial y en las diligencias de investigación penal". En PEREIRA PUIGVERT, S., y ORDÓÑEZ PONZ, F. (Dirs), *Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos*, Editorial Aranzadi, pp. 827-828.

RODRÍGUEZ AYUSO, J. F. (2021). "Nueva regulación en el tratamiento de datos personales con fines públicos de prevención, detección, investigación, enjuiciamiento y ejecución de sanciones penales: la Ley 7/2021, de 26 de mayo". En PEREIRA PUIGVERT, S., y ORDÓÑEZ PONZ, F. (Dirs), *Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos*, Editorial Aranzadi, p. 655.

RODRÍGUEZ FERNÁNDEZ, R. (2022). "Protección de datos personales: normativa europea y nacional (especial referencia a la normativa de protección de datos en la prevención, detección, investigación y enjuiciamiento de infracciones penales)". La Ley Penal, Nº 157, Sección Legislación aplicada a la práctica, Julio-Agosto 2022, Editorial Wolters Kluwer.

RODRÍGUEZ LAINZ, J. L. (2008). "El principio de proporcionalidad en la nueva ley de conservación de datos relativos a las comunicaciones (I)". Diario La Ley, Nº 6859, Sección Doctrina, 14 de enero de 2008, Editorial Wolters Kluwer, pp. 7-12.

RODRÍGUEZ LAINZ, J. L. (2016). "El secreto de las telecomunicaciones y su interceptación legal: adaptado a la Ley Orgánica 13/2015, de reforma de la Ley de Enjuiciamiento Criminal". Sepín, p. 291.

RODRÍGUEZ LAINZ, J. L. (2019). "La transferencia de datos obtenidos en el curso de una medida de investigación tecnológica a la luz de la Directiva (UE) 2016/680". En COLOMER HERNÁNDEZ, I., OUBIÑA BARBOLLA, S., y CATALINA BENAVENTE, M. Á. (Dirs), *Uso y Cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios*, Editorial Aranzadi, pp. 341-342.

RODRÍGUEZ LAINZ, J. L. (2022). "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". Diario La Ley, Nº 10058, Sección Tribuna, 28 de Abril de 2022, Editorial Wolters Kluwer.

RODRÍGUEZ LAINZ, J. L. (2024). "El ordenamiento jurídico español frente a la nueva doctrina del TJUE sobre utilización de datos obtenidos en el curso de una investigación criminal en otros procedimientos penales o administrativos (1)". Diario La Ley, Nº 10478, Sección Tribuna, 4 de Abril de 2024, Editorial Wolters Kluwer.

RUGGERI, E. (2022). "Principio de disponibilidad y libre circulación de evidencias y datos personales en Europa. Nuevas garantías y nuevos riesgos para los derechos individuales". En COLOMER HERNÁNDEZ, I., CATALINA BENAVENTE, M. Á., y OUBIÑA BARBOLLA, S. (Dirs), *Uso de la información y de los datos personales en los procesos: los cambios en la era digital*, Editorial Aranzadi, pp. 330-335.

SOBRINO GARCÍA, I. (2019). "Protección de datos y privacidad. Estudio comparado del concepto y desarrollo entre la Unión Europea y Estados Unidos". Revista de Derecho UNED, núm. 25, p. 691.

6.2 Jurídica: normativa y jurisprudencia

Unión Europea. Convenio de Roma de 4 de noviembre de 1950, para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Adhesión de la Unión Europea en su versión consolidada tras las modificaciones introducidas por el Tratado de Lisboa, firmado el 13 de diciembre de 2007.

Unión Europea. Convenio celebrado por el Consejo de conformidad con el artículo 34 del Tratado de la Unión Europea, relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea - Declaración del Consejo sobre el apartado 9 del artículo 10 - Declaración del Reino Unido sobre el artículo 20. *DOUE, nº. 197,* de 12 de julio de 2000. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:42000A0712(01)

Unión Europea. Convenio N° 185, del Consejo de Europa, sobre la Ciberdelincuencia. Hecho en Budapest el 23 de noviembre de 2001.

