Estudios de Deusto

Revista de Derecho Público

Vol. 73/2 julio-diciembre 2025

DOI: https://doi.org/10.18543/ed7322025

MONOGRÁFICO

POLÍTICA CRIMINAL EUROPEA Y ACTOS DE INVESTIGACIÓN PENAL EN LOS DELITOS CONTRA EL MEDIOAMBIENTE

European Criminal Policy and criminal investigations in environmental crimes

Carmen Rodríguez Rubio
Profesora Permanente Laboral de Derecho Procesal
Universidad Rey Juan Carlos, Madrid. España
https://orcid.org/0000-0001-9335-0138

https://doi.org/10.18543/ed.3451

Fecha de recepción: 23.09.2025
Fecha de aprobación: 16.12.2025
Fecha de publicación en línea: diciembre 2025

POLÍTICA CRIMINAL EUROPEA Y ACTOS DE INVESTIGACIÓN PENAL EN LOS DELITOS CONTRA EL MEDIOAMBIENTE[1]

European Criminal Policy and criminal investigations in environmental crimes

Carmen Rodríguez Rubio[2]
Profesora Permanente Laboral de Derecho Procesal
Universidad Rey Juan Carlos, Madrid. España
https://orcid.org/0000-0001-9335-0138

https://doi.org/10.18543/ed.3451

Fecha de recepción: 23.09.2025
Fecha de aprobación: 16.12.2025
Fecha de publicación en línea: diciembre 2025

Resumen

En el presente trabajo se ha procedido al examen de la legislación y de la jurisprudencia con el objetivo de analizar la lucha contra el crimen organizado y la delincuencia grave en la Unión Europea. Con este objetivo se han utilizado diversos instrumentos como parte integrante de la política criminal comunitaria. Desde este punto de vista, la Comisión Europea estableció diversas prioridades esenciales en la seguridad común a través de la Agenda Europea de Seguridad de 2015. Dentro de las preferencias europeas para combatir la criminalidad se dispuso expresamente la lucha contra los delitos medioambientales. Con esta finalidad se han efectuado diversas actuaciones que han dado lugar a diferentes instrumentos legales. Principalmente, en la lucha contra la criminalidad medioambiental, ha sido la Directiva (UE)

[1] Este trabajo se ha elaborado en el marco del proyecto titulado «Derecho Ambiental y el espacio judicial europeo: mecanismos de actuación y cooperación». Entidad financiadora: Comunidad de Madrid. Referencia externa: LÍNEA A, CP2301.

[2] Email: mariacarmen.rodriguez@urjc.es

2024/1203 la que se ha manifestado en torno a los actos de investigación que pueden realizarse en los procesos penales cuyo fin sea la persecución de este tipo de crímenes.

Palabras clave

Política criminal; Directivas europeas; Investigación penal; Medioambiente

Abstract

This paper examines legislation and case law to analyze the fight against organized crime and serious crime in the European Union. To this end, various instruments have been used and integral part of EU criminal policy. From this perspective, the European Commission established several key priorities for common security through the 2015 European Agenda on Security. Among the European priorities for combating crime, the fight against environmental crimes was expressly included. To this end, various actions have been undertaken, resulting in different legal instruments. Primarily, in the fight against environmental crime, Directive (EU) 2024/1203 has addressed investigative acts that can be carried out in criminal proceedings aimed at prosecuting this type of crime.

Key words

Criminal Policy; European Directives; Criminal Investigation; Environment

Sumario: I. Introducción. II. Averiguación de información financiera. III. Intervención de las comunicaciones telefónicas y telemáticas. IV. Datos electrónicos de tráfico o asociados incorporados al proceso. V. Registro de dispositivos electrónicos. VI. Entregas vigiladas. VII. Agente encubierto y agente encubierto informático. VIII. Conclusiones. IX. Referencias.

I. INTRODUCCIÓN

Desde el ámbito público los Estados han realizado diferentes planteamientos para tratar el fenómeno criminal. De este modo, se ha pretendido dar una respuesta desde los poderes públicos a los distintos desafíos que presenta la criminalidad. En tal sentido, la Política Criminal analiza las distintas posiciones que sigue la legislación penal, teniendo en consideración tanto las leyes penales como las de carácter procesal penal (Borja Jiménez, 2003: 22-35). Por otro lado, como se ha puesto de manifiesto, hay un cambio de actitud frente a determinadas conductas que en la actualidad se estima que han de recibir un mayor reproche penal (Hassemer, W., Muñoz Conde, 2012: 14-17).

En nuestros días la lucha contra el delito trasciende del propio Estado, esta circunstancia se debe principalmente a que la sociedad actual se ha organizado conforme a diferentes estructuras internacionales. Así, hoy por hoy, el proceso de internacionalización ha alcanzado un carácter global, como se ha llegado a afirmar "el conjunto de la humanidad está organizado". Los organismos que operan en el presente son principalmente de dos tipos, es decir, de un lado, los que tienen un carácter universal y, de otro, los que destacan por tener un carácter restringido (Barbé, 2020:185-302).

En torno a este tipo de organizaciones, las restringidas han limitado, en función de diversos criterios, los Estados que pueden formar parte de estas instituciones. Se ha estimado que el crecimiento de organizaciones internacionales se debe fundamentalmente al aumento de este tipo de estructuras internacionales, principalmente a partir de 1945 y hasta la actualidad. Se entiende que ha existido una primera oleada en este tipo de organizaciones desde el final de la Segunda Guerra Mundial hasta la década de 1970. Dicha afluencia dio lugar, entre otras cosas, a la Comunidad Económico-Europea, que se contempla como un caso singular que originó un genuino proceso de integración entre sus miembros (Barbé, 2020: 185-302).

Ahora bien, la presente sociedad internacional destaca por la interrelación entre sus miembros, siendo este el motivo de la existencia de un gran número de organizaciones internacionales. De este modo se produce una colaboración entre Estados para abordar problemas generales y para dar una respuesta

más eficaz a cuestiones particulares. No obstante, se ha considerado que las organizaciones internacionales no han relegado a los Estados ni tampoco han llegado a cambiar especialmente la configuración entre Estados que presenta la comunidad internacional (Casado Raigón, 2020: 43-61).

La importancia que han adquirido las organizaciones internacionales en la sociedad actual se puede constatar actualmente en la propia existencia de la Unión Europea (en adelante, UE). Desde el punto de vista jurídico esta organización cuenta con el derecho originario y también con el derecho producido por la propia UE, es decir, con los actos procedentes de sus instituciones, dichos actos son conocidos como derecho derivado. Por medio de los citados instrumentos, principalmente, a través de las directivas, se consigue la armonización de las legislaciones nacionales en el ámbito del ordenamiento jurídico comunitario, estimándose el acto más novedoso del derecho de la UE (Alcaide Fernández, Casado Raigón, 2019: 183-206).

Asimismo, los distintos actos de esta organización internacional sirven de cauce para establecer una política común contra la criminalidad en los diferentes Estados. Como se ha señalado, la UE se ha constituido como una entidad institucional con amplias funciones legislativas para aproximar las legislaciones de sus miembros (Corral Maraver, 2020: 9-15). De este modo, la UE ha dado prioridad a la lucha contra la delincuencia organizada, concretamente, el Consejo Europeo ha hecho hincapié en combatir la delincuencia medioambiental, pues este tipo de criminalidad es una de las actividades más lucrativas del mundo con consecuencias en el medioambiente y en la salud de las personas. En particular, ha sido la Directiva (UE) 2024/1203 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, relativa a la Protección del Medioambiente mediante el Derecho Penal y por la que se sustituyen las Directivas 2008/99/CE y 2009/123/CE, el instrumento de armonización en esta materia.

Entre los propósitos de la Directiva, más arriba mencionada, se encuentra la mejora de la investigación, del enjuiciamiento y de las resoluciones judiciales dictadas en los procedimientos por la comisión de este tipo de hechos delictivos. Igualmente, se alude a cómo se debe tener presente la implicación en estos delitos de grupos delictivos organizados, debiéndose abordar en estos procesos: la corrupción, el blanqueo de capitales, la ciberdelincuencia y el fraude documental, añadiendo que en las actividades empresariales también está presente el máximo beneficio, así como el ahorro de gastos.

Con el fin de garantizar satisfactoriamente el cumplimiento del Derecho Penal en materia de medioambiente, los Estados miembros deben poner a disposición de las autoridades competentes medios de investigación eficaces para los delitos medioambientales, como los que existen en su legislación para combatir la delincuencia organizada u otros delitos graves. La utilización de tales medios se hará en el caso y en la medida en que dichos medios

sean adecuados y proporcionados a la naturaleza y la gravedad de los delitos de acuerdo con el ordenamiento jurídico nacional. En relación con la gravedad de los delitos medioambientales se ha de tener presente que, de acuerdo con Interpol y Naciones Unidas, este tipo de crímenes se encuentra en tercer o cuarto lugar en cuanto a volumen de negocio ilegal, y por delante solo estarían el tráfico de drogas, los delitos en materia de propiedad industrial e intelectual y el tráfico y trata de personas (Alfaro Moreno, 2023: 31-48).

Entre esas herramientas cabría incluir la interceptación de comunicaciones, la vigilancia discreta (en particular la vigilancia electrónica) las entregas vigiladas, el control de cuentas bancarias y otros instrumentos de investigación financiera. Estos instrumentos deben utilizarse de conformidad con el principio de proporcionalidad y cumpliendo la Carta. De igual forma, se ha de respetar imperativamente el derecho a la protección de los datos personales. En definitiva, una vez expuestos los antecedentes de la Directiva 2024/1203, se exponen a continuación los actos de investigación que, sin ánimo de exhaustividad, podrán tener lugar en las investigaciones penales por la comisión de delitos contra el medioambiente.

II. AVERIGUACIÓN DE INFORMACIÓN FINANCIERA

La Directiva 2019/1153 del Parlamento y el Consejo, de 20 de junio de 2019, estableció unas normas destinadas a facilitar el uso de información financiera para la prevención, detección, investigación y enjuiciamiento de infracciones penales (www.boe.es). Dicha Directiva forma parte de la Agenda Europea de Seguridad de 2015. En relación con este marco de acción comunitario, la Comisión presentó una comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones en 2015. En dicho documento se recogieron diversas prioridades esenciales en la seguridad europea, a saber, la lucha contra el terrorismo y la prevención de la radicalización, el desmantelamiento de la delincuencia organizada y la lucha contra la ciberdelincuencia (Agenda Europea de Seguridad 2015).

