ESTUDIO COMPARADO HISPANO-FRANCÉS:

LAS DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICAS FRENTE A LA JURISPRUDENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS

RESUMEN. Este estudio propone analizar de manera sistemática la regulación de las diligencias tecnológicas en España y Francia. Como países vecinos que cooperan regularmente a nivel policial y judicial, el derecho comparado permite fomentar una buena mutua comprensión entre ambos sistemas, además de poner de manifiesto similitudes, diferencia, buenas prácticas y desafíos de estos mismos. En materia de diligencias tecnológicas, las operaciones consideradas por ambas legislaciones son de suma equivalencia, ya que se acoplan en gran mayoría al estado actual de las técnicas. Los conceptos españoles se encuentran también en la legislación francesa, aunque pueden diferir en su alcance técnico o legislativos. Además, ambos países deben de conformarse con la protección supranacional de los derechos fundamentales, derivada del convenio europeo de derechos humanos. En base a la protección de la vida privada, el TEDH fue desarrollando una amplia jurisprudencia en cuanto a la regulación de las diligencias tecnológicas. Aunque los regímenes de ambos países se conforman en su globalidad a los criterios fijados por el TEDH, cabe mencionar que ninguna de las diligencias está exenta de críticas frente a este marco jurídico.

PALABRAS CLAVES. Diligencias tecnológicas. Derecho a la vida privada. Estudio comparado.

I. INTRODUCCIÓN

Mientras la sociedad evoluciona con los cambios tecnológicos, dicha evolución incluye nuevas formas de cometer delitos. Sin detenerse en las mutaciones del derecho penal sustantivo, cabe estudiar cómo el legislador adaptó el proceso penal para que se adecue a las nuevas oportunidades técnicas de investigación y persecución. Se considera en particular los regímenes de las diligencias tecnológicas. Dicho concepto no se define en España, pero es posible aproximarlo de su equivalente francés. Entonces, la doctrina las define como cualquier acto de investigación destinado a obtener datos[1]. Estos actos se pueden dividir entre diligencias invasivas y no invasivas. Estas últimas consisten, por ejemplo, en la consulta de una base de datos pública o gestionada por una administración[2]. Por el contrario, las diligencias invasivas se consideran como "*medidas coercitivas e intrusivas, dado que las autoridades judiciales llevan a cabo acciones fuertes y activas en la búsqueda de elementos*"[3]. Dentro de esta categoría, se puede distinguir entre las diligencias puramente tecnológicas y las diligencias mixtas. Algunas diligencias se llevarán enteramente a cabo a través de un dispositivo tecnológico (registro remoto de un dispositivo informático), mientras que otras supondrán una intervención física (registro de un dispositivo informático durante un registro domiciliario).

Este trabajo propone un análisis objetivo y sistemático[4] de las diligencias tecnológicas tal y como las recoge la Ley de Enjuiciamiento Criminal (LECrim), a la luz del Código de Enjuiciamiento Criminal (*Code de procédure pénale*) francés. Existen numerosos y detallados estudios de la LECrim en cuanto a las diligencias tecnológicas, pero raramente se propone

[1] B. Roussel, *Les investigations numériques en procédure pénale*, Tesis doctoral, Université de Bordeaux, el 7 de julio de 2020, ¶ 211. Se pueden definir los datos como la "*representación de la información para su tratamiento automático*", European Commission for the Efficiency of Justice, "European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment", Consejo de Europa, el 4 de diciembre de 2018, p. 70

[2] B. Roussel, *Les investigations numériques en procédure pénale*, *op. cit.* nota 1, ¶ 214

[3] *Ibid.* ¶ 215

[4] J.M. Pérez Zúñiga, "La importancia del método comparado en la investigación y la docencia", *en* N. Marchal Escalona, M.C. Muñoz González, S. Muñoz González (eds.), *El Derecho Comparado en la Docencia y la Investigación*, Dykinson, S.L., 2017, p. 57

comparar este tema con legislaciones extranjeras[5]. Este trabajo se apoya principalmente en una metodología comparada. Aunque España y Francia son dos ordenamientos jurídicos de sistema continental, pertenecientes a la Unión Europea, el tema de las diligencias tecnológicas no forma parte de las competencias de regulación de dicha organización supranacional. Sin embargo, como países vecinos, llegan que cooperar a menudo en casos de investigaciones sobre delitos transfronterizos. El correcto entendimiento de los procesos penales es entonces de suma importancia para facilitar la cooperación. En particular, la metodología comparada permite poner de manifiesto las semejanzas y diferencias entre ambos sistemas jurídicos[6]. Esta comparación es de especial interés a la hora de reformar la ley, dado que puede dar lugar al encuentro de buenas prácticas que se pueden transponer en el ordenamiento jurídico del Estado receptor. Cabe mencionar la aprobación de un anteproyecto de LECrim por el Consejo de Ministros en 2020, así como la creación de una mesa de trabajo sobre dicho tema en 2021. El anteproyecto pone de manifiesto la necesidad de modernizar la LECrim, en particular en materia de diligencias tecnológicas.

La ley está aletargada a la hora de regular la innovación y la tecnología, y de adaptarse a las realidades criminológicas cambiantes. Uno de los mayores desafíos a los que nos enfrentamos es, entonces, el de la actualización las leyes de enjuiciamiento criminal. Aquí se puede notar una primera diferencia mayor entre los dos sistemas jurídicos de este estudio. En España, el legislador prefiere adoptar leyes de reformas globales de la LECrim. La versión vigente de la ley fue modificada en profundidad por la 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. Por el contrario, el

[5] O estudiaban la regulación anterior a la reforma española de 2015, J.R. Agustina, "Sobre la utilización oculta de GPS en investigaciones criminales y detección de fraudes laborales: análisis jurisprudencial comparado en relación con el derecho a la intimidad", *La ley penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, 2013, núm. 102, p. 2 ; C. Cuadrado Salinas, "Registro informático y prueba digital: estudio y análisis comparado de la ciberinvestigación criminal en Europa (1)", *La ley penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, 2014, núm. 107, p. 3

[6] M. Durán Bernardino, "El método comparado en los trabajos de investigación", *en* N. Marchal Escalona, M.C. Muñoz González, S. Muñoz González (eds.), *El Derecho Comparado en la Docencia y la Investigación*, Dykinson, S.L., 2017, p. 49

código francés se modifica muy regularmente[7], a medida que se subrayan lagunas[8]. Sin embargo, resulta en la regulación de las diligencias tecnológicas en parte variadas del código, sin verdadera coherencia.

La estructura de la LECrim ofrece un régimen unitario para la gran parte de las diligencias tecnológicas, cuando autorización e implementación debe basarse en los principios "*de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida*"[9]. El principio de especialidad "*supone que la medida esté relacionada con la investigación de un delito concreto*"[10]. La idoneidad de la medida "*servirá para definir el ámbito objetivo y subjetivo[11] y la duración de la medida en virtud de su utilidad*". Los principios de excepcionalidad y necesidad limitan el uso de las diligencias tecnológicas cuando no quepan "*otras medidas menos graves para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento de los hechos*". Por fin, la proporcionalidad de la medida supone que "*el sacrificio de los derechos afectado no ha de ser superior al beneficio*

[7] En particular, véase: Loi n° 91-646 relative au secret des correspondances émises par la voie des télécommunications; Loi n° 2003-239 pour la sécurité intérieure; Loi n° 2004-204 portant adaptation de la justice aux évolutions de la criminalité; Loi n° 2007-297 relative à la prévention de la délinquance; Loi n° 2011-267 d'orientation et de programmation pour la performance de la sécurité intérieure; Loi n° 2014-372 relative à la géolocalisation; Loi n° 2014-1353 renforçant les dispositions relatives à la lutte contre le terrorisme; Loi n° 2016-731 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale; Loi n° 2019-222 de programmation 2018-2022 et de réforme pour la justice

[8] A través, por ejemplo, una condena del Tribunal Europeo de Derechos Humanos (TEDH). Francia, fue condenada muchas veces por el TEDH: TEDH, *Kruslin c. Francia*, el 24 de abril de 1990, núm. 11801/85 ; TEDH, *Huvig c. Francia*, el 24 de abril de 1990, núm. 11105/84 ; TEDH, *Lambert c. Francia*, el 24 de agosto de 1998, núm. 88/1997/872/1084 ; TEDH, *Matheron c. Francia*, el 29 de marzo de 2005, núm. 57752/00 ; TEDH, *Vetter c. Francia*, el 31 de mayo de 2005, núm. 59842/00 ; TEDH, *Wisse c. Francia*, el 20 de diciembre de 2005, núm. 71611/01 ; TEDH, *Ben Faiza c. Francia*, el 8 de febrero de 2018, núm. 31446/12. Véase, J.-P. Marguénaud, "La réécriture du droit criminel français sous la dictée de la cour européenne des droits de l'homme", *en* J. Alix et al. (eds.), *Humanisme et justice: mélanges en l'honneur de Geneviève Giudicelli-Delage*, Dalloz, 2016, p. 936

[9] Artículo 588 bis a de la LECrim, a los cuales ya que añadir el principio de legalidad

[10] M.C. Rayón Ballesteros, "Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015", *Anuario Jurídico y Económico Escurialense*, Real Colegio Universitario "Escorial-María Cristina", 2019, núm. 52, pp. 183–184. En consecuencia, se prohíbe "*las medidas de investigación tecnológica de naturaleza prospectiva que supondrían una autorización en blanco*", I. López-Barajas Perea, "Garantías constitucionales en la investigación tecnológica del delito: previsión legal y calidad de la ley", *Revista de Derecho Político*, Universidad Nacional de Educacion a Distancia (UNED), 2017, núm. 98, p. 106. Este principio era asentado en la jurisprudencia anteriormente a la reforma de 2015, J. Vegas Torres, "Las medidas de investigación tecnológica", *en* M. Cedeño Hernán (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1a ed., 2017

[11] En particular con la referencia a la posible afectación de terceros

que de su adopción resulte para el interés público o de terceros"[12]. En cuanto al principio de proporcionalidad, en sentido estricto[13], se considera en particular la gravedad de los hechos punibles, en función de la pena, de "*la naturaleza del delito, la relevancia social de los hechos y el ámbito tecnológico de producción*"[14]. La ley fija disposiciones generales[15] y enmarca así casi todas las diligencias tecnológicas dentro de una regulación coherente.

Por el contrario, en Francia, la regulación de las diligencias tecnológicas depende por un lado del tipo de procedimiento y de la calidad del delito investigado. El estudio comparado podrá subrayar las posibilidades de construir con más coherencia regímenes armonizados de diligencias tecnológicas. En cuanto al procedimiento, la amplitud de las diligencias disponibles y su regulación será diferente según la etapa en la que se encuentra el proceso penal. La investigación, en sentido amplio, se divide en tres partes. En primer lugar, la investigación de flagrancia[16] permite realizar las primeras observaciones por parte de los policías, bajo el control del fiscal[17], y por una duración de ocho días. En segundo lugar, fuera del marco de un delito flagrante, la investigación preliminar, que constituye el 80% de todos los casos llevados a juicio[18], está a cargo de la policía, bajo la supervisión del fiscal[19], y con autorización, para ciertas diligencias intrusivas, del juez de las libertades y de la custodia. Por último, la instrucción o información judicial es obligatoria para los delitos graves y opcional para los delitos menos graves[20], y está contralada por el juez de instrucción[21].

---

[12] R. Serra Cristóbal, "La vigilancia de datos y de comunicaciones digitales en la lucha por la seguridad nacional: especial referencia a las previsiones legislativa de España", *en* F. Flores Giménez, C. Ramón Chornet (eds.), *Análisis de los riesgos y amenazas para la seguridad*, Tirant lo Blanch, Derechos humanos, 1a ed., 2017, pp. 126–128

[13] M. Cedeño Hernán, "Las medidas de investigación tecnológica. Especial consideración de la captación y grabación de conversaciones orales mediante dispositivos electrónicos", *en* M. Cedeño Hernán (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1a ed., 2017

[14] I. López-Barajas Perea, "Garantías Constitucionales En La Investigación Tecnológica Del Delito", *op. cit.* nota 10, p. 105. Véase también J.J. López Ortega, "La utilización de medios técnicos de observación y vigilancia en el proceso penal", *en* J. Boix Reig, Á. Jareño Leal (eds.), *La protección jurídica de la intimidad*, Iustel, 2010, p. 318

[15] Artículos 588 bis a to 588 bis k de la LECrim

[16] "*Se define como delito flagrante un delito que se está cometiendo o que se acaba de cometer*", artículo 53 del Code de procédure pénale

[17] Artículo 12 del Code de procédure pénale

[18] B. Bouloc, G. Stefani, G. Levasseur, *Procédure pénale*, Dalloz, Précis, 27a ed., 2020, ¶ 532

[19] Artículo 75 del Code de procédure pénale

[20] Artículo 79 del Code de procédure pénale

[21] Artículo 49 del Code de procédure pénale

En cuanto a la calidad del delito investigado, se recogen diligencias tecnológicas dedicadas a la investigación de delitos relacionados con la delincuencia organizada. Constituyen las denominadas diligencias tecnológicas especiales. Además, estos delitos también pueden modificar los regímenes de las diligencias tecnológicas comunes. Estos delitos se listan de manera exhaustiva en el título dedicado del código a su enjuiciamiento[22], ya que la ley no defina el concepto de delincuencia organizada. Aunque se recogen en un título único, se recogen varios ámbitos mediante listas de delitos diferentes a las cualas se aplicarán regímenes distintos[23]. La primera[24] lista 18 categorías de delitos, por naturaleza cometido en general de manera organizada (tráfico de drogas), o limitados a sus formas agravadas (en particular cuando se cometen de manera organizada, como el robo), o por su particular gravedad (delitos graves perjudicando los intereses fundamentales de la nación). La segunda lista[25] enumera otras 11 categorías de delitos considerados de menos gravedad (tráfico de bienes culturales por ejemplo).