Unión Europea. Carta de los Derechos Fundamentales de la Unión Europea. *DOUE, C 202/389*, de 7 de junio de 2016. Disponible en: http://data.europa.eu/eli/treaty/char_2016/oj

Unión Europea. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. *DOUE, L 119/1,* de 4 de mayo de 2016. Disponible en: http://data.europa.eu/eli/reg/2016/679/oj

Unión Europea. Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales. *DOUE, L 191/118*, de 28 de julio de 2023. Disponible en: http://data.europa.eu/eli/reg/2023/1543/oj

Unión Europea. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *DOUE, L*

281, de 23 de noviembre de 1995. Disponible en: http://data.europa.eu/eli/dir/1995/46/oj

Unión Europea. 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). *DOUE, L 201,* de 31 de julio de 2002. Disponible en: http://data.europa.eu/eli/dir/2002/58/oj

Unión Europea. Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. *DOUE, L 105/54*, de 13 de abril de 2006. Disponible en: http://data.europa.eu/eli/dir/2006/24/oj

Unión Europea. Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. *DOUE, L 119/89*, 4 de mayo de 2016. Disponibleen: http://data.europa.eu/eli/dir/2016/680/oj

Unión Europea. Directiva (UE) 2023/1544 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales. *DOUE, L 191/181*, de 28 de julio de 2023. Disponible en: http://data.europa.eu/eli/dir/2023/1544/oj

Unión Europea. Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. *DOUE, L 350/60*, de 30 de diciembre de 2008. Disponible en: http://data.europa.eu/eli/dec_framw/2008/977/oj

Unión Europea. Declaración sobre la lucha contra el terrorismo, emitida por el Consejo Europeo el 25 de marzo de 2004.

España. Constitución Española. *BOE, núm. 311,* de 29 de diciembre de 1978. Disponible en: https://www.boe.es/eli/es/c/1978/12/27/(1)/con

España. Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal. *BOE, núm. 11*, de 13 de enero de 1982. Disponible en: https://www.boe.es/eli/es/l/1981/12/30/50/con

España. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. *BOE, núm. 157*, de 02 de julio de 1985. Disponible en: https://www.boe.es/eli/es/lo/1985/07/01/6/con

España. Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. *BOE, núm. 262,* de 31 de octubre de 1992. Disponible en: https://www.boe.es/eli/es/lo/1992/10/29/5

España. Ley Orgánica 5/1995, de 22 de mayo, del Tribunal del Jurado. *BOE, núm. 122,* de 23 de mayo de 1995. Disponible en: https://www.boe.es/eli/es/lo/1995/05/22/5/con

España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *BOE, núm. 281,* de 24 de noviembre de 1995. Disponible en: https://www.boe.es/eli/es/lo/1995/11/23/10/con

España. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *BOE, núm. 298,* de 14 de diciembre de 1999. Disponible en: https://www.boe.es/eli/es/lo/1999/12/13/15/con

España. Ley Orgánica 15/2003, de 25 de noviembre, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *BOE, núm. 283,* de 26 de noviembre de 2003. Disponible en: https://www.boe.es/eli/es/lo/2003/11/25/15

España. Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica sobre las medidas de investigación limitativas de derechos constitucionales. *BOE, núm. 239,* de 6 de octubre de 2015. Disponible en: https://www.boe.es/eli/es/lo/2015/10/05/13

España. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *BOE, núm. 294*, de 06 de diciembre de 2018. Disponible en: https://www.boe.es/eli/es/lo/2018/12/05/3/con

España. 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. *BOE, núm. 126*, de 27 de mayo de 2021. Disponible en: https://www.boe.es/eli/es/lo/2021/05/26/7/con

España. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. *BOE, núm. 166*, 12 de julio de 2002. Disponible en: https://www.boe.es/eli/es/l/2002/07/11/34/con

España. Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. *BOE, núm. 264*, de 4 de noviembre de 2003. Disponible en: https://www.boe.es/eli/es/l/2003/11/03/32

España. Ley 58/2003, de 17 de diciembre, General Tributaria. *BOE, núm. 302*, de 18 de diciembre de 2003. Disponible en: https://www.boe.es/eli/es/l/2003/12/17/58/con

España. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. *BOE, núm. 251*, de 19 de octubre de 2010. Disponible en: https://www.boe.es/eli/es/l/2007/10/18/25/con

España. Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. *BOE, núm. 114*, de 10 de mayo de 2014. Disponible en: https://www.boe.es/eli/es/l/2014/05/09/9/con

España. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. *BOE, núm. 236*, de 02 de octubre de 2015. Disponible en: https://www.boe.es/eli/es/l/2015/10/01/39/con

España. Ley 11/2022, de 28 de junio, General de Telecomunicaciones. *BOE, núm 155*, de 29 junio de 2022. Disponible en: https://www.boe.es/eli/es/l/2022/06/28/11

España. Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. *BOE, núm 260*, de 17 de septiembre de 1882. Disponible en: https://www.boe.es/eli/es/rd/1882/09/14/(1)/con

España. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. *BOE, núm. 17,* de 19 de enero de 2008. Disponible en: https://www.boe.es/eli/es/rd/2007/12/21/1720/con

España. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso. *BOE, núm. 284*, de 25 de noviembre de 2011. Disponible en: https://www.boe.es/eli/es/rd/2011/11/18/1708/con

España. Orden PRE/199/2013, de 29 de enero, por la que se define el formato de entrega de los datos conservados por los operadores de servicios de comunicaciones electrónicas o de redes públicas de comunicaciones a los agentes facultados. *BOE, núm. 40*, de 15 de febrero de 2013. Disponible en: https://www.boe.es/eli/es/o/2013/01/29/pre199

España. Circular 2/2019, de 6 de marzo, de la Fiscal General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas. *BOE, núm. 70*, de 22 marzo de 2019. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4241

España. Informe Jurídico de la AEPD, N/REF: 0030/2021. Disponible en: https://www.aepd.es/documento/2021-0030.pdf

Unión Europea. Sentencia del Tribunal Europeo de Derechos Humanos 28341/1995, de 4 de mayo de 2000, Caso Rotaru contra Rumania.

Unión Europea. Sentencia del Tribunal Europeo de Derechos Humanos 23618/94, de 24 de agosto de 1998, Caso LAMBERT v. Francia.

Unión Europea. Sentencia del Tribunal Europeo de Derechos Humanos (Sección 4ª) 57752/00, de 29 de marzo de 2005, Caso MATHERON v. Francia.

Unión Europea. Sentencia del Tribunal Europeo de Derechos Humanos (Sección 3ª) 28005/12, de 7 de julio de 2015, Caso M.N y otros v. San Marino.

Unión Europea. Sentencia del Tribunal Europeo de Derechos Humanos (Sección 5ª) 49176/11, de 16 de junio de 2016, Caso VERSINI-CAMPINCHI y CRASNIANKI v. Francia.

Unión Europea. Sentencia del Tribunal Europeo de Derechos Humanos (Sección 5ª) 33242/12, de 29 de junio de 2017, Caso TERRAZZONI v. Francia.

Unión Europea. Sentencia del Tribunal Europeo de Derechos Humanos (Sección 2ª) 14833/18, de 18 de enero de 2022, Caso ADOMAITIS v. Lituania.

Unión Europea. Sentencia del Tribunal Europeo de Derechos Humanos (Sección 5ª) 2800/16, de 16 de mayo de 2023, Casos SHIPS WASTE OIL COLLECTOR B.V v. Holanda, BURANDO HOLDING B.V y PORT INVEST B.V v. Holanda, JANSSEN DE JONG GROEP B.V. y otros v. Holanda.

Unión Europea. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12.

Unión Europea. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15.

Unión Europea. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 2 de octubre de 2018, C-207/16.

Unión Europea. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 6 de octubre de 2020, asunto C-623/17.

Unión Europea. Sentencia del Tribunal de Justicia de la Unión Europea (Sala Octava) de 25 de abril de 2021, asunto C-658/19.

Unión Europea. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 5 de abril de 2022, asunto C-140/20.

Unión Europea. Sentencia del Tribunal de Justicia de la Unión Europea (Sala Sexta) de 7 de marzo de 2024, asunto C-740/22.

España. Sentencia del Tribunal Constitucional (Pleno) 292/2000, de 30 de noviembre de 2010.

España. Sentencia del Tribunal Constitucional (Pleno) 17/2013, de 31 de enero de 2013.

España. Sentencia del Tribunal Constitucional (Sala Segunda) 67/2020, de 29 de junio de 2020.

España. Sentencia del Tribunal Supremo (Sala Segunda) 727/2020, 23 de marzo de 2021.