En cuanto a la segunda preferencia, es decir, la desarticulación de la delincuencia organizada, el ciclo de actuación de la UE, según el comunicado, había conseguido una mayor coordinación de la estrategia política y también de las operaciones conjuntas en marcha. Además, puso de manifiesto como el objetivo más importante de la delincuencia organizada es el beneficio, por esta razón se ponía de relieve cómo las entidades con funciones coercitivas han de centrar su atención en la financiación de estas redes. A su vez ponía de manifiesto la relación del crimen organizado con la corrupción, el fraude, la falsificación y el contrabando. Igualmente, la Comisión exponía como las redes delictivas se sirven de las estructuras empresariales

legales para esconder el origen de sus beneficios. Por este motivo es necesario actuar para tratar la introducción de la delincuencia organizada en la economía legal.

Para abordar este tipo de delincuencia se acordó el paquete contra el blanqueo de capitales con el fin de identificar y realizar el seguimiento de transferencias de dinero sospechosas y conseguir un intercambio eficaz de información entre las Unidades de Información Financiera (en adelante, UIF). De esta manera la Comisión se propuso establecer una política en los países con deficiencias en sus regímenes de lucha contra el blanqueo de capitales y financiación del terrorismo. En tal sentido, se afirma que la vinculación más visible de los delitos medioambientales se encuentra en los delitos financieros, siendo uno de estos el blanqueo de capitales (Alfaro Moreno, 2023, pp. 31-48). Asimismo, hay que tener presente que las redes que financian el crimen organizado, a su vez, también facilitan el blanqueo de capitales, trasladando grandes cantidades de efectivo fuera del ámbito europeo con el fin de incluirlo en la estructura bancaria (Balas Dávila, 2023, pp. 49-70).

Además, en esta comunicación la Comisión se refirió expresamente a los delitos medioambientales pues su comisión puede causar importantes daños al medioambiente y a la salud humana, así como reducir los ingresos públicos e imponer gastos de saneamiento a los contribuyentes como puede suceder con los traslados ilícitos y posteriores vertidos de residuos. Asimismo, hay que tener presente que el comercio de especies silvestres representa una amenaza para la biodiversidad y en las regiones de origen, como puede ser África, un peligro para el desarrollo sostenible y la estabilidad regional.

En este comunicado la Comisión se comprometió a estudiar la necesidad de controlar el cumplimiento y la ejecución a través de distintas medidas, a saber, la formación del personal responsable perteneciente a los órganos con funciones coercitivas, el apoyo de redes profesionales y por medio del acercamiento de las sanciones por infracciones penales en los países de la UE.

Igualmente, la Comisión puso de relieve el papel que desempeñan las autoridades locales en la lucha contra el crimen organizado, contando también con jueces y policía. También destacó como la actuación de la delincuencia organizada, aunque es global actúa a nivel local por lo que hay que adoptar una perspectiva multidisciplinar para su prevención y para luchar contra esta.

En tal sentido, las autoridades locales son las primeras que han de prevenir la introducción del crimen organizado en la economía y deberían contar con instrumentos para compartir información con otras administraciones y autoridades. Igualmente se puso de manifiesto en la importancia de la Red Europea de Prevención de la Delincuencia, organismo que cuenta con el apoyo financiero de la UE. Entre las acciones destacadas por la Comisión se

presentó la revisión de la política y la legislación sobre delitos contra el medioambiente para sus propuestas en el 2016.

En cuanto a la Directiva 2019/1153, de conformidad con su articulado, se establecen medidas para facilitar el acceso a la información financiera y de cuentas bancarias, además se prevé su uso por las autoridades competentes con la finalidad de prevenir, detectar, investigar o enjuiciar las infracciones penales graves. Igualmente, recoge medidas dirigidas a facilitar el acceso a la información de los servicios de seguridad de las UIF para prevenir y luchar contra el blanqueo de capitales, los delitos en los que haya conexión y las medidas para facilitar la cooperación entre las unidades anteriormente mencionadas.

La Directiva examinada parte de la siguiente premisa, a saber: los Estados pertenecientes a la UE deben garantizar que las autoridades nacionales competentes estén facultadas para acceder directa e inmediatamente a la información relacionada con cuentas bancarias cuando sea preciso para la realización de las funciones relacionadas con la persecución criminal. Particularmente, el art. 4 determina este tipo de actuación para "la prevención, detección, investigación o enjuiciamiento de un delito grave o para apoyar la investigación en relación con un delito grave, incluida la identificación, la localización y la inmovilización de los activos relacionados con dicha investigación".

Para acceder a las cuentas bancarias hay que tener presente que solamente podrán hacerlo las personas que hayan sido designadas para efectuar dichas tareas, además para la realización de estos fines se debe velar por la confidencialidad y por la protección de datos. Por otra parte, los registros centralizados deben llevar un examen de las veces que las autoridades competentes acceden a la información sobre las cuentas bancarias, detallando el nombre de la autoridad competente designada que haya realizado el registro.

También la Directiva 2019/1153 establece el intercambio de información entre las UIF de los diferentes Estados miembros. De esta manera en casos excepcionales y urgentes, las UIF de los diferentes países europeos están autorizadas a intercambiar información financiera relacionada con el terrorismo y delincuencia organizada conectada con el terrorismo, incluso este intercambio de información podrá realizarse rápidamente. Adicionalmente el intercambio de información entre UIF de los diferentes países europeos podrá tener lugar cuando la infracción financiera se precise en la lucha contra el blanqueo de capitales, delitos conexos y financiación del terrorismo. De igual modo el intercambio de información podrá efectuarse con Europol.

El resultado de la transposición de la Directiva 2019/1153 ha sido la Ley Orgánica 9/2022, de 28 de julio, por la que se establecen ormas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales, de modificación de la Ley Orgánica 8/1980, de 22 de septiembre, de financiación de las

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

De acuerdo con la introducción de la ley arriba mencionada, la UE se ha enfocado en la lucha contra la delincuencia grave, particularmente contra el fraude financiero, el blanqueo de capitales y la financiación del terrorismo. Por esta razón, el acceso a los delitos financieros y su intercambio resulta imprescindible en la persecución del delito. Sin embargo, hay que tener en consideración que el acceso a la información financiera está relacionado directamente con el derecho a la intimidad de los ciudadanos reconocido en el art. 18.4 de la Constitución Española (en adelante, CE) donde se reconoce que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de sus ciudadanos y el pleno ejercicio de sus derechos". Asimismo, la protección de dichos derechos está reconocida en el Convenio Europeo de Derechos Humanos (art. 8) y en el art. 16 del Tratado de Funcionamiento de la Unión Europea.

Además, siguiendo el preámbulo de la ley, el Tribunal Constitucional (en adelante, TC) en Sentencia 292/2000, de 30 de noviembre, declaró la existencia del derecho fundamental a la protección de datos y en la mencionada resolución, reconoció el derecho fundamental a la protección de datos de carácter personal como una categoría autónoma y distinta del derecho a la intimidad. Dicha sentencia coincidió en el tiempo con otras del Tribunal Europeo de Derechos Humanos (en adelante, TEDH) que consideran la protección de datos como derecho fundamental autónomo y que permite a su titular disponer y controlar sus propios datos personales.

De conformidad con el articulado de la ley, la norma tiene como fin facilitar el acceso a la información financiera, y a la información del Fichero de Titularidades Financieras y a su utilización por las autoridades competentes para la persecución de infracciones penales graves. En relación con la gravedad de los hechos delictivos se ha de considerar que, según la ley examinada, los delitos graves son los reconocidos como tales en el Anexo I del Reglamento (UE) 2016/794.

En virtud del mencionado reglamento son numerosas las infracciones que permiten acceder a información bancaria. A los efectos que aquí interesan es importante saber que se podrá obtener información financiera en las investigaciones sobre: delincuencia organizada, blanqueo de capitales, falsificación de documentos administrativos, tráfico ilícito de especies animales protegidas y en delitos contra el medioambiente (incluida la contaminación procedente de buques).

En lo referente a las autoridades y órganos autorizados para acceder al Fichero de Titularidades Financieras, la Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, en su art. 43.3 dispone quién puede tener conocimiento de dicha información. De

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 73/2, julio-diciembre 2025, págs. 327-358
https://doi.org/10.18543/ed.3451 • http://www.revista-estudios.deusto.es/

esta manera podrán tener acceso a información financiera los órganos jurisdiccionales con competencias en investigación de infracciones penales, el Ministerio Fiscal y la Fiscalía Europea, las Fuerzas y Cuerpos de Seguridad del Estado y la Policía Autonómica con competencia en la investigación de delitos graves. Igualmente podrán acceder, los organismos de recuperación de activos (incluida la Oficina de Recuperación y Gestión de Activos) la Secretaría de la Comisión de vigilancia de Actividades de Financiación del Terrorismo, el Centro Nacional de Inteligencia y la Agencia Estatal de Administración Tributaria.

El Fichero de Titularidades Financieras es un fichero de titularidad pública y su tratamiento está atribuido al Sepblac, siendo su responsable la Secretaría de Estado de Economía y Apoyo a la Empresa (www.sepblac.es). Este fichero se ha constituido como un instrumento de investigación financiera de acceso restringido a través del cual se puede tener conocimiento sobre determinados productos financieros. En particular, contiene información relativa a la apertura y cancelación de cuentas corrientes, cuentas de ahorro, cuentas de valores y depósitos a plazo que las entidades de crédito están obligadas a comunicar al Sepblac.

Resulta importante señalar que a través de la información financiera obtenida por medio del acceso a datos bancarios en investigaciones penales se puede obtener información relevante para las indagaciones policiales y judiciales. En este sentido, el Tribunal Supremo en la Sentencia 434/2021, de 20 de mayo de 2021 (www.iberley.es) tuvo ocasión de pronunciarse sobre el acceso a información bancaria por parte de la policía y su incidencia en el derecho fundamental a la intimidad (art. 18 CE). Es preciso señalar que dicha resolución es anterior a la Ley Orgánica 9/2022, de 28 de julio, por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales, de modificación de la Ley Orgánica 8/1980, de 22 de septiembre, de financiación de las Comunidades Autónomas y otras disposiciones conexas y de modificación de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Dicha ley, como se ha mencionado con anterioridad, es el resultado de la transposición de la Directiva 2019/1153 del Parlamento y el Consejo, de 20 de junio de 2019, que estableció unas normas destinadas a facilitar el uso de información financiera para la prevención, detección, investigación y enjuiciamiento de infracciones penales.