Sin embargo, la regulación y el desarrollo de las diligencias tecnológicas no puede únicamente considerar las necesidades de la investigación. En particular, se requiere un balance con la injerencia a los derechos fundamentales que resulta de la implementación de diligencias intrusivas. Dicho balance se pone de manifiesto en el Anteproyecto de LECrim. Antes de la reforma de 2015, el Tribunal Supremo[26] como el Tribunal Constitucional[27] habían criticado la ausencia de regulación adecuada de las nuevas diligencias tecnológicas utilizadas en la práctica por las autoridades policiales y judiciales. Estas críticas hacen eco al desarrollo

[22] Título XXV del Libro IV del Code de procédure pénale
[23] El tercer concepto, artículo 706-74 del Code de procédure pénale, menciona otros delitos graves y menos graves cometidos de manera organizada, pero este artículo no viene a aplicarse en materia de diligencias tecnológicas. Además, la aplicación de las diligencias tecnológicas especiales también se extiende por preceptos fuera del título, véase los artículos 706-2-2, 706-1, 706-1-1 y 706-1-2 del Code de procédure pénale
[24] Artículo 706-73 del Code de procédure pénale
[25] Artículo 706-73-1 del Code de procédure pénale
[26] Tribunal Supremo. Sala Segunda, de lo Penal, el 26 de noviembre de 2014, núm. 850/2014
[27] Tribunal Constitucional, el 22 de septiembre de 2014, núm. 145/2014 ; F. Otamendi Zozaya, *Las últimas reformas de la ley de enjuiciamento criminal una visión práctica tras un año de vigencia*, Dykinson, 2017, p. 23

de la jurisprudencia del Tribunal Supremo en cuanto al artículo 18 de la Constitución española, que llega hoy en día a incluir un derecho a la protección del propio entorno virtual[28]. Sin embargo, dicho marco constitucional no se acopla a este estudio comparado. Cabe recordar que España y Francia han ratificado el convenio europeo de derechos humanos de 1950, que cuenta con un amplio desarrollo por la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH). En particular, las diligencias tecnológicas se enfrentan al derecho a la vida privada, protegido por el artículo 8 del convenio.

Entonces, este estudio consiste, por un lado, en el análisis de las diligencias tecnológicas actualmente reguladas en las leyes de enjuiciamiento criminal en España y en Francia, con el fin de poner de relieve las posibilidades ofertas a las autoridades policiales y judiciales y sus buenas prácticas o los obstáculos a los que se enfrentan. Por otro lado, este trabajo estudia la conformidad de dichas diligencias tecnológicas con la jurisprudencia del TEDH en materia de protección de derechos fundamentales, para subrayar las lagunas o discordancias frente a criterios supranacionales.

[28] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática: tipos delictivos e investigación: con jurisprudencia tras la reforma procesal y penal de 2015*, Tirant lo Blanch, 2019, pp. 265–267 ; I. López-Barajas Perea, "El derecho a la protección del entorno virtual y sus límites. El registro de los sistemas informáticos", *en* F. Bueno de la Mata, M. Díaz Martínez, I. López-Barajas Perea (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, pp. 137–138

II. DILIGENCIAS TECNOLÓGICAS: SIMILITUDES Y DIFERENCIAS

Antes de profundizar el estudio detallado de cada diligencia tecnológica, cabe enumerarlas con el fin de explicar lo que permiten y cuáles son las diferencias o similitudes entre las reguladas en España y las consideradas por el código de enjuiciamiento criminal francés. Dentro de las diligencias tecnológicas, pueden dividirse las que se realizan con el conocimiento de la persona interesada, y las que se pueden realizar sin este.

1. Diligencia tecnológica con conocimiento de la persona interesada

La única diligencia tecnológica que se implementa con el conocimiento de la persona interesada es el registro de dispositivos de almacenamiento masivo de información. Supone registrar un conjunto de "*componentes que tienen la capacidad de escribir, conservar y posteriormente recuperar o leer datos en un soporte de almacenamiento*"[29]. Pueden dividirse en tres categorías, es decir: los dispositivos magnéticos (como un disco duro), ópticos (DVD) o de memoria sólida (memoria USB)[30]. En España, no se regula junto con los registros[31], en particular los registros domiciliarios, mientras que en Francia se asocia a dicha regulación[32], con un articulado específico[33]. La LECrim prevé unos artículos específicos para los registros informáticos junto con las demás diligencias tecnológicas[34].

Aunque la diligencia consiste en los mismos actos en los dos países, la regulación española supone dos autorizaciones distintas: una primera específica para autorizar el registro[35], y una segunda para autorizar el acceso a la información contenida en los

[29] Fiscalía General del Estado, Circular 5/2019 sobre sobre registro de dispositivos y equipos informáticos, el 6 de marzo de 2019, p. 30164
[30] *Ibid.*
[31] Artículos 545 a 588 de la LECrim
[32] Artículos 56 y siguientes, 76 y siguientes, 94 y siguientes del Code de procédure pénale
[33] Artículos 57-1, 76-3 y 97-1 del Code de procédure pénale
[34] Artículos 588 sexies a a 588 sexies c de la LECrim
[35] Artículo 588 sexies a de la LECrim

dispositivos[36]. Dicha doble autorización asienta la jurisprudencia anterior[37], que se había desarrollado después de un cambio jurisprudencial, dado que antes de 2010, se interpretaba la autorización de registro domiciliario de manera extensiva "*a la aprensión de todos los soportes informáticos que pudieran encontrarse en el interior del mismo*"[38]. En Francia, la ley prevé la posibilidad de registrar a los dispositivos y de acceder a la información sin necesidad de autorización específica[39]. Así, el código de enjuiciamiento criminal prevé el acceso "*a los datos pertinentes para la investigación en curso almacenados en un sistema informático situado en el lugar de la búsqueda, ya sea en ese sistema o en otro sistema informático, siempre que los datos sean accesibles desde el sistema original o estén disponibles para él*"[40]. Cuando el registro de dispositivos se realiza dentro de un registro domiciliario, obviamente, se extiende las condiciones de implementación y los regímenes protectores para determinados lugares registrados[41].

Esta diligencia tecnológica también se extiende fuera del contexto del registro domiciliario. La LECrim considera la obtención de dispositivos fuera del domicilio (por ejemplo, incautar el teléfono de un procesado) y "*el acceso a repositorios telemáticos de datos*" (por ejemplo, la obtención de códigos para acceder a una cuenta Facebook)[42]. Una autorización será necesaria para acceder a los datos. En Francia, la ley solamente considera la posibilidad de acceder a un sistema informático a partir de los dispositivos de las fuerzas de seguridad, cuando se haya obtenido durante la investigación, por ejemplo, los códigos de acceso[43]. Este tipo de registro remoto con el conocimiento de la persona interesada se conoce en Francia

[36] Artículo 588 sexies c de la LECrim
[37] J. Vegas Torres, "Las medidas de investigación tecnológica", *op. cit.* nota 10
[38] I. López-Barajas Perea, "Garantías Constitucionales En La Investigación Tecnológica Del Delito", *op. cit.* nota 10, p. 116
[39] Artículo 57-1 del Code de procédure pénale
[40] Artículo 57-1¶ 1 del Code de procédure pénale
[41] En particular, se prevén regímenes específicos para los registros en lugares ocupados por abogados, jueces, médicos, ... Ver los artículos 56-1 to 56-5 del Code de procédure pénale; o para los registros de los lugares donde se encuentran los cuerpos colegisladores, el monarca, los representates de naciones extranjeras, … Ver los artículos 548, 555, 559 de la LECrim. En Francia, las condiciones protectoras son más limitadas en caso de investigación sobre criminalidad organizada, artículos 706-89 a 706-94 del Code de procédure pénale
[42] Artículo 588 sexies b de la LECrim
[43] Artículo 57-1¶ 2 del Code de procédure pénale

como un registro con "*droit de suite*" (derecho de continuación), que consiste en que "*todas las ramificaciones de este sistema [informático], incluidas las situadas en el extranjero, estarían entonces sujetas a los mismos procedimientos de consulta que el situado en Francia*"[44]. En Francia, las medidas protectoras del registro domiciliario se aplican explícitamente a estos registros remotos[45], mientras que no se encuentra indicación similar en la LECrim[46].

En ambas situaciones, el dispositivo informático estará habitualmente protegido por una contraseña o por códigos de acceso. En este caso, la LECrim prevé la posibilidad de pedir a cualquiera persona que conozca el funcionamiento del sistema que facilite la información necesaria para acceder a los datos. Obviamente, esta obligación no se extiende "*al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco y a aquellas que […] no pueden declarar en virtud del secreto profesional*"[47]. En caso de incumplimiento de dichas obligaciones, la persona obligada podría incurrir en un delito de desobediencia[48]. Similarmente, la regulación francesa prevé que se puede "*requerir a cualquier persona susceptible de: 1° Tener conocimiento de las medidas aplicadas para proteger los datos*"[49], sin excluir ni siquiera al investigado. El no cumplimiento del requerimiento se castiga con una multa de 3 750 euros.

Finalmente, el último tema relativo a los registros de dispositivos informáticos reside en la preservación de los dispositivos o de los datos obtenidos. La regulación española considera subsidiaria la incautación de los soportes físicos[50], especialmente cuando se pueda obtener copia de los datos, previa autorización judicial[51] (y salvo que no sea el objeto o instrumento del delito). La regulación francesa prevé también las dos posibilidades pero sin fijar un orden

[44] R. Boos, *La lutte contre la cybercriminalité au regard de l'action des États*, Tesis doctoral, Université de Lorraine, 2016, pp. 308–309
[45] Artículo 57-1¶ 2 del Code de procédure pénale
[46] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, pp. 393–396
[47] Artículo 588 sexies c.5 de la LECrim
[48] Artículo 556 del Código penal, con "*pena de prisión de tres meses a un año o multa de seis a dieciocho meses*"
[49] Artículo 57-1¶ 5 del Code de procédure pénale
[50] Artículo 588 sexies c.2 de la LECrim
[51] Artículo 588 sexies c.1 de la LECrim

de prioridad[52]. El código francés añade la posibilidad de que el fiscal o juez de instrucción autorice "*la supresión definitiva, en el soporte físico que no ha sido puesto en manos de la justicia, de los datos informáticos cuya posesión o utilización es ilegal o peligrosa para la seguridad de las personas o de los bienes*"[53].

Indicamos también que la regulación francesa también autoriza otra diligencia tecnológica implementada con el conocimiento de una parte interesada: la víctima. Así, intercepciones de comunicaciones podrán llevarse a cabo en las líneas de comunicación de la víctima, si ella lo pide, para cualquier delito penado con una pena de prisión y cometido mediante estas líneas de comunicación[54]. Similarmente, la cesión de datos de tráfico o asociados puede solicitarse a la petición de la víctima, para datos asociados a sus dispositivos[55]. Sin embargo, la totalidad de las demás diligencias tecnológicas que se detallan en este estudio se llevan a cabo sin el conocimiento de la persona interesada.

2. Diligencias tecnológicas sin conocimiento de la persona interesada

Las leyes de enjuiciamiento criminal española y francesa regulan numerosas diligencias tecnológicas llevadas a cabo sin el conocimiento de la persona interesada: la intercepción de comunicación, que se regula en España junto con la incorporación al proceso de datos electrónicos de tráfico o asociados y el acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad; la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos; la utilización de

[52] Artículos 57-1¶ 4, 56¶ 5 y 97¶ 3 del Code de procédure pénale. El Conseil constitutionnel decidió que "*la copia de datos equivale a un registro*", J.-M. Brigant, "Mesures d'investigation face au défi numérique en droit français", *en* c. Franssen, D. Flore, F. Stasiak (eds.), ***Société numérique et droit pénal : Belgique, France, Europe***, Bruylant, 2019, p. 225, citando la sentencia del Conseil constitutionnel, *Ligue des droits de l'homme [Perquisitions et saisies administratives dans le cadre de l'état d'urgence]*, el 19 de febrero de 2016, 2016-536 QPC, ¶ 14

[53] Artículos 56¶ 6 y 97¶ 4 del Code de procédure pénale

[54] Artículo 100¶ 3 del Code de procédure pénale

[55] Artículo 60-1-2.3° del Code de procédure pénale

dispositivos técnicos de captación de la imagen, de seguimiento y de localización; y los registros remotos y la ciber infiltración.

A. Interceptación de comunicaciones

En España, como en Francia, la regulación de las interceptaciones de las comunicaciones fue aprobada después de condenas por el Tribunal Europeo de los derechos humanos[56]. En Francia, se esperó un año antes de aprobar la primera versión de regulación de las interceptaciones[57], mientras que se tuvo que esperar hasta el 2015[58] en España para obtener una suficiente regulación de estas[59]. En particular, el Tribunal Supremo criticó ampliamente dicha carencia, indicando que era "*preciso subsanar[la] con la máxima urgencia*"[60].