En los hechos recogidos en la sentencia citada anteriormente se relata como el Juzgado de instrucción núm. 4 de Fuenlabrada (Madrid) instruyó un proceso abreviado por delitos contra la Hacienda Pública, blanqueo de capitales y asociación ilícita contra varias personas. Una vez concluido el procedimiento lo remitió a la Audiencia Provincial de Madrid y el día 4 de marzo de 2019 este tribunal procedió a dictar sentencia. En dicha resolución se

declaró probado que varios acusados con nacionalidad china y residentes en España realizaban una actividad consistente en recibir dinero de terceros enviando dichos fondos a China, constituyendo para este fin varias sociedades mercantiles. Tras el enjuiciamiento hubo sendas condenas por delitos contra la Hacienda Pública, blanqueo de capitales y falsificación de documento público.

Se presentó recurso extraordinario de casación fundamentado en varios motivos, tres de estas causas se apoyaban en distintas infracciones constitucionales a través del art. 852 de la Ley de Enjuiciamiento Criminal (en adelante, LECRIM). En una de las causas en las que se sustentaba el recurso se alegaba la violación del derecho al secreto bancario por parte de la policía. En este motivo se aducía la vulneración de precepto constitucional por la lesión del derecho a la intimidad (art. 18 CE en relación con el art. 11 de la Ley Orgánica del Poder Judicial) así como la lesión del principio de legalidad penal (art. 25 CE) y la lesión del derecho a la tutela judicial efectiva (art. 24 CE).

En lo referente a la lesión del derecho a la intimidad, en el medio de impugnación presentado se adujo cómo buena parte de las actuaciones investigadoras desarrolladas por la policía se realizó sin autorización judicial. De esta manera, según el recurrente, se había accedido a datos bancarios y personales sin que los agentes estuvieran legitimados. De acuerdo con el pronunciamiento del tribunal dicho motivo no podía ser estimado. De conformidad con lo manifestado por el Tribunal Supremo (en adelante, TS) "lo que el artículo 18.1 CE garantiza es, por tanto, el secreto sobre la propia esfera de vida personal y, por tanto, veda a terceros, particulares o poderes públicos, decidir sobre los contornos de la vida privada".

No obstante, en palabras del TS, el derecho a la intimidad puede ser limitado, siempre y cuando la limitación esté prevista en la ley y su práctica sea por presupuestos de proporcionalidad y razonabilidad. Por esta razón, debe justificarse de forma adecuada la necesidad e idoneidad de la medida limitativa y el equilibrio entre el sacrificio del derecho y los objetivos de la investigación. Sin embargo, el TS señaló como la CE no determina quién puede ordenar una injerencia en el derecho a la intimidad, lo que llevó al tribunal a examinar la jurisprudencia constitucional y europea.

Como consecuencia de esta apreciación el TS llega a la conclusión de que la policía "estará constitucionalmente habilitada para realizar investigaciones que supongan una injerencia no grave o leve en el derecho a la intimidad" y además exista habilitación legal y proporcionalidad. Asimismo, con posterioridad, se ha de poner a disposición de la autoridad judicial los datos obtenidos, existiendo de este modo un control jurisdiccional de la actividad policial.

De esta manera, el TS considera que la actuación de la policía que permitió identificar a las personas jurídicas titulares de cuentas bancarias donde se

realizaban determinados ingresos estaba amparada en normas habilitantes. Con este fin, el TS citó las Directivas 2005/60, 2015/849 y 2018/843 del Parlamento Europeo y del Consejo relativas a la Prevención del Blanqueo de Capitales y la Financiación del Terrorismo y a nivel interno mencionó la Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo. Atendiendo a estas argumentaciones, el TS concluyó que la actividad de la policía había sido necesaria y proporcional. Además, el acceso de la policía no había supuesto una injerencia en el derecho a la intimidad superior a lo que la propia policía podía realizar sin autorización judicial ni por más tiempo de lo necesario.

III. INTERVENCIÓN DE LAS COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS

En lo referente a la intervención de las comunicaciones telefónicas nos hallamos ante un acto de investigación que se introdujo tardíamente en la LECRIM, en especial, tuvo lugar por medio de Ley Orgánica 4/1988, de 25 de mayo, dando lugar a la modificación del art. 579 de la ley procesal penal. En esta materia se dictaron diferentes resoluciones procedentes del TEDH que fueron un elemento esencial en la nueva regulación de la diligencia. Dichos pronunciamientos afectaron a España, así, la Sentencia de 30 de julio de 1998 (Caso Valenzuela c. España) y también la Sentencia de 18 de febrero de 2003 (Caso Prado Bugallo c. España) en la que el Tribunal de Estrasburgo puso de manifiesto como la modificación introducida por la Ley 4/1988, de 25 de mayo, no se correspondía con lo mantenido en su jurisprudencia (Gómez Colomer, 2008, pp.162-182).

A este respecto, el pronunciamiento del TEDH expresó con claridad que la modificación operada era incompleta debido a que en la nueva ley se encontraban vacíos normativos que ya se habían expuesto con anterioridad, a saber: no se precisaban los delitos en los que la injerencia podía tener lugar; no se establecía un límite temporal en la medida ya que se admitían prórrogas indefinidas y como añadidura, no se recogía el modo de llevarse a cabo el acto de investigación, ni tampoco la forma de conservar de manera íntegra las conversaciones intervenidas. Pero no solo los pronunciamientos del TEDH pusieron de manifiesto la obsolescencia de la ley procesal en esta materia, sino que también el TC en reiterada jurisprudencia fue perfilando el modo en el que la intervención de las comunicaciones debía regularse de una manera novedosa desde el punto de vista legal.

Tras la última modificación operada a través de la Ley 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, se han incluido importantes avances en el acto

de investigación examinado, además se han incorporado una serie de requisitos que se aplican a todos los actos de investigación tecnológica (Rodríguez Lainz, 2025). En este contexto hay que tener en consideración que las diligencias tecnológicas han carecido de una reglamentación legal en la ley procesal y, que únicamente, la intervención de las comunicaciones ha estado regulada, aunque de manera insuficiente (Álvarez Sánchez de Movellán, 2019: 297-308). Asimismo, teniendo en consideración la ley mencionada, se ha afirmado que el legislador se ha decantado por una regulación garantista en la consecución de la prueba digital (Escudero García-Calderón, 2022: 381).

En relación con esas disposiciones comunes, la ley recoge primeramente los principios rectores que informan la adopción de alguna de las medidas de naturaleza tecnológica. En consecuencia, cuando se autorice judicialmente la medida esta deberá estar fundamentada en los principios de especialidad, excepcionalidad, idoneidad, necesidad y proporcionalidad. El primer principio lo que proclama es que la medida tiene que estar dirigida a la investigación de un hecho delictivo en particular, ya que se prohíben las investigaciones prospectivas sobre una persona o varias personas. Por otro lado, el de idoneidad pretende fijar el ámbito objetivo y subjetivo de la medida, así como su duración; los de excepcionalidad y necesidad, por su parte, expresan la necesidad de que, por un lado, no existan otras medidas menos gravosas para los derechos fundamentales del que aparece como investigado y, por otro, que si no se autorizara la medida difícilmente se conocería al autor y las circunstancias que rodean al delito. El último principio al que legalmente se hace referencia es el de proporcionalidad, en cuanto a este la ley se refiere a que la privación del derecho al secreto de las comunicaciones no sea superior a la utilidad que se obtiene con la medida de investigación en favor del interés público.

Retomando el principio de proporcionalidad, legalmente reconocido, este se encuentra formulado en la jurisprudencia constitucional, véanse al respecto SSTC 62/1982, de 15 de octubre y 49/1999, de 5 de abril; igualmente en la STC 104/2006, de 3 de abril, el propio Tribunal se manifestó en los siguientes términos: "la proporcionalidad de la restricción de todo derecho fundamental (…) precisa que el beneficio obtenido mediante la medida sea mayor que el coste que el sacrificio del derecho comporta, lo que requiere realizar una ponderación global, a la luz de las circunstancias concurrentes en el momento de su adopción, que tome en consideración el fin perseguido, la idoneidad de la medida para alcanzarlo y que no exista otra medida menos gravosa que la adoptada, siendo de eficacia similar a la autorizada". Asimismo, en esta misma resolución el TC declaró lo siguiente: "en el juicio de proporcionalidad de la interceptación de las comunicaciones telefónicas, además de la gravedad de la pena, del bien jurídico protegido y de la

comisión del delito por organizaciones criminales, también puede ponderarse la incidencia del uso de las tecnologías de la información, pues su abuso facilita la perpetración del delito y dificulta su persecución".

Ciertamente al tratarse de una medida limitadora de un derecho fundamental la restricción del derecho al secreto de las comunicaciones le corresponde decretarla al órgano jurisdiccional, pudiéndose adoptar de oficio o a instancia del Ministerio Fiscal (en adelante, MF) o de la Policía Judicial (en adelante, PJ), la solicitud que se haga al Juez debe reunir una serie de requisitos que están orientados a justificar la petición y que posteriormente se verán reflejados en el auto judicial. Las exigencias determinadas legalmente en el auto judicial tienen su fundamento en la jurisprudencia constitucional, así este Tribunal en Sentencia 136/2006, de 8 de mayo, expuso que: "la resolución en la que se acuerda la medida de intervención telefónica o su prórroga debe expresar o exteriorizar las razones fácticas y jurídicas que apoyan la necesidad de intervención, esto es, cuáles son los indicios que existen acerca de la presunta comisión de un hecho delictivo grave por una determinada persona, así como determinar con precisión el número o números de teléfono y personas cuyas conversaciones han de ser intervenidas –que, en principio, deberán ser aquellas sobre las que recaigan los indicios referidos-, el tiempo de duración de la intervención, quienes han de llevarla a cabo y cómo, y los períodos en los que deba darse cuenta al juez para controlar su ejecución".

Considerando lo declarado por el TC esos indicios han de ser sospechas fundadas en alguna clase de dato objetivo. En otras palabras, lo que exige la ley es que el contenido de la resolución judicial se refiera al delito y a los indicios en los que se funda la medida; la persona investigada y otros afectados; el tipo de intervención; motivación; sujetos que ejecutarán la medida; duración, forma y cuándo se informará al Juez sobre los efectos de la intervención.