La intercepción de comunicaciones[61] es una de las medidas más utilizadas dentro de las investigaciones y como diligencia tecnológica. Sin embargo, su regulación supone garantías específicas, dado que supone una violación del secreto de las comunicaciones, protegido a nivel constitucional[62]. Para delimitar dicho derecho fundamental, se define una comunicación como "*el proceso de transmisión de expresiones de sentido a través de cualquier conjunto de sonidos, señales o signos*"[63]. Dicho concepto se extiende a los metadatos, o datos de tráfico,

---

[56] TEDH, *Kruslin c. Francia*, *op. cit.* nota 8 ; TEDH, *Prado Bugallo c. Spain*, el 18 de febrero de 2003, núm. 58496/00

[57] Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques. Durante este año, la Cour de cassation fue añadiendo condiciones para regular de manera jurisprudencial las interceptaciones de manera conforme con la jurisprudencia del TEDH, J. Dumont, J.-C. Fombonne, "Fascicule 20 : Interceptions des correspondances émises par la voie de communications électroniques - Articles 100 à 100-7", *JurisClasseur Procédure pénale*, LexisNexis, el 18 de mayo de 2020, ¶ 10–14

[58] 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

[59] I. López-Barajas Perea, "Garantías Constitucionales En La Investigación Tecnológica Del Delito", *op. cit.* nota 10, p. 97

[60] Tribunal Supremo. Sala Segunda, de lo Penal, el 26 de noviembre de 2014, *op. cit.* nota 26

[61] Artículos 588 ter a a 588 ter i de la LECrim

[62] Tribunal Constitucional, el 29 de noviembre de 1984, núm. 114/1984 ; E. Frígols i Brines, "La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías", *en* J. Boix Reig, Á. Jareño Leal (eds.), *La protección jurídica de la intimidad*, Iustel, 2010, p. 54

[63] Tribunal Constitucional, el 9 de octubre de 2006, núm. 281/2006 ; A.I. Vargas Gallego, "Algunos apuntes sobre la interceptación de las comunicaciones telefónicas", *Revista de Jurisprudencia El Derecho*, el 16 de diciembre de 2020, núm. 8

producidos por la comunicación[64], tal como su "*momento, duración y destino*"; a comunicaciones no leídas o "*en fase de transferencia*"[65]. Los artículos consideran las comunicaciones a las telefónicas y telemáticas, lo que fue criticado como una precisión innecesaria dado la evolución rápida de los medios de comunicación[66]. Sin embargo, las comunicaciones telemáticas aprovechan de una amplia interpretación, incluyendo "*comunicaciones en las que interviene un software informático*"[67]. Diferentemente, el código de enjuiciamiento criminal francés regula la "*interceptación de la correspondencia enviada por comunicaciones electrónicas*"[68]. Este último concepto se define como la "*emisión, transmisión o recepción de signos, señales, escritos, imágenes o sonidos por cable, inalámbricos, ópticos u otros medios electromagnéticos*"[69]. Entonces, en ambos países, las interceptaciones ya no se limitan a escuchas telefónicas, sino que se entienden a SMS, correos electrónicos, …[70]

En ambas regulaciones, esta diligencia se autoriza por un juez y se limita a determinados delitos. El umbral es el mismo: pena de la menos tres años de prisión[71]. La LECrim añade todos delitos "*cometidos en el seno de un grupo u organización criminal*", los de terrorismo[72], y los "*delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación*"[73]. En Francia, esta medida está limitada a la fase de instrucción de los delitos, controlada por el juez de instrucción, salvo

[64] Artículos 588 ter b.2 y 588 ter d.2. b a d de la LECrim. El primer artículo define los datos de tráfico o asociados como "*todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga*". Se recoge aquí la siguiente definición doctrinal que resume dicho concepto: "*datos que rodean el mensaje que se transmite, pero que no forman parte de dicho mensaje*", J.J. Fernández Rodríguez, "Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente", *Revista Española de Derecho Constitucional*, el 14 de diciembre de 2016, núm. 108, p. 96

[65] Fiscalía General del Estado, Circular 2/2019 sobre interceptación de comunicaciones telefónicas y telemáticas, el 6 de marzo de 2019, p. 30093

[66] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 292

[67] F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial: principios teóricos y problemas prácticos*, Thomson Reuters Aranzadi, Aranzadi derecho penal núm. 1151, Primera edición, 2019, 2019, p. 65

[68] Artículos 100 a 100-8 del Code de procédure pénale

[69] Artículo L32 del Code des postes et des communications électroniques

[70] En Francia, estos servicios anexos representan 99% de los datos pedidos durante interceptaciones, B. Roussel, *Les investigations numériques en procédure pénale*, *op. cit.* nota 1, p. 184

[71] Artículos 588 ter a y 579.1.1° de la LECrim; artículo 100¶ 1 del Code de procédure pénale

[72] Artículos 588 ter a y 579.1.2° y 3° de la LECrim

[73] Artículo 588 ter a de la LECrim

investigación flagrante o preliminar sobre delitos cometidos en o considerados como criminalidad organizada, durante la cual se puede autorizar la interceptación por el juez de las libertades y de la custodia[74]. Al investigar estos delitos, la duración máxima de la diligencia también se extiende[75].

En ambos países, las interceptaciones de comunicación se llevan a cabo de manera centralizada. En España, se requieren al Sistema de Interceptación Legal de las Telecomunicaciones (SITEL)[76]. En Francia, son centralizadas por la Plataforma nacional de interceptaciones judiciales (PNIJ)[77].

Junto con la regulación de la interceptación de comunicaciones, la LECrim también incluye dos diligencias tecnológicas complementarias: la incorporación al proceso de datos electrónicos de tráfico o asociados y el acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad.

a. Incorporación al proceso de datos electrónicos de tráfico o asociados

Dentro de la regulación de la interceptación de comunicaciones, la LECrim también considera la cesión de datos de tráfico o asociados "*vinculados a procesos de comunicación*" conservados por prestadores de servicios[78]. Dicha cesión solamente podrá ser legal bajo autorización judicial[79]. Siendo regulado junto con las interceptaciones, el ámbito de aplicación corresponde al mismo que para estas diligencias[80].

[74] Artículo 706-95 del Code de procédure pénale
[75] Artículo 100-2 del Code de procédure pénale
[76] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, pp. 324–325 ; F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, pp. 57–58
[77] Artículos 230-45 y R40-42 a R40-56 del Code de procédure pénale
[78] Artículo 588 ter j de la LECrim
[79] De conformidad con la sentencia del Tribunal Constitucional, el 20 de mayo de 2002, núm. 123/2002 ; E. Frígols i Brines, "La protección constitucional de los datos de las comunicaciones", *op. cit.* nota 62, pp. 70–77
[80] Tribunal Supremo. Sala Segunda, de lo Penal, el 1 de junio de 2017, núm. 400/2017

De manera muy diferente, la regulación francesa sobre interceptaciones no considera una similar diligencia tecnológica, sino que articula poderes generales de cesión de datos, para cualquier. Esta cesión, de manera general, no requiere autorización judicial, ya que puede ser pedida por cualquiera persona encargada de la investigación: el inspector de policía judicial[81], el fiscal[82], o el juez de instrucción[83]. Por un lado, pueden solicitar "*a cualquier persona, establecimiento u organismo privado o público o administración pública que pueda poseer información pertinente para la investigación, incluida […] la información procedente de un sistema informático o del tratamiento de datos personales, que entregue dicha información*"[84]. Por otro lado, pueden solicitar, "*por medios telemáticos o informáticos, [que] los organismos públicos o las personas jurídicas de derecho privado [… pongan] a su disposición toda la información útil para establecer la verdad […] contenida en el sistema o sistemas informáticos o de tratamiento de datos personales que administran*"[85]. De manera general, se puede requerir todo tipo de dato para investigaciones sobre todo tipo de delitos. Como excepción, que se añadió recientemente[86], y sin que media autorización judicial, la solicitud de datos de tráfico o asociados[87] suponen un ámbito similar al de las interceptaciones: investigaciones sobre delitos penados con un mínimo de tres años de prisión[88].

[81] Durante una investigación flagrante, artículos 60-1 y 60-2 del Code de procédure pénale
[82] Durante una investigación flagrante, artículos 60-1 y 60-2 del Code de procédure pénale; o una investigación preliminar, artículos 77-1-1 y 77-1-2 del Code de procédure pénale
[83] Durante una instrucción, artículos 99-3 y 99-4 del Code de procédure pénale
[84] Artículos 60-1, 77-1-1 y 99-3 del Code de procédure pénale
[85] Artículos 60-2, 77-1-2 y 99-4 del Code de procédure pénale
[86] Loi n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire, artículo 12. Este nuevo artículo resulta de críticas a los artículos generales sobre cesión de datos, por la amplitud de su ámbito y la ausencia de control de un juez, B. Roussel, *Les investigations numériques en procédure pénale*, *op. cit.* nota 1, pp. 131–132
[87] "*Los datos técnicos que permiten identificar el origen de la conexión o los datos relativos al equipo terminal utilizado […] o los datos de tráfico y localización*", artículo 60-1-2 del Code de procédure pénale
[88] O sobre un delito penado con al menos un año de prisión, cometido mediante el uso de una red de comunicaciones electrónicas y con el único propósito de identificar al infractor; o para encontrar a una persona desaparecida o para investigar sobre crímenes en serie o sin resolver, artículo 60-1-2 del Code de procédure pénale

En España, el incumplimiento al deber de colaboración se cualifica como delito de desobediencia[89]. En Francia, la regulación prevé explícitamente una multa (3 750 euros) en caso de no cumplimiento con estas solicitudes[90].

En ambos países, dichas cesiones dependerán de la disponibilidad de los datos en los archivos de los prestadores de servicios. Por tanto, hay que acudir a las legislaciones sobre conservación de datos. Estas legislaciones fueron adoptadas como transposición a la 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. Sin embargo, dicha directiva fue invalidada por el Tribunal de Justicia de la Unión Europea (TJUE), por interpretación y aplicación de la Carta de los Derechos Fundamentales de la Unión Europea[91]. Antes y desde entonces, varios países fueron invalidando sus leyes de transposición, y el TJUE fue desarrollando su jurisprudencia sobre conservación de datos al estudiar la validez de algunas transposiciones nacionales. En particular, en su estudio de la legislación francesa, llegó a las siguientes conclusiones. Se valida, con el fin de luchar contra la delincuencia grave: la "*conservación selectiva de los datos de tráfico y de localización que esté delimitada, sobre la base de elementos objetivos y no discriminatorios, en función de las categorías de personas afectadas o mediante un criterio geográfico, para un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse*"; la "*conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión, para un período temporalmente limitado a lo estrictamente necesario*"; y "*conservación generalizada e indiferenciada de los datos relativos a la identidad civil de los usuarios de medios de comunicaciones electrónicas*"[92]. Desencadenó en una decisión del

[89] Artículo 556 del Código penal, con "*pena de prisión de tres meses a un año o multa de seis a dieciocho meses*"

[90] Artículos 60-1¶ 2 y 60-2¶ 4 del Code de procédure pénale

[91] TJUE, *Digital Rights Ireland Ltd (C-293/12), Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl e.a. (C-594/12) c. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána y Irlanda*, el 8 de abril de 2014, C- 293/12 y C- 594/12

[92] TJUE, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs c. Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre*

Consejo de Estado, intentando interpretar la ley de manera conforme a las exigencias europeas[93], y a la modificación subsiguiente de los textos legales[94]. Hoy en día, se requiere la conservación, para las necesidades de procedimientos criminales, de la "*información sobre la identidad civil del usuario, hasta cinco años después del fin de la validez del contrato*", y de "*otros datos facilitados por el usuario al suscribir un contrato o crear una cuenta, así como la información relativa al pago, hasta la expiración de un período de un año desde el final de la validez del contrato o el cierre de la cuenta*"[95]. Para la lucha contra la criminalidad grave, se requiere la conservación de "*los datos técnicos que permitan identificar el origen de la conexión o los datos relativos al equipo terminal utilizado, hasta la expiración de un período de un año a partir de la conexión o de la utilización del equipo terminal*"[96].

Por el contrario, la legislación española sobre conservación de datos[97] nunca fue considerada a la luz de la invalidación de la directiva y de las nuevas exigencias del TJUE. De manera redundante con el artículo de la LECrim sobre cesión de datos, vuelve a recordar la necesidad de autorización judicial[98]. La ley obliga a la conservación por una duración general de doce meses[99] de todos los datos enumerados, sin distinción, necesarios para: "*rastrear e identificar el origen de una comunicación*", "*identificar el destino de una comunicación*", "*determinar la fecha, hora y duración de una comunicación*", "*identificar el tipo de comunicación*", "*el equipo de comunicación*" y "*la localización del equipo de comunicación*

des Armées ; y Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX c. Conseil des ministres, el 6 de octubre de 2020, C-511/18, C-512/18 y C-520/18, ¶ 168

[93] Conseil d'Etat, *French Data Network et autres*, el 21 de abril de 2021, núm. 397844, 397851, 393099, 394922, 424717, 424718

[94] Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement

[95] Artículo L34-1.II bis.1° y 2° del Code des postes et des communications électroniques

[96] Artículo L34-1.II bis.3° del Code des postes et des communications électroniques

[97] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

[98] Artículo 6.1 de la Ley 25/2007

[99] Artículo 5 de la Ley 25/2007 (salvo disposición reglamentaria diferente). Hay que indicar que en general "*los investigadores no suelen precisar de datos de gran antigüedad*" sino precisan de "*los inmediatamente anteriores al conocimiento policial de los hechos*", L. Vallés Causada, "Utilidad de los datos conservados de las comunicaciones electrónicas para la resolución de emergencias", *en* F. Bueno de la Mata, M. Díaz Martínez, I. López-Barajas Perea (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, p. 79

móvil"[100]. Sin embargo, el precepto de la LECrim no se limite a los datos conservados por obligación legal, sino a todo dato de tráfico o asociado conservado "*por propia iniciativa por motivos comerciales o de otra índole*"[101]. Estos dos regímenes de cesión de datos ya han sido criticados frente a las exigencias europeas[102], pero este estudio de conformidad no corresponde al ámbito de este estudio.

Junto con la cesión de datos de tráfico para tu incorporación al proceso, la LECrim también regula, dentro de la interceptación de comunicaciones, la obtención de ciertos datos de tráfico para la identificación de usuarios, terminales y dispositivos de conectividad. Aunque se agrupen dentro de una misma sección, la LECrim regula tres conceptos y regímenes diferentes[103].

b. Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad

Por un lado, la LECrim regula específicamente dos diligencias tecnológicas para la obtención de ciertos datos de tráfico con solicitud a los prestadores de servicios. Estos datos permiten la identificación de una persona o de un dispositivo. Entonces, cuando agentes de policía judicial constatan la comisión de un delito en Internet en una determinada IP, el juez de instrucción puede solicitar a prestadores "*los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso*"[104]. Este concepto se aproxima a la cesión de datos de archivos gestionados por operadores, dado que requiere autorización judicial, aunque la LECrim no es explícita[105].

[100] Artículo 3.1 de la Ley 25/2007
[101] Artículo 588 ter j.1 de la LECrim
[102] J.C. Ortiz Pradillo, "Europa: auge y caída de las investigaciones penales basadas en la conservación de datos de comunicaciones electrónicas", *Revista General de Derecho Procesal*, Iustel, 2020, núm. 52, p. 7
[103] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 305
[104] Artículo 588 ter k de la LECrim
[105] Fiscalía General del Estado, Circular 2/2019, *op. cit.* nota 65, p. 30116. Sin embargo, la mera obtención del número IP no requiere autorización judicial, F. Bueno de Mata, *Las Diligencias de*

De manera similar, el Ministerio Fiscal o la Policía Judicial podrá dirigirse a los prestadores para obtener la "*titularidad de un número de teléfono o de cualquier otro medio de comunicación*" o "*el número de teléfono o los datos identificativos de cualquier medio de comunicación*" de una persona determinada[106].

Estos dos conceptos no se regulan de manera específica en Francia, y se deberá acudir a los artículos generales sobre cesión de datos, en particular, el precepto sobre cesión de datos de tráfico[107]. El segundo concepto español se aproxima a la regulación de la cesión de datos de la legislación francesa, dado que no requiere autorización judicial, pero es limitado a datos muy específicos.

Por otro lado, la LECrim permite el uso de "*artificios técnicos*" para la captación de códigos de identificación de dispositivos, cuando no se haya podido "*obtener un determinado número de abonado y este resulte indispensable a los fines de la investigación*"[108]. La ley menciona explícitamente la obtención del número IMSI (*International Mobile Subscriber Identity* – Identidad Internacional del Abonado Móvil, por medio de un instrumento llamado un *IMSI cátcher*), situado en cada tarjeta SIM, o del número IMEI (*International Mobile Equipment Identity* – Identidad Internacional de Equipo Móvil), integrado a los teléfonos para conectarse a la red. La utilización de estos artificios no requiere autorización judicial[109]. Si se pide posteriormente una interceptación en dichos dispositivos, se tendrá que indicar este uso en la solicitud[110].

investigación penal en la cuarta revolución industrial, *op. cit.* nota 67, p. 89; lo que corrobora la jurisprudencia del Tribunal Supremo, Fiscalía General del Estado, Circular 2/2019, *op. cit.* nota 65, p. 30114

[106] Artículo 588 ter m de la LECrim

[107] Artículo 60-1-2 del Code de procédure pénale

[108] Artículo 588 ter l de la LECrim

[109] Lo que fue criticado, J. Vegas Torres, "Las medidas de investigación tecnológica", *op. cit.* nota 10. Sin embargo, es consistente con la jurisprudencia del Tribunal Supremo, que considera estos datos, así como el número IP, como "*información de conocimiento público para cualquier usuario de internet*" o porque dicha obtención solamente es "*una labor equivalente a una vigilancia convencional, aunque sea en un medio como es internet*", M. Cedeño Hernán, "Las medidas de investigación tecnológica", *op. cit.* nota 13

[110] Artículo 588 ter l.2 de la LECrim

De manera similar, el código de enjuiciamiento criminal francés prevé un artículo sobre la obtención de datos técnicos de conexión e interceptación de la correspondencia transmitida por las comunicaciones electrónicas[111]. Esta diligencia tecnológica solamente puede llevarse a cabo en la investigación de actos de criminalidad organizada[112]. Los artificios implementados permitirán obtener más datos que los previstos bajo el concepto español: el código permite la "*identificación de un equipo terminal o el número de abono de su usuario, así como los datos relativos a la ubicación de un equipo terminal utilizado*" pero también la directa interceptación de las comunicaciones entre los dispositivos identificados. Efectivamente, el *IMSI catcher* permite, en un área específica (unos pocos kilómetros), redirigir todas las correspondencias (tanto el contenido como los metadatos) de todos los teléfonos utilizados[113]. Dado la amplitud del concepto, siempre requiere autorización judicial[114].

En ambos casos, esta diligencia es especialmente útil para "*teléfonos no identificados, adquiridos bajo una identidad falsa o [investigados] que utilizan los teléfonos de su entorno*"[115]. También es de particular interés cuando el investigado utiliza tarjetas SIM de prepago, que no requieren proporcionar tantos datos como para un contrato permanente.

Además de regular la interceptación de comunicaciones, la LECrim también contempla otras diligencias tecnológicas para la obtención de comunicaciones.

[111] Artículo 706-95-20 del Code de procédure pénale
[112] Artículo 706-95-11 del Code de procédure pénale
[113] M. Quéméner, "Fascicule 20 : La preuve numérique dans un cadre pénal - Articles 427 à 457", *JurisClasseur Procédure pénale*, LexisNexis, el 18 de abril de 2019, ¶ 74 ; T. Meindl, "Fascicule 20 : Procédure applicable à la criminalité et la délinquance organisées – Poursuite. Instruction. Jugement. Assistants spécialisés – Dispositions dérogatoires de procédure – Articles 706-73 à 706-106", *JurisClasseur Procédure pénale*, LexisNexis, el 31 de enero de 2020, ¶ 63
[114] Artículo 706-95-12 del Code de procédure pénale
[115] J.-M. Brigant, "Mesures d'investigation face au défi numérique en droit français", *op. cit.* nota 52, p. 239

B. Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos

Otra manera de obtener comunicaciones y pruebas es la captación, por la policía judicial[116], de comunicaciones orales con dispositivos electrónicos (por ejemplo, sonorización con micrófonos)[117], "*una de las novedades más relevantes*"[118] de la reforma de 2015 de la LECrim. En efecto, dicha diligencia no era prevista por la ley, pero sí había sido admitida por el Tribunal Supremo[119], hasta la invalidación de dichas diligencias por el Tribunal Constitucional[120], por falta de habilitación legal. Desde 2015, dicha diligencia tecnológica se regula de manera expresa, incluyendo la captación y grabación de comunicaciones orales y la obtención de imágenes (uso de cámaras)[121]. En Francia, el concepto parece regularse de manera cuasi similar: incluye "*la captación, la fijación, la transmisión y la grabación de las*

[116] Por el contrario, "*La grabación clandestina por particulares de sus propias comunicaciones quedará fuera de esta regulación, no atentando nunca contra el derecho al secreto de las comunicaciones*", Fiscalía General del Estado, Circular 3/2019 sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, el 6 de marzo de 2019, p. 30123, véase también la sentencia del Tribunal Supremo. Sala Segunda, de lo Penal, el 15 de julio de 2016, núm. 652/2016; y solamente afectará al derecho a la intimidad cuando "*la conversación tuviera un contenido que afectará al núcleo esencial del derecho a la intimidad*", Tribunal Supremo. Sala Segunda, de lo Penal, el 16 de mayo de 2014, núm. 421/2014. Este precepto de la LECrim tampoco cubre "*las grabaciones subrepticias propiciadas por la policía*", es decir, llevadas a cabo por un particular, pero bajo incentivo de las fuerzas de seguridad, E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 440 ; Tribunal Supremo. Sala Segunda, de lo Penal, el 27 de junio de 2018, núm. 311/2018

[117] Lo que diferencia dicha diligencia de la interceptación de comunicaciones, en la que "*el sonido se capta a través del teléfono o medio de comunicación telemático intervenido*", Fiscalía General del Estado, Circular 3/2019, *op. cit.* nota 116, p. 30125. Sin embargo, las redacciones españolas y francesas aparentemente solamente prevén la colocación de dispositivos no incluye la referencia a "*dispositivos inteligentes que conforman el denominado internet de las cosas como son el uso de dispositivos como Alexa de Amazon*", F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, p. 100. En dicho caso, la comunicación no se transmite a través de un dispositivo, sino que se escucha a través de él, por lo cual no se podría aplicar la interceptación de comunicaciones. Sin embargo, dichos dispositivos son implementados por empresas privadas: la diligencia tecnológica más adecuada sería probablemente una solicitud de cesión de datos. Este tipo de colaboración ya se solicita en Estados Unidos, M. Burke, "Amazon's Alexa may have witnessed alleged Florida murder, authorities say", *NBC News*, el 2 de noviembre de 2019, en línea https://www.nbcnews.com/news/us-news/amazon-s-alexa-may-have-witnessed-alleged-florida-murder-authorities-n1075621 (recuperado el 12 de octubre de 2022)

[118] M.C. Rayón Ballesteros, "Medidas de investigación tecnológica en el proceso penal", *op. cit.* nota 10, p. 196

[119] El Tribunal Supremo fijó unas cuantas condiciones: autorización judicial mediante auto motivado, aplicación del principio de proporcionalidad, limitación de la diligencia a lo imprescindible y a hechos de suficiente gravedad, M. Cedeño Hernán, "Las medidas de investigación tecnológica", *op. cit.* nota 13

[120] Tribunal Constitucional, el 22 de septiembre de 2014, *op. cit.* nota 27

[121] Artículos 588 quater a a 588 quater c de la LECrim

palabras pronunciadas por una o varias personas […] o de la imagen de una o varias personas"[122].

El concepto español se extiende a "*medidas de muy distinta índole y alcance*"[123]: estas diligencias pueden llevarse a cabo "*en la vía pública*", en un domicilio o en cualquier lugar o espacio cerrado[124]. Similarmente, el código francés prevé su posible implementación en "*lugares o vehículos privados o públicos*"[125]. Sin embargo, el código precisa que las comunicaciones tienen que ser "*privadas o confidenciales*"[126]. En el caso contrario, no se considera la medida como una injerencia al secreto de las comunicaciones. Hay que precisar que la obtención de imágenes en Francia solamente se regula cuando se implementa en un lugar privado[127]. Cuando se requiere la entrada en lugares protegidos (tal como un domicilio), ambas legislaciones prevén autorizaciones específicas para la instalación de los dispositivos[128].

En ambas leyes, la captación de comunicaciones orales y de imágenes requiere autorización judicial[129] y se limita a la investigación de determinados delitos. En España, el ámbito material de aplicación se ajusta al de interceptaciones de comunicaciones[130], además de deber probarse que se puede prever que dicha diligencia "*aportará datos esenciales y de relevancia probatoria para el esclarecimiento de los hechos y la identificación de su autor*"[131]. Por el contrario, en Francia, la diligencia tiene un ámbito material mucho más restringido, es decir, una lista de delitos relacionados o cometidos en grupos organizados[132].

---

[122] Artículo 706-96 del Code de procédure pénale
[123] M. Díaz Martínez, "La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos", *en* F. Bueno de la Mata, M. Díaz Martínez, I. López-Barajas Perea (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, p. 94
[124] Artículo 588 quater a.1 de la LECrim
[125] Artículo 706-96 del Code de procédure pénale
[126] Artículo 706-96 del Code de procédure pénale
[127] Artículo 706-96 del Code de procédure pénale
[128] Artículo 588 quater a.2 de la LECrim y artículo 706-96-1 del Code de procédure pénale
[129] Artículo 588 quater a de la LECrim y artículo 706-95-12 del Code de procédure pénale
[130] Salvo que quedan excluidos los delitos cometidos a través de instrumentos informáticos, lo que ha sido criticado como una paradoja: "*la captación de imágenes como complemento a una comunicación en un lugar o espacio público, no podrá ser autorizada para esta clase de delitos*", E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 445
[131] Artículo 588 quater b.2 de la LECrim
[132] Artículo 706-95-11 refiriéndose a los artículos 706-73 y 706-73-1 del Code de procédure pénale

Sin embargo, la diferencia más relevante en cuanto a esta diligencia tecnológica es la delimitación temporal de la misma. En Francia, su duración se regula con un tiempo limitado fijado por ley (un mes o cuatro meses)[133], lo que es lo más común. Por el contrario, la regulación española no se basa en un límite temporal, sino en la autorización de "*uno o varios encuentros concretos del investigado con otras personas*"[134]. Eso se ha venido criticado ampliamente por la doctrina, dado el "*concepto indeterminado de encuentro*"[135], generando una diligencia "*potencialmente mucho más lesiva*" que, por ejemplo, una interceptación[136]. Una vez colocados los dispositivos, puede solicitarse una nueva autorización para cada nuevo encuentro previsto, en particular cuando los encuentros son periódicos[137]. Sin embargo, siempre se necesita indicios de dichos encuentros, lo que complica la solicitud de la diligencia[138]. Comparando con la legislación francesa, se replantea la necesidad de fijar un concepto tan poco operacional como límite temporal de dicha medida.