Por lo demás, son numerosas las disposiciones que regulan la medida de investigación objeto de estudio, realizándose en la ley citada una regulación detallada de la diligencia. Por lo que aquí respecta se quiere destacar, además de lo anteriormente mencionado, la delimitación de los delitos a los que es aplicable la medida de investigación tecnológica, esto es, delitos dolosos castigados con pena con límite máximo de, al menos tres años de prisión, crimen organizado y delitos de terrorismo, a estos habría que sumar los que se hayan cometido a través de los nuevos instrumentos informáticos de la información y de la comunicación. Asimismo, es relevante la duración de la diligencia que no puede superar los dieciocho meses. En atención a esto último, aunque nuestro texto constitucional no indica nada al respecto, es preciso que la ley establezca una limitación en la duración de la medida ya que es acorde con el principio de proporcionalidad (Gómez Colomer, 2025: 259-269).

De igual manera, desde el punto de vista legal, se ha querido dejar constancia del modo en el que se pretende el aseguramiento de las grabaciones intervenidas, de forma que los registros efectuados por la PJ se pondrán a disposición judicial en dos soportes digitales distintos: de una parte, se entregarán las transcripciones de los fragmentos que se consideren de interés para la investigación y, de otra, se entregarán las grabaciones completas, utilizándose los medios adecuados para asegurar su autenticidad. Además, se utilizan una serie de controles con la finalidad de que los registros originales se borren y se establecen unas condiciones concretas para las copias que se conserven.

IV. DATOS ELECTRÓNICOS DE TRÁFICO O ASOCIADOS INCORPORADOS AL PROCESO

En el ámbito de la interceptación de las comunicaciones telefónicas y telemáticas (Ley 13/2015, de 5 de octubre) se contempla una sección dedicada a la incorporación en el proceso de datos electrónicos. A este respecto, el art. 588 j LECRIM recoge la cesión de datos que se encuentren vinculados a un proceso de comunicación, estableciéndose que para que estos se incorporen se necesitará autorización judicial. En el contexto criminal hay que tener presente la importancia del análisis de datos de tráfico. Así, en la investigación, habrá un interés en conocer tanto el hecho delictivo como sus responsables; para cumplir con este objetivo las autoridades cuentan con una gran cantidad de información que es retenida por los operadores de telecomunicaciones (Freire Montero, 2024: 139-167).

En lo que respecta al tratamiento de los datos personales producidos por el uso de las comunicaciones, antes de la promulgación de la Ley 13/2015, de 5 de octubre, fueron diversas las normas aprobadas en el núcleo de la UE que regularon esta materia; la más relevante ha sido la Directiva 2006/24/CE. Dicha norma comunitaria, a modo de justificación, se refería a la existencia de distinta legislación en los Estados miembros sobre esta cuestión; además, la norma añadía otras causas para tener en cuenta, a saber: las conclusiones del Consejo de Justicia e Interior de 19 de diciembre de 2002, la Declaración sobre la lucha contra el terrorismo, adoptada por el Consejo Europeo de 25 de marzo de 2004 y la Declaración de 13 de julio de 2005 condenando los atentados terroristas de Londres. Estas circunstancias, en su conjunto, justificaban la adopción de medidas comunes sobre la conservación de datos de telecomunicaciones. Así pues, la lucha contra el terrorismo se ha situado como uno de los elementos esenciales a la hora de regular la conservación de datos en los países miembros de la UE.

La norma europea estableció que los datos únicamente podrían proporcionarse a las autoridades nacionales competentes en los casos y de acuerdo

con la legislación del Estado miembro. De este modo se estableció la facultad de cada Estado para definir el procedimiento y las condiciones a seguir para conocer los datos conservados, siempre teniendo presentes los principios de necesidad y proporcionalidad, así como las disposiciones del Convenio Europeo de Derechos Humanos y su interpretación por el TEDH. El tipo de injerencia que reguló la Directiva es la que se contempló su art. 5, es decir, conservación de aquellos datos necesarios para rastrear e identificar el origen de una comunicación, su destino, la fecha, la hora, su duración y el tipo de comunicación, al igual que los que se precisen para identificar el equipo de los usuarios, pero nunca se aplicaría para conocer el contenido de las comunicaciones.

La Directiva más arriba mencionada dio lugar a su transposición por medio 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. Esta ley, haciéndose eco de la norma comunitaria, determinó la obligación que tienen los operadores de telecomunicaciones de retener los datos que se producen por una comunicación, así como la de ponerlos a disposición de los agentes facultados, previa autorización judicial. También la Directiva aludía a la necesidad de que cada Estado miembro fuera quien determinara a qué delitos se aplicaría esta medida de investigación, sin embargo, la Ley 25/2007, de 18 de octubre, quebranta la Directiva debido a que no ha determinado cuáles son los hechos delictivos de gravedad a los que ha de aplicarse. No obstante, considerando los antecedentes legales, la medida se dirigirá a la investigación y enjuiciamiento de los delitos de terrorismo y de crimen organizado.

Ahora bien, hay que tener presente que la Directiva 2006/24/CE fue objeto de varias cuestiones prejudiciales ante el Tribunal de Justicia de la Unión Europea (en adelante, TJUE) en las que se solicitó el examen sobre la validez de la norma comunitaria, a la luz de dos derechos fundamentales de la Carta de los Derechos Fundamentales de la Unión Europea, es decir, el derecho al respeto de la vida privada y el derecho a la protección de datos de carácter personal. El TJUE, en Sentencia de 8 de abril de 2014 en los casos acumulados C-293/12 y C-594/12 Digital Rights Ireland y Seitlinger y otros, declaró que la conservación de datos se inmiscuye de forma especialmente grave en los dos derechos antes indicados, considerando que el legislador de la Unión había sobrepasado los límites exigidos por el principio de proporcionalidad.

Volviendo a la idea de la cesión de datos, concretamente lo que determina la Ley 25/2007, de 18 de octubre, es que la información referida con anterioridad se debe proporcionar a los agentes facultados, esto es, a las Fuerzas y Cuerpos de Seguridad del Estado cuando desempeñen funciones de PJ, de conformidad con el art. 547 de la Ley Orgánica 6/1985, de 1 de julio, del

Poder Judicial. Precisamente los agentes que dependan del Gobierno Central, Comunidades Autónomas y Corporaciones Locales son los que podrán ser requeridos judicialmente para que se les proporcionen los datos concretos de una comunicación con la finalidad de averiguar circunstancias relevantes de un hecho delictivo. A estos hay que sumar los funcionarios de la Dirección Adjunta de Vigilancia Aduanera cuando desarrollen funciones de PJ, así como el personal del Centro Nacional de Inteligencia en el ámbito de su competencia.

Es posible sostener que la Ley 13/2015, de 5 de octubre, recoge el testigo de la ley de transposición de la Directiva examinada y reconoce como novedad en la LECRIM la incorporación de datos electrónicos conservados por los prestadores de servicios, requiriéndose al efecto, para que puedan ser cedidos, autorización judicial (art. 588 ter j LECRIM). Además, en la ley procesal penal existe una sección dedicada singularmente al acceso de los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad.

De este modo, el art. 588 ter K LECRIM regula la identificación mediante número IP; así la PJ, en sus funciones de prevención y descubrimiento de los delitos cometidos a través de Internet, cuando conozca el Protocolo de Internet y desconozca la identificación del dispositivo y el usuario, solicitará autorización al Juez para que se cedan los datos relacionados con el dispositivo y con la identidad del sospechoso. Siguiendo con la sección citada, el art. 588 ter l LECRIM autoriza a la PJ, dentro de una investigación criminal, a utilizar los artificios técnicos que permitan acceder a los códigos IMEI e IMSI o a otros medios que sirvan para conocer el equipo que se utiliza. Una vez que conozcan estos números, la PJ podrá solicitar al Juez la intervención de las comunicaciones, teniendo que poner de manifiesto ante la autoridad judicial los instrumentos utilizados.

Para concluir añadir que el art. 588 ter m LECRIM pone fin a la sección mencionada. Este artículo permite al MF y a la PJ, en el ejercicio de sus funciones, dirigirse a los prestadores de servicios de comunicaciones cuando necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o en su caso, un número de teléfono o los datos identificativos de cualquier medio de comunicación (lo que puede incluir el IMEI debido a que es un código que identifica cualquier terminal de móvil) con la finalidad de que les proporcionen esa información. Es más, los operadores están legalmente obligados a facilitarla bajo apercibimiento de incurrir en un delito de desobediencia. Este precepto difiere de lo dispuesto en la Ley 25/2007, de 18 de octubre, ya que en esta se establece que únicamente podrán obtener este tipo de información los agentes facultados previa autorización judicial.

Considerando todo lo dicho con anterioridad y, en lo que concierne a la regularización que se da al acceso por la PJ de los códigos de identificación,

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 73/2, julio-diciembre 2025, págs. 327-358
https://doi.org/10.18543/ed.3451 • http://www.revista-estudios.deusto.es/

hay que advertir que la Exposición de Motivos de la Ley 13/2015, de 5 de octubre, declara que su tratamiento es acorde con la jurisprudencia del TS en esta materia. Al respecto habría que citar diversas sentencias anteriores a la ley examinada, específicamente, SSTS 130/2007, de 19 de febrero y 630/2008, de 8 de octubre, y que después se reiteran en la Sentencia 551/2016, de 22 de junio. Esta última resolución dice lo siguiente: "debe distinguirse entre la captura del IMSI asociado a un teléfono móvil, toda vez que dicho número ni siquiera contiene el número concreto del teléfono móvil, ni menos el del usuario y el sistema de *comptage* que se refiere al listado de llamadas entrantes y salientes efectuadas desde un teléfono móvil; es obvio que este listado puede incidir en la intimidad de las personas y así lo tiene declarado esta Sala, bien que el nivel de la injerencia sea superior que la interceptación de una comunicación, lo que puede ser relevante para efectuar el juicio de ponderación y de proporcionalidad". El TS en esta resolución alude a que en la Sentencia 130/2007, de 19 de febrero, hubo dos votos particulares, pero en otras sentencias de la Sala de lo Penal se hizo referencia directa a la obtención de los números IMSI, rechazando que estos estén bajo la cobertura del art. 18.3 CE, por lo que la captura de los números IMSI o IMEI no precisan de previa autorización judicial.