Además de regular diligencias tecnológicas para la obtención de comunicaciones, las leyes de enjuiciamiento criminal también ofrecen posibilidades para obtener otros tipos de datos.

---

[133] Artículo 706-95-16 del Code de procédure pénale

[134] Artículo 588 quater b.1 de la LECrim. Por lo cual "*no cabe autorizar la colocación de dispositivos para la grabación de todas las conversaciones que pudiera mantener durante un determinado periodo de tiempo*", M.C. Rayón Ballesteros, "Medidas de investigación tecnológica en el proceso penal", *op. cit.* nota 10, p. 197. Pero "*no impide que el Juez pueda establecer un límite máximo como garantía añadida*", I. López-Barajas Perea, "Garantías Constitucionales En La Investigación Tecnológica Del Delito", *op. cit.* nota 10, pp. 110–111

[135] F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, p. 103

[136] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 442

[137] M. Díaz Martínez, "La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos", *op. cit.* nota 123, p. 105. Ver el artículo 588 quater e de la LECrim

[138] Incluso puede llegar a ser inoperativa: "*1ª Se exige que sea para uno o varios encuentros concretos del investigado […], se hace porque se tiene constancia de que con carácter general los investigados se reúnen y hablan del delito en el mismo, en la confianza de que allí nunca podrán ser escuchados. Y esto, a veces durante meses, pero sin aviso de cuándo se van a producir. 2ª Por otro lado, en muchísimas ocasiones el "encuentro concreto" se conoce con poca antelación de tiempo, impidiendo a las unidades investigadoras colocar los dispositivos […] 3ª Por último, no sabemos cómo pretende el legislador grabar encuentros concretos en la vía pública por cuanto con antelación debe conocerse el momento, el punto concreto de desarrollo y sujetos afectados*", E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, pp. 443–444

C. Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización

Dentro de un capítulo único, la LECrim regula la obtención de imágenes en espacios públicos y la obtención de datos de localización.

a. Captación de imágenes en lugares o espacios públicos

Dentro de la protección de los derechos fundamentales a nivel constitucional en el ordenamiento español, el derecho a la imagen "*no es un objeto de protección penal específica y autónomo sino que se protege a través de los derechos al honor y a la intimidad*"[139]. No se protege de manera directa y restrictiva como las comunicaciones, dado que no afecta su secreto (artículo 18.3 de la Constitución española). Así, desde 1998, la jurisprudencia autoriza "*la filmación de escenas presuntamente delictivas que suceden en espacios o vías públicas*"[140]. Posición similar se desarrolla en Francia, con una gran diferencia: la diligencia tecnológica asociada se regula explícitamente en España, cuando en Francia no existe un precepto legal específico. La captación de imágenes en lugares públicos puede implementarse por material utilizado directamente por la policía judicial, o puede obtenerse a través del uso de los sistemas de videovigilancia. Dicho concepto se define ampliamente como "*toda actividad continuada de observación o control de un espacio a través de medios técnicos de la que resulte una grabación de imágenes susceptible de ser aportada a un proceso penal*"[141]. Este uso continuado se regula por una legislación específica[142], y se diferencia de

[139] C. Juanatey Dorado, A. Doval Pais, "Límites de la protección penal de la intimidad frente a la grabación de conversaciones o imágenes", *en* J. Boix Reig, Á. Jareño Leal (eds.), *La protección jurídica de la intimidad*, Iustel, 2010, p. 132

[140] Fiscalía General del Estado, Circular 4/2019 sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, el 6 de marzo de 2019, p. 30139

[141] A. Martínez Santos, "Las grabaciones obtenidas a través de sistemas de videovigilancia en el proceso penal: derechos fundamentales afectados y tipología de supuestos", *en* M. Cedeño Hernán (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1a ed., 2017

[142] Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos

la obtención puntual de imágenes captadas para las necesidades de una investigación[143] de un hecho delictivo ya cometido[144].

En España, la LECrim considera la captación de imágenes en lugares públicos enfocadas, por un lado, en la persona investigada para "*facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos*"[145]. Por otro lado, esta diligencia se puede extender a otras personas cuando sea necesario a la "*utilidad de la vigilancia*" (por ejemplo, cuando la persona investigada encuentre terceras personas) o cuando "*existan indicios fundados de la relación de dichas personas con el investigado y los hechos objeto de la investigación*"[146]. El concepto de "*utilidad de la vigilancia*" ha sido criticado por no concordar con el principio fundamental de necesidad que se aplica de manera transversal a todas las diligencias tecnológicas, lo que supone "*una rebaja sustancial del nivel de exigibilidad*"[147]. Esta captación se limita a los espacios públicos. Sin embargo, se ha venido cuestionado la delimitación con los espacios privados, en particular, el domicilio. El Tribunal Supremo fijó el criterio siguiente[148]: depende de si la injerencia es física o virtual. Cuando la injerencia es física, no incide en los derechos fundamentales dado que la persona no ha "*resguardado su intimidad*". Por el contrario, cuando la injerencia es virtual, se utilizan artilugios para mejorar la visión del agente, lo que desencadena en una vulneración del derecho a la intimidad (resultando en la necesidad de autorización judicial). En consecuencia, dicho concepto no se extiende a la captación de imágenes en espacios privados desde lugares públicos mediante artilugios (prismáticos, …)[149].

---

[143] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 464
[144] E. Gómez Soler, "La utilización de dispositivos técnicos de captación de la imagen de seguimiento y de localización. Cuando la práctica forense no puede esperar", *en* F. Bueno de la Mata, M. Díaz Martínez, I. López-Barajas Perea (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, p. 121
[145] Artículo 588 quinquies a.1 de la LECrim
[146] Artículo 588 quinquies a.2 de la LECrim
[147] E. Gómez Soler, "La utilización de dispositivos técnicos de captación de la imagen de seguimiento y de localización", *op. cit.* nota 144, p. 124
[148] Tribunal Supremo. Sala Segunda, de lo Penal, el 20 de abril de 2016, núm. 329/2016
[149] F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, p. 130

De manera similar, en Francia, la captación de imágenes en la vía pública no entra dentro del concepto restrictivo de sonorización con obtención de imágenes, dado que no se considera como una vulneración del derecho a la vida privada[150]. Como la delimitación del ámbito en España, la Corte de Casación indicó que el uso de artilugios para obtener imágenes dentro de un lugar privado vulnera dicho derecho fundamental[151].

El concepto de la LECrim, que se considera como ausente de vulneración a derechos fundamentales, no requiere autorización judicial y puede implementarse para cualquier delito[152]. Por el contrario, en Francia, la gran diferencia reside en la ausencia de concepto legal específico para la realización de dicha diligencia y la necesidad de una autorización. La Corte de Casación validó tal captación de imágenes en lugares públicos, con base en conceptos generales enumerando los poderes de los fiscales[153] y de los jueces de instrucción[154]. La captación de imágenes en lugares públicos requiere autorización: no puede implementarse de manera proactiva por la policía judicial, sino que requiere el control de un magistrado (no se requiere específicamente autorización de un juez), particularmente para definir su duración y ámbito[155].

Por fin, cabe mencionar que la doctrina ha venido extendiendo este concepto de la LECrim al uso de drones. Un dron se define como "*un conjunto de elementos configurables que constituyen una aeronave pilotada de forma remota, sus estaciones de pilotaje asociadas, los*

[150] Ver por ejemplo Cour de Cassation, Chambre criminelle, el 6 de abril de 2022, 21-84.092 ; Cour de Cassation, Chambre criminelle, el 7 de mayo de 2019, 18-85.596

[151] Cour de Cassation, Chambre criminelle, el 21 de marzo de 2007, 06-89.444 ; H. Vlamynck, "Le point sur la captation de l'image et des paroles dans l'enquête de police", *Actualité juridique Pénal*, Dalloz, 2011, p. 574

[152] Aunque ha sido criticado, J.C. Ortiz Pradillo, "Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos fundamentales en el proceso penal", *Diario La Ley*, Wolters Kluwer, 2021, núm. 9955, p. 9

[153] Artículo 41 del Code de procédure pénale y Cour de Cassation, Chambre criminelle, el 8 de diciembre de 2020, 20-83.885 ; S. Fucini, "Vidéosurveillance sur la voie publique durant l'enquête : conditions d'autorisation", *Dalloz Actualité*, Dalloz, el 6 de enero de 2021

[154] Artículo 81 del Code de procédure pénale y Cour de Cassation, Chambre criminelle, el 11 de diciembre de 2018, 18-82.365 ; S. Fucini, "Vidéosurveillance sur la voie publique durant l'enquête : conditions de réalisation", *Dalloz Actualité*, Dalloz, el 18 de enero de 2019

[155] Para un resumen de la jurisprudencia sobre este tema, véase J.-P. Valat, "Prise de photos ou enregistrement vidéo : que peut faire un enquêteur ?", *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2022, p. 399

enlaces de control y mando requeridos y cualquier otro elemento del sistema que pueda ser necesario, en cualquier momento durante la operación de vuelo"[156]. Son utilizados por las fuerzas de seguridad desde 2013, pero su regulación jurídica, en particular como medio de investigación[157], sigue siendo cuestionada[158]. Se podría considerar la captación de imágenes en lugares públicos como base legal para dicha diligencia[159]. Sin embargo, cuando el uso de dron desencadene a la obtención de sonidos e imágenes dentro de un ámbito privado o datos de localización, se tendría que acudir a otros conceptos[160].

Por el contrario, en Francia, el legislador modificó el código de enjuiciamiento criminal para incluir de manera explícita una nueva diligencia tecnológica dedicada al uso de drones en lugares públicos. Desde 2022[161], se regula el uso de "*cámaras aéreas […] para establecer un dispositivo técnico con el fin de captar, fijar, transmitir y grabar la imagen de una o varias personas en un lugar público sin su consentimiento*"[162]. Primeramente, hay que subrayar que dicho concepto es muy reducido a nivel tecnológico: hubiera sido más interesante aprobar un concepto tecnológicamente neutro, incluyendo la regulación de la captación de imágenes en lugares públicos de manera general. De manera similar, como en España, se tendrá que acudir a otras diligencias tecnológicas cuando el uso de drones resulta en la captación de sonidos e imágenes, en particular en lugares privados[163], o en datos de localización[164].

---

156 F. Bueno de Mata, "Peculiaridades probatorias del DRON como diligencia de investigación tecnológica", *en* F. Bueno de la Mata, M. Díaz Martínez, I. López-Barajas Perea (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, p. 170

157 L. Donoso Abarca, "Legitimidad de los sistemas de videovigilancia activa como medida de investigación tecnológica", *en* F. Bueno de Mata, I. González Pulido, L. Bujosa Vadell (eds.), *Fodertics 8.0: estudios sobre tecnologías disruptivas y justicia*, Comares, 2020, p. 251

158 M. Alejandra Suárez, "Diligencias de investigación tecnológicas. La licitud de la actividad probatoria de un dron", *en* F. Bueno de la Mata, I. González Pulido, L.M. Bujosa Vadell (eds.), *Fodertics 9.0: Estudios sobre tecnologías disruptivas y justicia*, Comares, 2021, pp. 393–403. En particular en cuanto a los principios de inmediación y de contracción, F. Bueno de Mata, "Peculiaridades probatorias del DRON como diligencia de investigación tecnológica", *op. cit.* nota 156, pp. 185–187

159 Artículo 588 quinquies a de la LECrim

160 Artículos 588 quater a y siguientes o 588 quinquies b de la LECrim, M.E. Laro-González, "El dron al servicio de las diligencias de investigación", *en* F. Bueno de Mata, I. González Pulido, L. Bujosa Vadell (eds.), *Fodertics 8.0: estudios sobre tecnologías disruptivas y justicia*, Comares, 2020, pp. 279–280

161 Loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure, artículo 16

162 Artículo 230-47 del Code de procédure pénale. Sobre este concepto, véase M. Bouchet, "Les drones face aux enjeux de droit pénal et de libertés fondamentales", *Dalloz IP/IT*, Dalloz, 2022, p. 299

163 Artículos 706-96 a 706-98 del Code de procédure pénale

164 Artículos 230-32 a 230-44 del Code de procédure pénale

El otro concepto dentro del mismo capítulo de la LECrim corresponde a la obtención de datos de localización y se regula de manera muy diferente.

b. Utilización de dispositivos o medios técnicos de seguimiento y localización

Se define la geolocalización como "*un protocolo automatizado que ubica cualquier objeto móvil tanto en un espacio físico concreto como en un tiempo y momento determinado*"[165]. Pueden dividirse en técnicas para obtener un movimiento grabado anteriormente ("*datos electrónicos asociados a sistemas de comunicación de telefonía*"[166])[167] u otras para obtener un movimiento en tiempo real (que también pueden derivar de datos asociados a sistemas de telefonía[168]). El concepto aquí estudiado solamente considera las últimas[169]. Estas pueden basar principalmente en tecnología *bluetooth* (radiofrecuencia de muy corto alcance); en radiofrecuencia; en sistemas de posicionamiento basados en satélites (GPS); o en sistema de posicionamiento global de la red de satélites (GNSS-GPS)[170].