V. REGISTRO DE DISPOSITIVOS ELECTRÓNICOS

En lo concerniente al registro de dispositivos electrónicos son los artículos 588 sexies a LECRIM a 588 sexies c LECRIM los que regulan este medio de investigación. Nos hallamos ante una diligencia que al afectar a diversos derechos fundamentales relacionados con la privacidad de la persona (art. 18 CE) necesita de autorización judicial. Justamente es el juez quien debe fijar el alcance del registro, evitando la incautación de los equipos cuando se pueda producir un grave perjuicio a su titular o propietario y sea posible realizar una copia de la información. Es preciso señalar que la existencia del consentimiento del investigado es una excepción a la obligación de contar con la resolución judicial pertinente (Sánchez Medrano, 2022, p. 94).

Cuando se lleve a cabo la realización del acto de investigación habrá que aplicar los sistemas de garantías necesarios para lograr la autenticidad de los datos y preservarlos debidamente con el fin de que pueda practicarse un dictamen pericial. En esta diligencia de investigación (art. 588 sexies c LECRIM) se establecen una serie de actuaciones que han sido introducidas en cumplimiento del Convenio de Budapest y que tienen como objetivo lograr la efectividad de los registros efectuados. Asimismo, esta diligencia se puede realizar excepcionalmente sin previa autorización judicial.

Conectando con lo dicho, el acto de investigación podrá ser realizado por la PJ a pesar de no existir previa resolución judicial (art. 588 sexies c 4

LECRIM). En este contexto, y recogiendo la jurisprudencia constitucional, la PJ podrá efectuar el examen de un dispositivo electrónico con el objeto de conocer su contenido. Así, cuando vaya a realizar esta acción se habrán de cumplir los siguientes requisitos: por una parte, se ha de tratar de una situación urgente, esto es, inaplazable; de otra parte, se precisa la existencia de un interés constitucionalmente legítimo. Respecto a este último requisito, el TC, en la Sentencia 70/2002, 3 de abril, ha considerado como tal "el interés público propio de la investigación de un delito y, más en concreto, la determinación de hechos relevantes para el proceso penal". Además de las exigencias aludidas, se requiere que la intervención se comunique de manera inmediata a la autoridad judicial, existiendo un plazo de veinticuatro horas; se hará por escrito motivado y el Juez deberá pronunciarse sobre la adecuación de la medida en un plazo de setenta y dos horas.

Recientemente la Gran Sala del Tribunal de Justicia de la Unión Europea (en adelante, TJUE) ha conocido de una cuestión prejudicial planteada por un tribunal austríaco en Sentencia de 4 de octubre de 2024 (Tribunal de Justicia de la Unión Europea, curia.europa.eu). En esta resolución ha precisado cuáles son las condiciones en las que las autoridades nacionales competentes pueden acceder a los datos contenidos en un teléfono móvil para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales en general, de acuerdo con la Directiva 2016/680. Por otra parte, mediante el conocimiento de la mencionada cuestión prejudicial, el TJUE reconoce el derecho del interesado a ser informado de los motivos en los que se fundamenta la autorización de acceso a dichos datos a partir del momento en el que la comunicación no pone en riesgo la realización de las investigaciones.

Con el fin de conocer el pronunciamiento del TJUE es preciso examinar el supuesto de hecho en el que se fundamenta su resolución. De este modo, con ocasión de un control de estupefacientes (23 de febrero de 2021) agentes de aduanas austríacos interceptaron un paquete que iba dirigido a cierta persona (conteniendo 85 gramos de cannabis) este paquete fue trasladado a las autoridades policiales austriacas con el objeto de que fuera examinado. Con posterioridad (6 de marzo de 2021) en el marco de una investigación policial en materia de tráfico de estupefacientes, dos agentes registraron el domicilio de la persona a la que se había dirigido el paquete, interrogándole sobre el remitente del envío. Al negarse el interrogado a dar acceso a los agentes de policía a los datos de conexión de su teléfono móvil, estos procedieron a su incautación.

Subsiguientemente el teléfono móvil de la persona afectada por el registro domiciliario y cuyo dispositivo fue requisado por los agentes fue objeto de varios intentos de desbloqueo por la propia policía, teniendo en cuenta que "en el caso de autos, tanto la incautación del teléfono como los posteriores intentos de análisis y lectura de este fueron efectuados por los agentes de

policía sin autorización del Ministerio Fiscal o del Juez". Ulteriormente (31 de marzo de 2021) el afectado por la incautación del dispositivo interpuso recurso ante el órgano jurisdiccional competente, impugnando la legalidad de la confiscación de su teléfono móvil (dispositivo que le fue devuelto el 20 de abril de 2021). Además, el afectado no fue informado inmediatamente de los intentos de analizar y leer su dispositivo teniendo conocimiento de esta circunstancia en el procedimiento pendiente ante el órgano jurisdiccional.

En la apreciación que hace el TJUE este tribunal declara que el principio de proporcionalidad ha de estar presente en las limitaciones de los derechos fundamentales en materia de vida privada y familiar y de protección de los datos personales. Dichas restricciones únicamente podrán incorporarse cuando sean necesarias y obedezcan realmente a objetivos de interés general contemplados por la UE. En tal sentido, el Tribunal considera que el tratamiento de datos personales en el ámbito de una investigación policial que se dirige a la represión de una infracción penal, en el caso que se cuestiona los agentes de policía intentaron acceder a los datos contenidos en el dispositivo, tiene como fin un objetivo general reconocido por la Unión. Por otra parte, se requiere una ponderación de todos los elementos pertinentes en cada caso, teniendo presente el carácter proporcionado de las limitaciones en el ejercicio de los derechos fundamentales en materia relativa al respeto de la privacidad y de protección de los datos personales.

Asimismo, el Tribunal declara que el acceso al contenido de un teléfono móvil con restricción de los derechos fundamentales en virtud de una normativa que permite a la policía acceder sin autorización previa puede dar lugar a conocer datos muy precisos sobre la vida privada de la persona afectada. Por esta razón, esta injerencia en los derechos fundamentales "en materia de respeto de la privacidad y de protección de los datos personales debe considerarse grave, incluso especialmente grave". Igualmente, para dar cumplimiento a la exigencia de que cualquier limitación del ejercicio de un derecho fundamental esté establecida por la ley "corresponde al legislador nacional definir de manera suficientemente precisa los elementos que deben tenerse en cuenta, en particular la naturaleza o las categorías de las infracciones de que se trate".

Además, el TJUE determina que para garantizar el respeto del principio de proporcionalidad cuando el acceso a los datos personales por parte de las autoridades nacionales implique un riesgo de injerencia grave o muy grave en los derechos fundamentales de la persona afectada dicho acceso debe depender de un control previo de un órgano jurisdiccional o de una entidad administrativa independiente. Dicho control debe de realizarse con anterioridad al acceso de los datos salvo que se trate de un caso de urgencia debidamente justificada.

Teniendo en cuenta lo expuesto con anterioridad, el TJUE afirma que "el principio de minimización de datos" desde el punto de vista de los derechos

relativos a la protección de los datos personales y el respeto a la privacidad, no es contrario a la existencia de una regulación nacional que permita a las autoridades acceder al contenido de un teléfono móvil con la finalidad de prevenir, investigar, detectar o enjuiciar infracciones penales en general. No obstante, este tipo de actuaciones están subordinadas a un control previo por parte de un juez o una entidad administrativa independiente.

Finalmente, el TJUE en la cuestión prejudicial examinada se pronuncia sobre si la persona afectada por la medida de investigación debería haber sido informada de las actuaciones policiales realizadas, esto es, de las tentativas de acceso a los datos recogidos en su dispositivo. Ante esta tesitura el Tribunal declara que las autoridades nacionales que hayan sido autorizadas por un juez o por una entidad administrativa independiente para acceder a los datos conservados en un dispositivo deben informar de las razones en las que se funda dicha autorización, en cuanto la comunicación de esta información no ponga en peligro las investigaciones realizadas. La comunicación de esta información, de conformidad con la Directiva 2016/680 es necesaria para que el afectado por la medida pueda ejercer su derecho a la tutela judicial efectiva.

Por esta razón, en el caso de autos, el TJUE declara que la persona afectada debería haber sido informada previamente de las tentativas de acceso de datos contenidos en su dispositivo, ya que este ya había sido confiscado por la policía. Consecuentemente el Tribunal concluye que la Directiva 2016/680 desde el enfoque de la Carta de los Derechos Fundamentales de la Unión se opone al acceso de datos contenidos en un teléfono móvil sin informar al interesado de cuáles son los motivos en los que se fundamenta la autorización emitida por un órgano jurisdiccional o por una entidad administrativa independiente. Todo ello desde el momento en el que la comunicación de esta información no afecte a las investigaciones.

El TEDH también ha tenido ocasión de pronunciarse sobre el registro policial de material informático en el Asunto Trabajo Rueda c. España, Sentencia de 30 de mayo de 2017 (Ministerio de Justicia, repositorio.mpd.gov.ar). Se trata de un caso en el que, a través de la denuncia de un técnico informático, se pone en conocimiento de la policía la posesión de material pornográfico de menores por parte de un ciudadano español. La causa surge con la entrega voluntaria del poseedor del equipo informático al profesional para su reparación, manifestando el interesado la inexistencia de contraseña para acceder al equipo. Tras su reparación, el técnico procedió, con el fin de comprobar el arreglo del ordenador, a la apertura de varios ficheros ubicados en la carpeta "mis documentos" y descubrió que en la carpeta mencionada se encontraba material pornográfico de menores. Esta circunstancia dio lugar a que el técnico lo pusiera en conocimiento de la policía, entregando el ordenador a los agentes. La policía procedió directamente a examinar el contenido

de la computadora. Posteriormente se entregó el dispositivo a la PJ experta en informática y después se comunicó la investigación al órgano instructor.

Tras la sustanciación del juicio, el acusado fue condenado a una pena de cuatro años de prisión por posesión y difusión de imágenes de menores de carácter pornográfico. La Audiencia Provincial de Sevilla (en adelante, APS) para declarar su culpabilidad se fundamentó en el informe pericial de la policía y otros documentos, así como en el contenido de ciertos archivos del ordenador intervenido. La defensa manifestó la vulneración del derecho a la intimidad personal de su cliente porque la policía había accedido al contenido de su ordenador y además había procedido a la grabación de los archivos. En virtud de esta presunta vulneración se solicitaba la declaración de nulidad de estos elementos probatorios.

Se trataría, por lo tanto, de prueba ilícita o prueba prohibida que al contravenir lo dispuesto en el art. 11 de la Ley Orgánica del Poder Judicial no tendría ningún efecto en el proceso. Ante estas peticiones, la APS declaró la ausencia de violación del derecho a la vida privada del acusado por los siguientes motivos: el interesado había permitido el acceso a su ordenador por parte del técnico informático por lo que no pretendía reservar la información de sus ficheros y no había configurado el programa eMule de manera reservada frente a terceros. En este sentido la APS señaló que difícilmente se podría reconocer la vida privada del acusado cuando ni el mismo había establecido restricciones en sus ficheros respecto de otros usuarios.

Después de la sentencia condenatoria, el interesado interpuso recurso de casación argumentando la violación de sus derechos fundamentales. El recurso fue desestimado en base a que la intromisión en su intimidad había sido consentida por el recurrente al entregar el ordenador sin limitación alguna y al encontrarse los ficheros en una carpeta compartida con otros usuarios del programa eMule. Con posterioridad, el condenado formuló recurso de amparo ante el TC, alegando su derecho a la intimidad personal (art.18.1 CE) y el respeto del principio a la presunción de inocencia (art. 24.2 CE). El fiscal apoyó sus peticiones al entender que se habían vulnerado sus derechos fundamentales.

El TC, en su pronunciamiento, aludió a su jurisprudencia y, en particular, a la STC 70/2002, de 3 de abril, manifestando que el acceso al contenido de un ordenador personal necesitaba previamente del consentimiento de su propietario o de autorización judicial que respetara el principio de proporcionalidad. El TC afirmó que en el caso examinado la autorización dada por el interesado se limitaba a la manipulación del técnico sobre el equipo informático para su arreglo, lo que no legitimaba la intervención hecha posteriormente por otras personas.

Asimismo, el TC declaró que el hecho de compartir los archivos a través del programa eMule con otros usuarios no suponía una autorización

genérica frente a posteriores y diferentes injerencias en su intimidad, aunque esta hubiera sido la argumentación utilizada por los tribunales que con anterioridad le habían condenado. A juicio del TC, había existido una intromisión no consentida en el derecho a la vida privada del recurrente en amparo. Así, el Tribunal consideró que la intervención policial no contaba con autorización judicial, sin embargo, esta circunstancia se podía considerar como una excepción a la regla general que permite la jurisprudencia española.

El TC justificó la necesidad de la medida por las siguientes circunstancias: el poseedor del material pornográfico no se encontraba detenido, lo que eventualmente podría dar lugar al borrado de los datos desde otra ubicación o de los que se pudieran contener en otro lugar. Además de estas particularidades, también es relevante que la policía con rapidez comprobara si existían otros partícipes en el acto ilícito, incluso si se habían producido otros hechos como el abuso de menores. La sentencia presentó un voto particular que discrepaba del parecer del resto de los miembros del Tribunal, de acuerdo con esta decisión, el acceso al ordenador personal se había realizado sin autorización judicial previa y ante la inexistencia de una situación de urgencia que justificara la intervención judicial.

Ulteriormente, el TEDH al conocer el caso declaró la vulneración del art. 8 del Convenio Europeo de Derechos Humanos al considerar que es difícil valorar la urgencia que forzó a la policía a intervenir el ordenador personal del interesado sin autorización judicial. Entendiendo que no existía riesgo de desaparición de ficheros al ser un ordenador intervenido y retenido por la policía y sin conexión a la red. En esta línea, el TEDH dedujo que no había razones por las que no se podía haber esperado a obtener una autorización judicial que se podría haber conseguido con relativa rapidez.

VI. ENTREGAS VIGILADAS

En relación con las entregas vigiladas, esta técnica de investigación propia del crimen organizado, especialmente dirigida a luchar contra el narcotráfico, se introdujo en la LECRIM por medio de Ley Orgánica 5/1999, de 13 de enero. Dicha regulación es una manifestación de la Convención de Viena de 20 de diciembre de 1998 (Naciones Unidas) y el Convenio de Schengen de 14 de julio de 1985. Históricamente el Acuerdo de Schengen se suscribió por Países bajos, Francia y Alemania (14 de julio de 1985) su finalidad principal fue eliminar de forma gradual las fronteras entre los países mencionados. La declaración realizada resultó en la elaboración de un instrumento que se llamó Convenio de Aplicación del Acuerdo Schengen y que dio lugar a la creación de un espacio de libre circulación de personas, siendo una idea básica de la UE. El Convenio también recoge figuras de cooperación policial

de gran importancia como son las entregas vigiladas y los policías de enlace (Delgado Rodríguez, 2016: 249-257).

Este acto de investigación no solo tiene como finalidad combatir el tráfico de drogas, sino que también es utilizado en otros delitos como la fabricación, transporte y producción de materiales para la producción de sustancias alucinógenas; transmisión de bienes de origen delictivo; tráfico de especies amenazadas o protegidas de la flora o fauna (arts. 332 y 334 CP); falsificación de moneda, de tarjetas de crédito y tráfico de armas (art. 263 bis LECRIM, según Ley Orgánica 5/2010, de 22 de junio).

Con respecto a las autoridades adecuadas para su autorización, les corresponde a los Juzgados de Instrucción competentes, Ministerio Fiscal, Jefes de las Unidades Orgánicas de Policía Judicial (centrales o provinciales) y mandos superiores (Moreno Catena, 2023, pp. 291-292). Necesita de autorización motivada y la autoridad judicial que la dicte se lo comunicará al Juzgado Decano para su registro. La policía debe dar cuenta al fiscal sobre las autorizaciones que hubiera concedido y si existiera un proceso penal iniciado se comunicará al Juez de Instrucción competente. A través de esta técnica policial se pretende tener conocimiento, sin interferencia de la autoridad, de quiénes son las personas involucradas en la comisión de esta clase de crimen organizado.

Este tipo de diligencia investigadora está reconocida en la Circular 2/2022, de 20 de diciembre, de la Fiscalía General del Estado, sobre la Actividad Extraprocesal del Ministerio Fiscal en el Ámbito de la Investigación Penal. De conformidad con lo señalado en la Circular, nuestro ordenamiento jurídico contiene una escasa regulación de la actividad extraprocesal de la fiscalía en el ámbito de las investigaciones criminales. Estas actividades de investigación se han considerado como la antesala del modelo procesal que se trata de impulsar, es decir, tras la sustitución de la instrucción judicial se implantará la investigación dirigida por la fiscalía.

En otro orden de cosas, desde el punto de vista jurisdiccional, el TS ha tenido ocasión de examinar el art. 263 bis LECRIM a través del recurso de casación, concretamente tras su interposición contra sentencia condenatoria procedente de la Audiencia Provincial de Almería por un delito contra la salud pública. Mediante la Sentencia 723/2013, de 2 de octubre (vlex.es) el alto tribunal ha declarado que esta técnica de investigación puede adoptarse no solo por el Juez de Instrucción, sino también por el Ministerio Fiscal, por los Jefes de las Unidades Orgánicas de la Policía Judicial (centrales o provinciales) y por sus mandos superiores, conforme a lo señalado con anterioridad. Desde esta perspectiva el acto de investigación no trata de preservar el derecho a la intimidad del imputado ni el secreto de las comunicaciones (excepto casos del art. 263 bis 4 LECRIM) con la autorización. Precisamente lo que se persigue con la resolución habilitante es evitar espacios incontrolados en el marco de una investigación policial.

Se trata de un acto de investigación eficaz en la lucha contra el crimen organizado cuando actúan redes a nivel internacional. En este contexto es constatable que en el comercio de especies amenazadas o protegidas de la flora o fauna pueden intervenir personas de distintos ámbitos, de manera que el origen y los destinatarios pueden ser muy diversos. En diferentes actuaciones policiales se ha puesto de manifiesto esta situación, así, en la operación Namib se procedió a la desarticulación de una red delictiva dedicada al tráfico y tenencia ilegal de especies protegidas (www.interior.gob.es).

En lo concerniente a esta operación fueron detenidas numerosas personas pertenecientes a una organización criminal que actuaba a nivel nacional e internacional debido a que diversas especies provenían de Portugal. La red investigada realizaba operaciones de transporte, comercialización y tenencia ilegal de especies animales incluidas en la Convención sobre el Comercio Internacional de Especies Amenazadas de Fauna y Flora Silvestres (CITES) cuyo comercio está prohibido o rigurosamente regulado.

Asimismo, continuando con las redes que trafican con animales y plantas, a través de Interpol se ha tenido conocimiento de la operación Thunder, es decir, una operación realizada a nivel mundial y dirigida a la lucha contra las redes de tráfico de especies silvestres y de maderas. Esta investigación ha sido coordinada conjuntamente por Interpol y la Organización Mundial de Aduanas (OMA). Esta operación se saldó con la incautación de veinte mil animales vivos de especies protegidas o en peligro. En dicha investigción colaboraron agentes forestales, policía y otros organismos de ciento treinta y ocho países. Además de animales, se decomisó madera que era transportada en buques de carga, así como otras incautaciones que tuvieron lugar en aeropuertos y centros de correo (www.interpol.int).

VII. AGENTE ENCUBIERTO Y AGENTE ENCUBIERTO INFORMÁTICO

El agente de policía infiltrado también se sitúa como una técnica de investigación policial propia del crimen organizado (art. 282 bis LECRIM). Su objetivo es recabar y transmitir información sobre el hecho delictivo a través de la introducción de agentes policiales en las organizaciones criminales (Moreno Catena, 2023: 287-291). Se trata de una actividad investigadora, como antes se ha señalado, dirigida nuevamente a luchar contra la criminalidad organizada. En este sentido, desde la ley procesal penal se ha dado una definición del crimen organizado (art. 282 bis 4) con el fin de determinar esta conducta delictiva. La lucha contra esta modalidad criminal es tan relevante que se ha recogido en los Objetivos de Desarrollo Sostenible de la Agenda 2030, pretendiéndose una actividad en conjunto a nivel internacional (Anguita Osuna, 2023: 69-89).