La reforma de 2015 modificó en profundidad la jurisprudencia del Tribunal Supremo en materia de seguimiento y localización con dispositivos técnicos (geolocalización mediante

[165] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 471
[166] F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, pp. 142–143. Depende entonces de su conservación por los operadores involucrados, L. Vallés Causada, "Utilidad de los datos conservados de las comunicaciones electrónicas para la resolución de emergencias", *op. cit.* nota 99, pp. 60–61
[167] Desafortunadamente, la Circular 4/2019 sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización se olvida de esta posibilidad, F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, pp. 140–141
[168] En estos casos, su implementación se llevará a cabo a través del SITEL en España, L. Vallés Causada, "Utilidad de los datos conservados de las comunicaciones electrónicas para la resolución de emergencias", *op. cit.* nota 99, pp. 67–68, y a través de la PNIJ en Francia, artículos 230-44 y 230-45 del Code de procédure pénale
[169] Es explícito en el caso francés que solamente considera la geolocalización en "*tiempo real*", artículo 230-32 del Code de procédure pénale. Cuando la obtención de datos de localización sea posterior, la policía judicial deberá ampararse en el artículo 588 ter j de la LECrim cuando estén vinculados a datos telefónicos, o en el artículo 588 sexies a cuando estén vinculados a un dispositivo GPS. En Francia, se considerará como una cesión de datos, amparada por los artículos 60-1, 60-2, 77-1-1, 77-1-2, 99-3 o 99-4 del Code de procédure pénale
[170] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, pp. 472–473

balizas, GPS integrados a dispositivos como un teléfono, …)[171]. Antes del 2015, dicha diligencia no se consideraba como una vulneración al derecho a la intimidad, por lo cual no necesitaba autorización judicial[172]. Desde la creación del concepto legal en la LECrim[173], se requiere autorización judicial. Resultó en el reconocimiento por el Tribunal Supremo de un "*Derecho a no estar localizado*"[174]. Contrariamente, en Francia, aún antes de la creación del concepto específico, la Corte de Casación requería autorización judicial[175]. Hoy en día, el concepto legal requiere autorización previa, judicial de manera general. Sin embargo, la diligencia también puede estar autorizada por el Ministerio Público por una duración muy corta: de quince días en materia de investigación contra hechos de criminalidad organizada, sino ocho días como máximo[176]. La legislación prevé una autorización específica y adicional para la entrada en lugares privados para la colocación de los dispositivos[177] (lo que no considera la legislación española[178]). Sin embargo, ambas legislaciones prevén la posibilidad de implementar dicha diligencia sin autorización en caso de urgencia[179].

[171] Por el contrario, cuando el seguimiento se realiza personalmente, no se requiere autorización judicial, *Ibid.* pp. 469–470

[172] Tribunal Supremo. Sala Segunda, de lo Penal, el 22 de junio de 2007, núm. 562/2007 ; J.J. López Ortega, "La utilización de medios técnicos de observación y vigilancia en el proceso penal", *op. cit.* nota 14, p. 266 ; J. Vegas Torres, "Las medidas de investigación tecnológica", *op. cit.* nota 10. Sin embargo, el Tribunal Supremo hace depender esta ausencia de injerencia al "*grado de precisión con que se determine la localización geográfica de una persona a través de instrumentos electrónicos*", lo que depende mucho de la evolución de los medios técnicos utilizados, J.C. Ortiz Pradillo, "Big Data, vigilancias policiales y geolocalización", *op. cit.* nota 152, pp. 1–2.

[173] Artículos 588 quinquies b y 588 quinquies c de la LECrim

[174] J.C. Ortiz Pradillo, "Big Data, vigilancias policiales y geolocalización", *op. cit.* nota 152, pp. 1–2. Dicho derecho ya había sido reconocido por el alto Tribunal por la sala de lo social, J.R. Agustina, "Sobre la utilización oculta de GPS en investigaciones criminales y detección de fraudes laborales", *op. cit.* nota 5, p. 4

[175] Invalidación de autorización de la medida por un fiscal: Cour de Cassation, Chambre criminelle, el 22 de octubre de 2013, núm. 13-81949 ; Cour de Cassation, Chambre criminelle, el 22 de octubre de 2013, núm. 13-81945. Validación de la medida autorizada por un juez, aún en ausencia de base legal: Cour de Cassation, Chambre criminelle, el 14 de enero de 2014, núm. 13-84909

[176] Artículo 230-33 del Code de procédure pénale. El artículo también extiende la duración máxima de las renovaciones dentro de este tipo de investigaciones. La doctrina critica las diferencias de regulación de la diligencia según se autoriza dentro de una investigación o dentro de una instrucción, B. Roussel, *Les investigations numériques en procédure pénale*, *op. cit.* nota 1, p. 167

[177] Artículo 230-34 del Code de procédure pénale

[178] De manera general, la regulación de la geolocalización es mucha más desarrollada en Francia, dado que el Code de procédure pénale cuenta con trece artículos (230-32 a 230-44), cuando la LECrim solamente incluye dos artículos para regular dicha diligencia

[179] Artículo 588 quinquies b.4 de la LECrim y artículo 230-35 del Code de procédure pénale

En España, no todo tipo de geolocalización supone una necesaria autorización previa. En particular, "*la colocación y utilización de dispositivos o medios técnicos de seguimiento y localización en objetos, sin que con ello puedan conocerse datos de geolocalización de alguna persona concreta identificada, no afecta al derecho fundamental a la intimidad personal, por lo que cae fuera del ámbito que regulan los arts. 588 quinquies b y c LECrim y, en consecuencia, de la exigencia de previa habilitación judicial*"[180]. Por el contrario, en Francia la diligencia tecnológica de geolocalización se extiende al seguimiento de los movimientos "*de una persona […] de un vehículo o cualquier otro objeto*"[181].

La diferencia más importante radica en que la diligencia regulada por la legislación española puede autorizarse para toda clase de delitos, siempre que medie necesidad y proporcionalidad[182]. Por el contrario, en Francia, se puede llevar a cabo solamente dentro de investigación sobre delitos penados con un mínimo de tres años de prisión[183].

Por fin, las disposiciones comunes establecidas por la LECrim en el capítulo IV también se aplican al registro remoto sobre equipos informáticos, diligencia que se regula en pocos países de la Unión Europea[184]. Por aplicación del principio de necesidad, solamente tendría que autorizarse cuando "*la policía no logra determinar la localización física de esos datos*" con el fin de solicitar un registro físico de los dispositivos[185].

[180] Tribunal Supremo. Sala Segunda, de lo Penal, el 7 de julio de 2016, núm. 610/2016 ; Fiscalía General del Estado, Circular 4/2019, *op. cit.* nota 140, pp. 30156–30157
[181] Artículo 230-32 del Code de procédure pénale
[182] Artículo 588 quinquies b.1 de la LECrim
[183] Artículo 230-32 del Code de procédure pénale, o para investigar la causa de muerte o de desaparición, o la búsqueda de un fugitivo
[184] L. Bachmaier Winter, "Registro remoto de equipos informáticos en la Ley Orgánica 13/2015: algunas cuestiones sobre el principio de proporcionalidad", *en* M. Cedeño Hernán (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1a ed., 2017. Por el contrario, se fue desarrollando en los Estados Unidos desde finales del siglo XX, E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, pp. 492–493
[185] L. Bachmaier Winter, "Registro remoto de equipos informáticos en la Ley Orgánica 13/2015", *op. cit.* nota 184

D. Registros remotos sobre equipos informáticos

Dentro de los registros remotos sobre equipos informáticos, la LECrim considera dos diligencias diferentes[186]. Por un lado, se puede autorizar "*la utilización de datos de identificación y códigos*" para acceder, a distancia y sin conocimiento de la persona interesada[187], al contenido de un dispositivo o sistema informático[188]. Una diligencia similar se considera en Francia, aunque de forma más restringida. El código de enjuiciamiento criminal regula el "*acceso a distancia a la correspondencia almacenada mediante comunicaciones electrónicas accesibles por medio de un identificador informático*"[189]. Entonces, esta diligencia no permite acceder al contenido de un sistema de manera general, sino a comunicaciones, a través de los sistemas informáticos de la policía judicial[190]. Sin embargo, el concepto de comunicaciones, como mencionado, es muy amplio, lo que permite que dicha diligencia se extienda a cualquier tipo de comunicación: no solamente correos electrónicos, sino también comunicaciones en redes sociales o cualquier otro sitio, …

Por otro lado, la LECrim permite la autorización de "*la instalación de un software*" (los denominados "*troyanos*"[191] – a distancia o mediante instalación física en el dispositivo[192]) que permita obtener dichos contenidos de la misma manera[193]: permite acceder "*a la red del*

[186] Artículos 588 septies a a 588 septies c de la LECrim
[187] Lo que diferencia dicha diligencia con los otros registros. Los registros con conocimiento de la persona interesada se limitan a un período de tiempo muy limitado y corto, mientras que este tipo de acceso se limita a la duración establecida en la autorización. El acceso a los datos del sistema podría producirse todos los días durante este período, como una verdadera medida de vigilancia
[188] Artículo 588 septies a de la LECrim
[189] Artículos 706-95-1 a 706-95-3 del Code de procédure pénale
[190] T. Meindl, "Articles 706-73 à 706-106", *op. cit.* nota 113, ¶ 56
[191] M.C. Rayón Ballesteros, "Medidas de investigación tecnológica en el proceso penal", *op. cit.* nota 10, p. 201. La doctrina subraya la necesidad de crear una base de datos sobre la existencia de dichos programas, con el fin de poder "*diferenciar los archivos o programas que han sido enviados por la Policía, de los que han sido conseguidos por el propio sospechoso, de forma ilícita*", I. López-Barajas Perea, "El derecho a la protección del entorno virtual y sus límites", *op. cit.* nota 28, pp. 166–167
[192] La LECrim no considera una autorización adicional para la entrada en un lugar privado para la instalación de dicho programa, cuando lo considera el Code de procédure pénale, artículo 706-102-5. La doctrina explica dicha falta "*con el fin de no ofrecer pistas a los delincuentes para que puedan contra programar aplicaciones que detecten estos*", F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, p. 190
[193] Artículo 588 septies a de la LECrim

equipo "intervenido" o "hackeado""[194]. Similarmente, en Francia, se regula la captación de datos informáticos[195]. Consiste en la instalación de un "*dispositivo técnico que tiene por objeto, sin el consentimiento de los interesados, acceder, registrar, conservar y transmitir en cualquier lugar datos informáticos almacenados en un sistema informático, visualizados en una pantalla para el usuario de un sistema de tratamiento automatizado de datos, introducidos por el usuario tecleando caracteres o recibidos y transmitidos por dispositivos periféricos*"[196]. Entonces, el concepto francés es más amplio que el español. En Francia, se limita a la utilización de un *screenlogger* software, que permite a los agentes ver y recoger los datos tal y como se muestran en la pantalla del usuario; de un *keylogger* software, que permite ver y recoger los datos tal y como se escriben en el teclado por el usuario; de un software que permite acceder a los datos audiovisuales cuando se utilizaran periféricos audiovisuales (por ejemplo los datos de una webcam)[197]; o de un *backdoor server* que incluye el acceso a los datos almacenados[198]. Por el contrario, parece que el concepto español solamente considera la última posibilidad, dado que la LECrim solamente permite acceder al contenido de un sistema, y no incluye la posibilidad de ver el uso en tiempo real del sistema.

Ambas legislaciones requieren autorización judicial para la implementación de estas diligencias tecnológicas[199]. La legislación española prevé la necesidad de una autorización complementaria en caso de poder buscar datos en otros sistemas, con el fin de ampliar el

[194] L. Bachmaier Winter, "Registro remoto de equipos informáticos en la Ley Orgánica 13/2015", *op. cit.* nota 184
[195] Artículos 706-102-1 a 706-102-5 del Code de procédure pénale
[196] Artículo 706-102-1 del Code de procédure pénale
[197] La CNIL (Comisión Nacional de Informática y Libertades) subraya que los agentes no pueden activar y controlar esos periféricos, CNIL, *Délibération portant avis sur un projet de décret modifiant le décret n°2015-1700 du 18 décembre 2015 relatif à la mise en œuvre de traitements de données informatiques captées en application de l'article 706-102-1 du code de procédure pénale (demande d'avis n°18004354)*, el 26 de septiembre de 2019, núm. 2019-119
[198] M. Quéméner, "Les dispositions liées au numérique de la loi du 3 juin 2016 renforçant la lutte contre le crime organisé et le terrorisme", *Dalloz IP/IT*, 2016, p. 431 ; B. Roussel, *Les investigations numériques en procédure pénale*, *op. cit.* nota 1, pp. 199–200
[199] Artículo 588 septies a de la LECrim y artículos 706-95-1, 706-95-2 y 706-95-12 del Code de procédure pénale

registro[200]. Además, la autorización necesita la explícita mención, que no es automática, de la copia de los datos[201], mientras se autoriza por defecto en Francia[202].

En España, estas diligencias pueden autorizarse dentro de investigaciones sobre: "*a) Delitos cometidos en el seno de organizaciones criminales; b) Delitos de terrorismo; c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente; d) Delitos contra la Constitución, de traición y relativos a la defensa nacional; e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación*"[203]. En Francia, solamente pueden implementarse cuando se investiga un delito de las listas de delitos considerados como constitutivos de criminalidad organizada[204].

Finalmente, cabe mencionar una última diligencia tecnológica que no se enmarca dentro de las disposiciones comunes a las demás diligencias tecnológicas: la ciber infiltración.

E. Ciber infiltración

En primer lugar, cabe definir la ciber infiltración, es decir, el agente encubierto informático (o investigación con seudónimo en Francia)[205]. Dicha definición puede ser negativa, indicando lo que no es. Por un lado, se diferencia de la infiltración clásica[206], que se define como la diligencia en la cual el agente ingresa "*bajo identidad supuesta en el entramado organizativo para la investigación y represión de los delitos cometidos, la prevención de los que se van a*

[200] Artículo 588 septies a.3 de la LECrim
[201] Artículo 588 septies a.2.d de la LECrim
[202] Artículos 706-95-1, 706-95-2 y 706-95-11 del Code de procédure pénale
[203] Artículo 588 septies a de la LECrim
[204] Artículos 706-95-1, 706-95-2 y 706-102-1 del Code de procédure pénale
[205] Artículo 282 bis.6 y 7 de la LECrim, y artículo 230-46 del Code de procédure pénale. De manera general, las dos legislaciones son muy "*parca[s]*", M.L. Villamarín López, "La nueva figura del agente encubierto online en la lucha contra la pornografía infantil. Apuntes desde la experiencia en Derecho Comparado", *en* M. Cedeño Hernán (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1a ed., 2017. En el mismo sentido, véase F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, p. 115
[206] Aunque se regula en el mismo artículo en la LECrim: artículo 282 bis.1 a 5; en Francia, se regula separadamente en los artículos 706-81 a 706-87 del Code de procédure pénale

cometer, así como la averiguación de toda la información relevante sobre la organización criminal concreta en que se infiltra con el fin de llegar a su total desarticulación"[207]. Es un procedimiento más ampliamente desarrollado y limitado a las investigaciones contra delincuencia organizada[208]. Por el contrario, la ciber infiltración es más flexible[209], porque los poderes otorgados a los agentes son más restringidos por el contexto virtual[210]. Además, tiene ventajas en comparación con la infiltración clásica: "*es más fácil simular ser otra persona y mantener más tiempo la identidad falsa [por la ausencia de contactos físicos*[211]*;] el agente tiene margen para dilatar o posponer sus respuestas y así poder pensar cuál puede ser la contestación más adecuada en cada momento*[212]*[;] esta opción supone un menor sacrificio personal para el policía infiltrado, que puede seguir con su vida normal*[213]*[;] implica un riesgo casi nulo para su vida y su integridad física[;] su trabajo cuesta menos a las arcas del Estado y es más efectivo, ya que el mismo policía puede estar llevando a cabo a la vez varias operaciones de seguimiento, incluso comunicándose simultáneamente con delincuentes muy*

[207] R. Zafra Espinosa de los Monteros, *El policía infiltrado: los presupuestos jurídicos en el proceso penal español*, Tirant lo Blanch, 2010, p. 65

[208] Artículo 282 bis.4 de la LECrim y artículo 706-81 del Code de procédure pénale

[209] M. Quéméner, "Fascicule 1110 : Infiltrations numériques", *JurisClasseur Communication*, LexisNexis, el 3 de julio de 2019, ¶ 6. Dicha autora considera entonces que el nombre de ciber infiltracion es "*un término equivocado, jurídicamente erróneo*", *Ibid.* ¶ 17. Sin embargo, con el desarrollo de la técnica, y el aumento de los intercambios de imágenes y otros tipos de archivos, la distinción entre la ciber infiltración y la infiltración probablemente comenzará a difuminarse, para crear una gran escala de métodos de infiltración, más o menos virtuales

[210] Aunque en Francia se sigue requiriendo una habilitación especial, Arrêté du 21 octobre 2015 relatif à l'habilitation au sein de services spécialisés d'officiers ou agents de police judiciaire pouvant procéder aux enquêtes sous pseudonyme. Se critica la ausencia de regulación más detallada en España sobre los agentes que pueden implementar dicha diligencia, F. Bueno de Mata, "El agente encubierto en Internet como instrumento para la lucha contra el 'child grooming' y el 'sexting'", *en* F. Bueno de Mata et al. (eds.), *Cambio de paradigma en la prevención y erradicación de la violencia de género*, Editorial Comares, Estudios de Derecho constitucional, 2017, p. 14. Sin embargo, "*lo razonable es que el agente encubierto sea un miembro del Grupo de Delitos Telemáticos de la Guardia Civil o de la Brigada de Investigación Tecnológica de la Policía Nacional*", B. Rizo Gómez, "La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la 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", *en* J.M. Asencio Mellado, M. Fernández López (eds.), *Justicia penal y nuevas formas de delincuencia*, Tirant lo Blanch, Monografías, 1a ed., 2017, p. 108

[211] Aunque los delincuentes piden más y más pruebas de la identidad de su interlocutor (fotos, audios, …)

[212] Aunque se sigue requiriendo una cierta velocidad en los contactos para mantener el interés del delincuente

[213] Aunque los intercambios e interacciones pueden ocurrir en todo momento, incluso fuera de las horas de servicio, requiriendo entonces una alta disponibilidad del agente

variados[; y] existe menos peligro de que el agente se corrompa ya sea por el establecimiento de relaciones personales con el investigado más allá de lo permitido o porque termine implicándose como uno más en las actividades de los investigados"[214]. Hay que subrayar, en la regulación española, que el concepto de ciber infiltración no remite en todo al resto del artículo sobre la infiltración clásica. En particular, falta la mención a la "*protección del nombre real del agente*", la realización de otras diligencias que afecten a derechos fundamentales, y la exención de responsabilidad del agente por sus actuaciones, cuando califican como delitos[215]. Similares faltas pueden subrayarse en la regulación francesa.

Por el otro lado, es diferente del ciber patrullaje, que no se regula específicamente, dado que se considera como una mera inspección ocular de espacios públicos en línea[216]. Esta vigilancia es útil para las investigaciones proactivas, al comprobar la evolución de determinadas partes del ciberespacio[217]. Los datos dejados de manera abierta en Internet no son protegidos por el secreto de comunicaciones, por lo cual no se requiere autorización judicial[218]. Sin embargo, el límite puede ser sutil con la ciber infiltración: en ambas legislaciones, esta se regula para interactuar en línea. Pero para acceder a determinados espacios, se requiere una cuenta, y, por tanto, el uso de una identidad supuesta, aunque no se lleve a cabo ninguna interacción[219].

En definitiva, el agente encubierto informático se define como el agente que procura "*averiguar información sobre el sospechoso, sobre sus circunstancias, sobre sus intenciones*

---

[214] M.L. Villamarín López, "La nueva figura del agente encubierto online en la lucha contra la pornografía infantil", *op. cit.* nota 205

[215] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, pp. 525–526. Lleva a los autores a solicitar un articulado específico para el agente encubierto en Internet

[216] Cyberlex, Centre expert contre la cybercriminalité français, "Code de procédure pénale et lutte contre la cybercriminalité : propositions pour une efficacité juridique renforcée", el 24 de enero de 2018, p. 17. Ver también los artículos 326 a 333 de la LECrim

[217] M. Quéméner, "Infiltrations numériques", *op. cit.* nota 209, ¶ 19

[218] Tribunal Supremo. Sala Segunda, de lo Penal, el 9 de mayo de 2008, núm. 236/2008 ; Tribunal Supremo. Sala Segunda, de lo Penal, el 28 de mayo de 2008, núm. 292/2008 ; E. Velasco Nuñez, "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías", *Revista de Jurisprudencia*, el 1 de febrero de 2011, núm. 4, p. 6 ; E. Velasco Núñez, "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica", *Diario La Ley*, el 4 de noviembre de 2013, núm. 8183

[219] M. Quéméner, "Infiltrations numériques", *op. cit.* nota 209, ¶ 20. Además, la diferencia se reduce cuando la utilización de los dos tipos de diligencias son compatibles y pueden coexistir, E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 517

y propósitos, de modo análogo a como lo hace un agente que está patrullando en la calle, pero en este caso [interactuando] de forma virtual en [canales cerrados de] Internet"[220].

La ciber infiltración, como numerosas diligencias tecnológicas, ya estaba utilizada en España desde mucho tiempo: la reforma de 2015 le dio base legal[221]. Sin embargo, dicho uso ya venía validado por el Tribunal Supremo, con una interpretación extensa del concepto de organización, fijando el ámbito material de la diligencia de infiltración, para autorizar estas operaciones en "*la persecución de delitos de abusos sexuales a menores*"[222]. Por el contrario, en Francia, la técnica se reguló desde 2007[223], aunque su ámbito material se limitaba a delitos específicos (trata de seres humanos, aprovechamiento de la prostitución de otras personas, solicitud de servicios sexuales llevados a cabo por menores)[224]. Fue extendida en 2014: se aplicaba a una lista de delitos considerados como criminalidad organizada[225]. Finalmente, su versión actual resulta de una reforma de 2019[226].

Hoy en día, los dos ámbitos materiales de la ciber infiltración son muy amplios. En España, se puede implementar dentro de las investigaciones sobre: hechos de delincuencia organizada tal y como definida en el mismo artículo[227]; "*delitos cometidos a través de*

[220] M.L. Villamarín López, "La nueva figura del agente encubierto online en la lucha contra la pornografía infantil", *op. cit.* nota 205. Sin embargo, se critica tal expresión "*ya que la tarea de estos sujetos no es realizar operaciones de investigación sobre los equipos informáticos*". Ver también la definición de B. Rizo Gómez, "La infiltración policial en internet", *op. cit.* nota 210, p. 102. Harbottle Quirós considera tres características: "*1) la infiltración en una red de delincuentes; 2) la ocultación de la verdadera identidad; y 3) la condición de agente de la Policía Judicial*", F. Harbottle Quirós, "El agente encubierto informático: Reflexiones a partir de la experiencia española", *Revista Judicial, Poder Judicial de Costa Rica*, 2021, núm. 131, p. 125

[221] F. Bueno de Mata, "El agente encubierto en Internet como instrumento para la lucha contra el 'child grooming' y el 'sexting'", *op. cit.* nota 210, p. 10

[222] M.L. Villamarín López, "La nueva figura del agente encubierto online en la lucha contra la pornografía infantil", *op. cit.* nota 205

[223] Loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance, artículo 35

[224] Artículos 225-4-1,225-4-8,225-4-9,225-5,225-6 y 225-12-1 a 225-12-4 del Code pénal. Una técnica idéntica se introdujo en el artículo 706-47-3 del Code de procédure pénale, aplicable a la persecución de las infracciones vinculadas a la puesta en peligro de los menores (incitación al consumo de drogas, de alcohol, a la comisión de un delito, ...), artículos 227-18 a 227-24 del Code pénal

[225] Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, artículo 19

[226] Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, artículo 45

[227] Artículo 282 bis.4 de la LECrim: "*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*": secuestro, trata de seres humanos, falsificación de moneda, de tarjetas de crédito o débito

instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación"[228]; y todo delito doloso penado "*con límite máximo de, al menos, tres años de prisión*"[229]. En Francia, el agente encubierto en Internet puede implementarse "*con el único fin de comprobar los delitos sancionados con penas de prisión, cometidos a través de las comunicaciones electrónicas*"[230].

Por el contrario, los ámbitos de autorización son regulados de manera distinta en los dos países. En España, se requiere autorización judicial "*para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación*"[231]. Sin embargo, no se definen dichos canales cerrados[232], complicando la delimitación con el patrullaje en Internet como ya se ha mencionado. La legislación hubiera podido mencionar de manera explícita la posibilidad de actuar en canales abiertos con identidad supuesta, sin necesidad de autorización judicial, tal y como se ha validado por el Tribunal Supremo[233]. Por el contrario, en Francia, no se requiere ninguna autorización para, bajo identidad supuesta, "*1° Participar en*

---

o cheques de viaje, terrorismo; tráfico de órganos, de especies de flora o fauna amenazada, de material nuclear y radiactivo, de armas, municiones o explosivos; delitos relativos a la prostitución, a la propiedad intelectual e industrial; delitos contra el patrimonio y el orden socioeconómico, los derechos de los trabajadores, los derechos de los ciudadanos extranjeros, la salud pública y el patrimonio histórico. Se extiende este artículo con los siguientes mencionados por la imposibilidad de prever por legislación "*la realidad actual de la delincuencia por Internet*", E. Velasco Nuñez, "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías", *op. cit.* nota 218, p. 5. De la misma opinión, véase M.L. Villamarín López, "La nueva figura del agente encubierto online en la lucha contra la pornografía infantil", *op. cit.* nota 205 ; B. Rizo Gómez, "La infiltración policial en internet", *op. cit.* nota 210, pp. 97–123. Por el contrario, sobre la necesidad de extender el ámbito material, véase F. Bueno de Mata, "El agente encubierto en Internet como instrumento para la lucha contra el 'child grooming' y el 'sexting'", *op. cit.* nota 210, p. 12

[228] Artículos 282 bis.6 y 588 ter a de la LECrim

[229] Artículos 282 bis.6, 588 ter a y 579.1 de la LECrim. Este último artículo añade los delitos de terrorismo, sin mencionar artículos específicos del Código penal, al contrario del artículo 282 bis.4, lo que produce una inconsistencia. Similarmente, menciona a los delitos cometidos en grupo u organización criminal, sin que este concepto venga a ser armonizado con el concepto de delincuencia organizada del artículo 282 bis.4

[230] Artículo 230-46 del Code de procédure pénale

[231] Artículo 282 bis.6¶ 1 de la LECrim

[232] V. de Jorge Pérez, "El escondite virtual y el nuevo agente encubierto", *en* F. Bueno de Mata (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*, Comares, 2016, p. 249. La doctrina define las comunicaciones en canales cerrados como "*aquellas que se caracterizan por la expresa voluntad del comunicante de excluir a terceros del proceso de comunicación*", B. Rizo Gómez, "La infiltración policial en internet", *op. cit.* nota 210, p. 103

[233] Tribunal Supremo. Sala Segunda, de lo Penal, el 5 de julio de 2007, núm. 767/2007 ; Tribunal Supremo. Sala Segunda, de lo Penal, el 14 de julio de 2010, núm. 752/2010 ; F. Alba Cladera, G. García Martínez, "Blanqueo de capitales y agente encubierto en internet", *en* F. Bueno de Mata (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*, Comares, 2016, p. 192

intercambios electrónicos, incluso con personas susceptibles de ser autores de estos delitos; [y] 2° Extraer o conservar por este medio los datos de las personas susceptibles de ser autoras de estos delitos y cualquier prueba"[234].