Así, se considera delincuencia organizada la asociación de tres o más personas para realizar de forma permanente o reiterada, conductas que tengan como fin cometer alguno o algunos de los delitos siguientes: tráfico de órganos, secuestro de personas, trata de seres humanos, delitos relativos a la prostitución, delitos contra el patrimonio y el orden socioeconómico, delitos contra la propiedad intelectual e industrial, delitos contra los derechos de los trabajadores, contra los derechos de los ciudadanos extranjeros, delitos de tráfico de especies de flora o fauna amenazada (arts. 332 y 334 CP) tráfico de materia nuclear; delitos contra la salud pública; falsificación de moneda y de tarjetas bancarias; tráfico de armas; terrorismo y delitos contra el patrimonio.

Tratándose de este tipo de crimen organizado, el Juez o el Fiscal (comunicándoselo al Juez) podrán autorizar a la PJ mediante resolución motivada, teniendo en cuenta su necesidad para los fines de la investigación, a actuar con una identidad supuesta y también para adquirir y transportar los instrumentos del delito. Dichos agentes podrán mantener su falsa identidad cuando testifiquen en el proceso y se les aplicará la Ley de Testigos y Peritos de 1994. En este sentido, las declaraciones del agente encubierto son consideradas prueba testifical en el plenario, pudiéndose ser tenidas en cuenta como prueba de cargo (Sánchez González, 2024: 398-441). Por otro lado, cuando en sus actuaciones se vean afectados derechos fundamentales deberán solicitar al Juez las autorizaciones que determina la Constitución. Asimismo, el agente encubierto está exento de responsabilidad penal.

Igualmente, a través de las reformas operadas en el año 2015 se permite que el Juez pueda autorizar a funcionarios de la PJ (con identidad supuesta) en comunicaciones para la averiguación de los delitos en los que actúa el agente encubierto y también en aquellos en los que la ley procesal penal permite decretar la intervención de las comunicaciones. En relación con el agente encubierto informático, el policía infiltrado podrá intervenir en comunicaciones de carácter cerrado, con este fin se precisará autorización judicial, lo que no es necesario si se actúa en canales de comunicación abiertos. Al tratarse de canales de comunicación de carácter cerrado se puede excluir la intervención de terceras personas (León Camino, 2024: 28-48). De esta manera en actuaciones de vigilancia digital la policía puede llevar a cabo actividades de observación en canales de comunicación abiertos, pero si por sus investigaciones han de entrar en un chat o conversación que precise una contraseña, necesitarán la pertinente autorización judicial (León Camino, 2024: 28-48).

Recientemente el TC se ha pronunciado por primera vez sobre la legalidad de la actuación del agente infiltrado conforme a la CE. De conformidad con la nota informativa nº55/2024, el Pleno del TC procedió a respaldar las investigaciones realizadas mediante la utilización del agente encubierto. En la resolución, el Tribunal, siendo ponente el magistrado César Tolora

Tribiño, se manifiesta por vez inicial y avala la constitucionalidad de la actuación de los agentes encubiertos en operaciones de lucha contra el crimen organizado.

De acuerdo con los antecedentes de la Sentencia 87/2024, de 4 de junio, la Sección de estupefacientes de la Unidad Central de Droga y Crimen Organizado (UDYCO) perteneciente a la Brigada Provincial de Policía Judicial de Madrid (enero de 2019) pidió la apertura de diligencias de investigación y la habilitación de tres agentes encubiertos.

En el caso examinado se puso en conocimiento de la Fiscalía Especial Antidroga que se había recibido notificación por parte de la Sección de Agentes Encubiertos (UDYCO) de la presencia de una importante organización criminal (ciudadanos venezolanos) que estaría dedicándose a introducir en España grandes cantidades de droga por vía aérea. Dicha circunstancia estaría relacionada con otras líneas de investigación seguidas en esa Sección en el aeropuerto Adolfo Suárez Madrid-Barajas, por lo que se estaba utilizando dicha estructura como vía para introducir las sustancias estupefacientes.

En el oficio presentado a la Fiscalía se puso de manifiesto que uno de los principales dirigentes en España era un varón de origen venezolano llamado "Rafa", persona encargada de coordinar la entrada ilícita de mercancía en el aeropuerto por medio de "maleteros". Uno de los agentes encubiertos realizó un acercamiento a la persona antes mencionada comprobando que este individuo alardeaba de tener varias salidas de mercancía en Sudamérica, además de tener en España la infraestructura para rescatar el producto pudiéndolo hacer de manera periódica. El individuo en cuestión también se interesó por si el agente encubierto tenía algún medio de comunicación encriptado, aunque en un primer momento la comunicación fue por WhatsApp.

Del oficio se deducía "la existencia de una organización y agotadas las tradicionales vías de investigación, se estaba en disposición de introducir en dicha organización a tres funcionarios de la sección de agentes encubiertos". Por este motivo, se solicitó a la Fiscalía que se abrieran diligencias de investigación y también la autorización de tres funcionarios de la PJ para actuar como agentes encubiertos.

Ante estas circunstancias la Fiscalía Especial Antidroga abrió diligencias de investigación. En su decisión destacó que los hechos podían ser constitutivos de un delito de tráfico de drogas y/o blanqueo de capitales y refiriéndose al art. 282 bis LECRIM, donde se regula al agente encubierto, pudiéndose ser autorizado por el Fiscal comunicándoselo inmediatamente al Juez. El decreto de la Fiscalía disponía la autorización de tres agentes encubiertos y sus identidades verdaderas se consignaron en un sobre cerrado, firmado y sellado por la Fiscalía.

Los mencionados agentes fueron autorizados, si fuera necesario para la investigación "para adquirir y transportar los objetos, efectos e instrumentos

del delito". Uno de los agentes encubiertos mantuvo sendas sesiones con la persona antes indicada y de estas resultó la existencia de indicios delictivos. Asimismo, se produjo la prórroga para la actuación de los agentes encubiertos. Posteriormente hubo otra prórroga y después se remitieron las diligencias a la Fiscalía Provincial de Madrid al considerarse que los hechos no eran de competencia de la Audiencia Nacional.

Tras la llegada de las diligencias se acuerda la judicialización de la investigación, enviándola al Juzgado Decano de Madrid. Ulteriormente, el Juez de Instrucción competente dispuso una nueva habilitación de los agentes encubiertos y una vez efectuada la instrucción y el enjuiciamiento a través de los trámites propios del proceso abreviado, la Audiencia Provincial de Madrid dictó sentencia condenatoria por un delito de tráfico de drogas con penas de ocho años de prisión, inhabilitación especial y pena de multa.

Después de dictada la sentencia de primera instancia el condenado interpuso recurso de apelación ante el órgano jurisdiccional competente. En el escrito del recurso se expusieron los siguientes motivos: nulidad de la habilitación del agente encubierto por incumplir el art. 282.1 bis LECRIM; concurrencia de las figuras del agente provocador y del delito provocado; vulneración del derecho a la tutela judicial efectiva por motivación insuficiente en la individualización de las penas y, finalmente, improcedencia del decomiso del dinero y efectos intervenidos.

La Sala de lo Civil y Penal del Tribunal Superior de Justicia de Madrid desestimó el recurso y confirmó la sentencia dictada por la Audiencia Provincial de Madrid. Ulteriormente frente a la sentencia desestimatoria dictada por el órgano de segunda instancia se interpuso recurso de casación fundamentado en diversos motivos.

Las causas alegadas por el recurrente en el recurso extraordinario de casación abarcaban la infracción de ley y el quebrantamiento de forma. En relación con lo primero, esto es, la infracción de ley, el recurrente argumentó diferentes razones en su escrito. Entre estas, alegó la nulidad de actuación del agente encubierto por vulneración del derecho fundamental a la intimidad personal y familiar, así como de la prueba derivada de sus actuaciones. Asimismo, fundamentó su recurso en la falta de competencia de la fiscalía para autorizar la actuación del agente encubierto, también la falta de proporcionalidad y necesidad de la medida, seguido de la falta de motivación de la resolución habilitante del agente encubierto y, por último, el insuficiente control judicial de la medida de investigación del agente encubierto.

En relación con el quebrantamiento de forma, el recurrente argumentó varias razones en su recurso, a saber: falta de resolución en la sentencia de todos los puntos objeto de defensa tanto en primera como en segunda instancia; concurrencia del delito provocado y del agente provocador; falta de motivación en la pena impuesta e insuficiencia de motivación del decomiso.

Después de interpuesto el medio de impugnación extraordinario, la Sala Segunda del TS declaró mediante sentencia no haber lugar al recurso de casación.

Seguidamente se presentó recurso de amparo constitucional y en la demanda el recurrente interesó como único motivo la indebida actuación del agente encubierto respaldada por los órganos judiciales, así como la falta de observancia de los requisitos exigidos en el art. 282 bis LECRIM "para la habilitación y control de su actuación por los órganos judiciales". En particular, denunció la falta de competencia de la Fiscalía Especial Antidroga para autorizar al agente encubierto, también la falta de proporcionalidad y necesidad de la medida, así como su falta de motivación en el decreto habilitante y la falta de control judicial de la medida de investigación.

En cuanto a los preceptos constitucionales alegados por el demandante de amparo se consideraron vulnerados el art. 24.2 CE, concretamente el derecho a un proceso con todas las garantías, además del derecho a la tutela judicial efectiva sin indefensión (art. 24.1 CE) y el derecho a la intimidad (art. 18.1 CE) relacionados con el principio de legalidad (art. 9.3 CE).

En la sentencia que resuelve la demanda de amparo el Pleno se pronuncia sobre las diferentes modalidades de infiltración policial, afirmando que la actividad de infiltración tiene sustento en diversos preceptos del ordenamiento jurídico, y que la introducción del agente encubierto en el art. 282 bis LECRIM tiene como objetivo principal reforzar su actuación frente a los riesgos físicos y jurídicos que presenta esta figura. De esta forma para garantizar la seguridad del agente encubierto se le otorga una identidad supuesta y la capacidad de actuar frente a terceros. Asimismo, se le exime de responsabilidad penal por los hechos que pueda cometer atendiendo a ciertas condiciones.

Igualmente, la sentencia del Pleno recoge que la regulación de esta figura ha tenido como finalidad fortalecer los derechos de la persona investigada frente a la existencia del delito provocado. De esta manera ha previsto un procedimiento de habilitación por el fiscal que se fundamenta en la preexistencia de indicios delictivos.

Asimismo, cabe destacar que el Pleno considera que ha de efectuarse una interpretación sistemática de la "exigencia de comunicación inmediata al Juez" pues ha de ser acorde con las normas que regulan la investigación preprocesal del Fiscal como con la finalidad del art. 282 bis LECRIM que atribuye a este funcionario la realización de investigaciones utilizando esta figura.

De este modo el TC declara que el fiscal puede realizar sin la inspección del Juez las diligencias para las que esté legitimado, salvo las que limiten derechos fundamentales. Por lo tanto, la exigencia de dación de cuenta debe tenerse en cuenta al concluirse las diligencias preprocesales, pues no hay una

previsión normativa del procedimiento para fiscalizar judicialmente la habilitación del Fiscal; también ha de tenerse presente la finalidad del art. 282 bis LECRIM, incluso los derechos del investigado pues una vez que se judicializan las investigaciones podrá continuar ante el Juez la decisión del Fiscal. Por último, de acuerdo con el Pleno la habilitación del agente encubierto no afecta a ningún derecho fundamental y cuando estos derechos puedan verse menoscabados entonces sí intervendrá la autoridad judicial (art. 282 bis 3. LECRIM).

Por otra parte, el TC considera que la actuación del agente encubierto será la que pueda afectar al derecho a la intimidad o a otros derechos fundamentales, en cuyo caso y, de acuerdo con lo recogido en el texto constitucional, se requerirá autorización judicial.

Asimismo, el TC entiende que no se produjo la vulneración del derecho a un proceso con todas las garantías en relación con el delito provocado porque hay un procedimiento previsto legalmente para la habilitación del agente encubierto, también se requieren indicios delictivos previos, motivación del decreto del Fiscal; además el investigado puede proponer pruebas si considera que hay provocación del delito y las declaraciones de los agentes de policía se consideran prueba válida.

La resolución del TC insiste en que la habilitación del agente encubierto por sí misma no afecta al derecho a la intimidad y afirma que será la concreta actuación del agente la que pueda acceder al ámbito de la intimidad personal y familiar de la persona investigada. El TC al examinar los informes remitidos por el agente encubierto observa que su actuación no ha afectado la intimidad del investigado.

La sentencia contó con un voto particular (magistrado Ramón Sáez Valcárcel) quien discrepó de la decisión de la mayoría. De conformidad con la opinión de este magistrado el agente encubierto afecta "cuando menos, al derecho fundamental a la intimidad (art. 18 CE)". El magistrado aprecia que el policía tiene que ganarse la confianza de la persona investigada, así accede mediante el engaño a su privacidad y logra una complicidad que no conseguiría si conociera la identidad del agente. Al afectarse el derecho fundamental mencionado se necesita la autorización judicial de la medida, conforme al principio de proporcionalidad. Finalmente hay que señalar que se anunciaron los votos particulares concurrentes del Presidente de Tribunal, de la Vicepresidenta y de los magistrados Juan Carlos Campo y María Luisa Segoviano.

VIII. CONCLUSIONES

1. Hoy por hoy, la lucha contra el crimen organizado se ha internacionalizado debido a que la sociedad actual se ha conformado en diferentes estructuras internacionales. Dentro de este fenómeno destaca la UE

que sobresale por haberse constituido a través de un auténtico proceso de integración. Por medio del derecho derivado, principalmente a través de las directivas, la UE ha establecido una política común contra la criminalidad, y en particular, en la lucha contra los delitos medioambientales.

2. Mediante la Directiva (UE) 2024/1203 se pretende la mejora de la investigación, del enjuiciamiento penal y de las resoluciones judiciales, además ha recogido ciertos actos de investigación para la averiguación de los hechos delictivos relacionados con el medioambiente.
3. Entre las diligencias de investigación que podrán efectuarse se distingue la averiguación de información financiera. Para la realización de este medio de investigación, hay que partir de la Directiva 2019/1153 cuyo contenido alude a una serie de medidas para facilitar el acceso a la información financiera y de cuentas bancarias. El resultado de la transposición de la Directiva mencionada ha tenido lugar por medio de la Ley Orgánica 9/2022, de 28 de julio. Esta disposición legal posibilita el acceso a información financiera en delitos graves.
4. Asimismo, la intervención de las comunicaciones telefónicas y telemáticas se posiciona como otra diligencia a practicar en los delitos contra el medioambiente. A este respecto, la Ley 13/2015, de 5 de octubre, ha incluido importantes avances en dicho acto de investigación disponiendo una serie de requisitos comunes en todos los medios de investigación tecnológica.
5. Además, cabe destacar la incorporación de datos electrónicos en el proceso penal. Sobre esto hay que tener en consideración la gran cantidad de información que es retenida por los operadores de telecomunicaciones. Desde el punto de vista legal hay que partir, principalmente, de la regulación recogida en la Ley 13/2015, de 5 de octubre, así como de la Ley 25/2007, de 18 de octubre, que fue el instrumento legal por medio del cual se procedió a la transposición de la Directiva 2006/24/CE.
6. En cuanto al registro de dispositivos electrónicos nos hallamos ante una diligencia de investigación que afecta a diversos derechos fundamentales relacionados con la privacidad de la persona (art. 18 CE) por lo que la regla general para su práctica requiere la existencia de autorización judicial, salvo excepciones que se justifiquen en razones de urgencia. A este respecto se ha de tener presente la jurisprudencia del TC, TJUE y también del Tribunal de Estrasburgo.
7. Respecto a las entregas vigiladas, se trata de una técnica de investigación que es utilizada en el tráfico de especies amenazadas o protegidas de la flora o fauna (arts. 332 y 334 CP). En un primer momento, este tipo de actividad investigadora legalmente se refirió a la lucha contra el narcotráfico, pero posteriormente tras la reforma introducida por

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 73/2, julio-diciembre 2025, págs. 327-358
https://doi.org/10.18543/ed.3451 • http://www.revista-estudios.deusto.es/

Ley Orgánica 5/2010, de 22 de junio, se extendió a otros tipos delictivos. Por medio de esta técnica de investigación se pretende tener conocimiento de quiénes son las personas que participan en este tipo de criminalidad cuando actúan redes a nivel internacional.

8. En referencia al agente encubierto su objetivo es recabar y transmitir información sobre el delito por medio de la introducción de agentes policiales en las organizaciones criminales. Esta técnica de investigación también está dirigida a luchar contra la criminalidad organizada. Asimismo, expresamente se ha establecido en la ley procesal penal para combatir ciertos delitos contra el medioambiente. Además, tras la reforma operada en 2015 también se permite la actuación del agente encubierto informático. Recientemente la intervención efectuada por el agente encubierto en el crimen organizado ha sido avalada por el TC mediante Sentencia 87/2024, de 4 de junio.

IX. REFERENCIAS

Alfaro Romero, J. A. (2023). "Aproximación a las consecuencias de la priorización del delito medioambiental en la Unión Europea". *Cuadernos de la Guardia Civil. Revista de Seguridad Publica* (69), pp. 31-48.

Álvarez Sánchez de Movellán, P. (2019). "La motivación de la resolución que acuerda la investigación tecnológica". *El nuevo proceso penal sin código procesal penal* (obra colectiva), Barcelona: Atelier, pp. 297-308.

Anguita Osuna, J. E. (2023). "La lucha de la Unión Europea contra la delincuencia organizada: la nueva hoja de ruta de 2030*". Anuario de la Facultad de Derecho. Universidad de Extremadura*, (69), pp. 69-89.

Balas Dávila, A. (2023). "La financiación de la delincuencia organizada factor relevante en la lucha contra la criminalidad organizada en transformación constante". *Cuadernos de la Guardia civil. Revista de Seguridad Publica* (69), pp. 49-70.

Barbé, E. (2020). *Relaciones Internacionales.* Madrid: Tecnos.

Borja Jiménez, E. (2003). *Curso de Política Criminal.* Valencia: Tirant lo Blanch.

Casado Raigón, R. (2020). *Derecho Internacional.* Madrid: Tecnos.

Casado Raigón R. y Alcaide Fernández, J. (2019). *Curso de la Unión Europea.* Madrid: Tecnos.

Corral Maraver, N. (2020). *La política criminal de la Unión Europea. Especial referencia a su influencia en el Derecho Penal español*. Barcelona: Reus.

Delgado Rodríguez, J.M. (2016). *El blanqueo de capitales y el crimen organizado en España: regulación, tendencias de política criminal y alternativas*. Tesis doctoral.

Escudero García-Calderón, B. (2022). "La investigación penal ante las nuevas tecnologías: reflexiones acerca de la carga desproporcionada y la facilitación de información en el registro de datos". *Anuario de Derecho Penal y Ciencias Penales* (75).

Freire Montero, A.F. (2024). "La intervención de las comunicaciones telemáticas en el contexto digital". *Revista Española de Derecho Constitucional* (130), pp. 139-167.

Gómez Colomer, J.L. (2008). "Las diligencias de investigación". *Derecho Jurisdiccional III. Proceso Penal* (obra colectiva), Valencia, Tirant lo Blanch, pp. 162-182.

Gómez Colomer, J.L. (2025). "La intervención de las comunicaciones telefónicas y telemáticas". *Proceso Penal. Derecho Procesal III* (obra colectiva). Valencia: Tirant lo Blanch, pp. 259-269.

Hassemer, W. y Muñoz Conde, F. (2012). *Introducción a la Criminología y a la Política Criminal.* Valencia: Tirant lo Blanch.

León Camino, A. (2024). "Modo de actuación del agente encubierto virtual". *Revista Claves Jurídicas* (13), pp. 28-48.

Moreno Catena, V. (2023). "Actos de investigación reservados a la instrucción judicial". *Derecho Procesal Penal* (obra colectiva), Valencia: Tirant lo Blanch, pp. 287-291.

Rodríguez Lainz, J.L. (2025). "El artículo 588 sexies c. 4 de la Ley de Enjuiciamiento Criminal frente a la nueva jurisprudencia del TEDH y TJUE sobre el examen policial de dispositivos telefónicos móviles". *Diario La Ley, sección Doctrina*, (núm. 10644).

Sánchez González, S. (2024). "El agente encubierto en el ordenamiento jurídico italiano, un acercamiento desde el punto de vista procesal". *Rev. Boliv. de Derecho* (38), pp. 398-441.

Sánchez Medrano, F. de P. (2022). "El registro de dispositivos de almacenamiento masivo de información". *Revista Derecho y Proceso* (1).