Sin embargo, en los dos países, se requiere autorización para el intercambio de contenidos o datos. Pero la delimitación de dichas acciones se regula de manera diferente. En España, se necesita autorización judicial específica[235] para "*intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos*"[236]. Este último apartado permite en particular el uso de los algoritmos y bases de datos existentes en materia de pornografía infantil, que permiten identificar las imágenes para poner de manifiesto las similares[237]. Dicha diligencia no está prevista en Francia, aunque se esté utilizando[238]. Sin embargo, la primera diligencia sobre el intercambio de contenidos es más desarrollada en el código francés. Prevé que el fiscal o el juez de instrucción podrá autorizar la adquisición de "*cualquier contenido, producto, sustancia, muestra o servicio, incluido ilegal*", o la transmisión de contenido ilegal "*en respuesta a una solicitud expresa*"[239]. Aunque, como en España, no se define el concepto de archivo o contenido ilegal[240]. En materia de investigaciones sobre trata de seres humanos, de proxenetismo o de solicitud de servicios sexuales llevados a cabo por menores, solamente

[234] Artículo 230-46 del Code de procédure pénale
[235] "*Se trata de un plus, algo que debe ser adicional a la actuación del agente encubierto en Internet, a pesar de que en ocasiones la propia circulación se vuelva imprescindible al objeto de asegurar el éxito de la investigación penal*", B. Rizo Gómez, "La infiltración policial en internet", *op. cit.* nota 210, p. 118
[236] Artículo 282 bis.6¶ 2 de la LECrim. La doctrina considera que se debería ampliar las acciones previstas, en particular para incluir la posibilidad de abrir cuentas bancarias y disponer de dinero, F. Alba Cladera, G. García Martínez, "Blanqueo de capitales y agente encubierto en internet", *op. cit.* nota 233, p. 197
[237] Comisión Europea, "Commission Staff working document - Impact assessment report accompanying the document Proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse", UE, el 11 de mayo de 2022, pp. 71–72, SWD(2022) 209 final. "*Esta herramienta de investigación resulta absolutamente relevante en materia de delitos de pornografía infantil donde las fotografías pornográficas son digitalizadas a su huella numérica hash y por medio de un programa informático se puede determinar donde se encuentran almacenadas dichas fotografías en cualquier parte del mundo*", B. Rizo Gómez, "La infiltración policial en internet", *op. cit.* nota 210, p. 119
[238] Groupe de travail interministériel sur la lutte contre la cybercriminalité, *Protéger les Internautes - Rapport sur la cybercriminalité*, Francia, febrero de 2014, pp. 37–38
[239] Artículo 230-46.3° del Code de procédure pénale
[240] Lo que ha sido criticado en España, y no en Francia, véase por ejemplo, F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, p. 118

se precisa en Francia que se puede transmitir "*contenido ilegal proporcionado por el Centro Nacional de Análisis de Imágenes de Pornografía Infantil y que no permite la identificación de personas físicas*"[241]. Resulta que la doctrina considera que "*debería haberse limitado el tipo de archivos que se pueden enviar, ya que, en nuestra opinión, no debe permitirse en ningún caso la creación de nuevas imágenes de pornografía infantil para su intercambio en este tipo de operaciones o el envío de imágenes de pornografía infantil que nunca hayan circulado previamente por Internet*"[242].

Un último tema tiene que ser mencionado en relación con el agente encubierto: son delimitación con el agente provocador o delito provocado, que constituye "*el principal límite que debe presidir la actuación del agente encubierto*"[243]. En efecto, se prohíbe que los agentes de policía inducen de manera engañosa a una persona para que cometa un delito[244]. En caso de ser considerado delito provocado, los resultados de las diligencias se harán nulas[245]. En particular, cuando el agente "*intercambiar material ilícito con el investigado podría llevar a la defensa a una acusación de inducción al delito por parte del propio agente*"[246]. De manera sencilla, se considera que la autorización judicial permite excluir en todo caso la existencia de

[241] Artículo D47-9 del Code de procédure pénale
[242] M.L. Villamarín López, "La nueva figura del agente encubierto online en la lucha contra la pornografía infantil", *op. cit.* nota 205. Incluso otro autor considera que no se debería poder utilizar "*material recabado previamente en otras operaciones*", V. de Jorge Pérez, "El escondite virtual y el nuevo agente encubierto", *op. cit.* nota 232, p. 251. Consecuente, se propone la creación de "*material camuflado creado* ah hoc", con actores profesionales "*que aparezcan como menores de edad*", F. Bueno de Mata, "El agente encubierto en Internet como instrumento para la lucha contra el 'child grooming' y el 'sexting'", *op. cit.* nota 210, p. 13 ; F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, p. 119
[243] B. Rizo Gómez, "La infiltración policial en internet", *op. cit.* nota 210, p. 123
[244] Artículo 282 bis.5 de la LECrim, y M.L. Villamarín López, "La nueva figura del agente encubierto online en la lucha contra la pornografía infantil", *op. cit.* nota 205. De manera más precisa, "*el delito provocado se integra por tres elementos: 1. Un elemento subjetivo constituido por una incitación engañosa a delinquir por parte del agente a quien no está decidido a delinquir. 2. Un elemento objetivo, consistente en la detención del sujeto provocado que comete el delito inducido. 3. Un elemento material que consiste en la inexistencia de riesgo alguno para el bien jurídico protegido y, como consecuencia, la atipicidad de tal acción*", F. Harbottle Quirós, "El agente encubierto informático", *op. cit.* nota 220, pp. 126–128. Para un resumen de las diferencias entre agente encubierto y delito provocado, véase la sentencia del Tribunal Supremo. Sala Segunda, de lo Penal, el 7 de febrero de 2019, núm. 65/2019
[245] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 519
[246] A. Valiño Ces, "El agente encubierto informático y la ciberdelincuencia. El intercambio de archivos ilícitos para la lucha contra los delitos de pornografía infantil", *en* F. Bueno de Mata (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*, Comares, 2016, p. 284

un delito provocado[247]. Además, existiría una relación previa con el investigado y ya se habría comprobado la comisión de delitos[248]. Aunque se considera clara y asentada la jurisprudencia en la materia[249], el límite sigue siendo tenue.

Por el contrario, en Francia, el tema resulta en amplias reflexiones por la doctrina, dado la evolución de la jurisprudencia de la Corte de Casación, bajo el principio de la lealtad de las pruebas[250]. Las pruebas desleales no serán entonces admisibles en el proceso. La jurisprudencia francesa se basa en el criterio de la distinción entre la provocación a la comisión de un delito, y la provocación a la producción de pruebas[251]. Dicho criterio se ha introducido explícitamente en el régimen de la ciber infiltración[252]. El objetivo general es determinar si los actos del agente encubierto provocan que la persona afectada pierda su libre albedrío para cometer un delito[253]. Sin embargo, se critica que la jurisprudencia francesa es muy inestable[254].

---

[247] B. Rizo Gómez, "La infiltración policial en internet", *op. cit.* nota 210, p. 118

[248] F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, pp. 120–121. En particular, se consideraron admisibles las pruebas obtenidas mediante procedimientos engañosos relacionados con delitos ya cometidos, y luego con delitos que se estaban cometiendo o durante los actos de preparación, A. Melón Muñoz (ed.), *Procesal penal 2021*, Francis Lefebvre, Memento práctico, 2020, ¶ 5143–5149

[249] J.L. De la Cuesta, "Organised Crime Control Policies in Spain: A 'Disorganised' Criminal Policy for 'Organised' Crime", *en* C. Fijnaut, L. Paoli (eds.), *Organised crime in Europe: concepts, patterns and control policies in the European Union and beyond*, Springer, Studies of organized crime núm. 4, 1a ed., 2006, p. 809. Por lo que no todos los autores lo consideran cuando tratan de la figura del agente encubierto en Internet

[250] Este principio no desencadena de un texto legal. Dicho concepto se desarrolló para mitigar el principio de libertad de las pruebas (artículo 427 del Code de procédure pénale) y para fijar los límites de cómo se pueden obtener las pruebas. El principio se aplica a los magistrados desde 1888, H. Vlamynck, "La loyauté de la preuve au stade de l'enquête policière", *Actualité juridique Pénal*, Dalloz, 2014, p. 325; y a la policía judicial desde 1952, E. Vergès, "Loyauté et licéité, deux apports majeurs à la théorie de la preuve pénale", *Recueil Dalloz*, 2014, p. 407. Sin embargo, la mención explícita del concepto fue desarrollada más tarde, Cour de Cassation, Chambre criminelle, el 27 de febrero de 1996, núm. 95-81366

[251] A. Bensoussan, A. Lepage, M. Quéméner, "Loyauté de la preuve et nouvelles technologies : entre exigences processuelles et efficacité répressive", *Les transformations de la justice pénale: cycle de conférences 2013 à la Cour de cassation*, 2014, p. 236 ; M. Quéméner, "Infiltrations numériques", *op. cit.* nota 209, ¶ 39

[252] Sin embargo, esta disposición se limita a los actos considerados en el artículo 230-46.3° del Code de procédure pénale, lo que no es coherente con la práctica, ya que cualquier acto podría en teoría provocar el delito

[253] La doctrina menciona varios criterios, como la actividad delictiva previa, el objetivo social de la medida, la gravedad del delito, el carácter del delincuente, … P. Maistre du Chambon, "La régularité des « provocations policières » : l'évolution de la jurisprudence", *La Semaine Juridique Edition Générale*, LexisNexis, el 27 de diciembre de 1989, núm. 51, ¶ 8, 10, 15

[254] M. Quéméner, "Les spécificités juridiques de la preuve numérique", *Actualité juridique Pénal*, Dalloz, 2014, p. 63 ; J.-B. Perrier, "Le fair-play de la preuve pénale", *Actualité juridique Pénal*, Dalloz, 2017, p. 436 ; A. Lepage, "Provocation sur Internet - La distinction entre provocation à la preuve et provocation

Tres decisiones de la misma sala de la Corte de Casación consideran la creación de sitios para atraer delincuentes e identificarlos. En la primera decisión, sobre un sitio de pornografía infantil creado por fuerzas de seguridad, la Corte decide, sin motivación detallada, que dicha técnica era desleal, y entonces, todas las pruebas, incluidas las del registro posteriores[255], no podían ser admisibles[256]. En la segunda decisión, sobre el mismo caso, la Corte subraya que no hay elementos previos para sospechar la existencia del delito, por lo cual la diligencia es desleal[257]. Por tanto, parece basarse en el criterio del agente pasivo, exigiendo indicios previos de la comisión o preparación de un delito. Por el contrario, en la tercera decisión, sobre la creación de un fórum hablando de fraudes con tarjetas bancarias, la Corte considera la prueba leal, aunque no habían indicios anteriores a los recabados en el sitio[258]. En consecuencia, el criterio de la Corte de Casación no parece ser la existencia de indicios previos, sino el comportamiento pasivo o activo de la persona investigada. La mera conexión a un sitio de pornografía infantil no crea la sospecha de que la persona sea un delincuente[259], sobre todo porque el delito no se habría cometido sin el sitio falso. Gracias a la presunción de inocencia, siempre se puede considerar que hacer clic en un enlace podría haber sido un error[260]. Por el contrario, si la persona sospechosa escribe mensajes después de aceptar la invitación a unirse al foro, el proceso no sería desleal.

à la commission d'une infraction à l'épreuve d'Internet", *Communication Commerce électronique*, septiembre de 2014, núm. 9. Para una lista de la jurisprudencia que admite o excluye las pruebas leales o desleales, véase H. Vlamynck, "La loyauté de la preuve au stade de l'enquête policière", *op. cit.* nota 250, p. 325

[255] La inadmisión de la prueba se basa en la cronología de los actos procesales, anulando todas las pruebas obtenidas con posterioridad a la diligencia desleal. El tribunal no tiene en cuenta la cronología de la comisión de los delitos, J. Francillon, "Provocation à la commission d'actes de pédophilie organisée par un service de police étranger utilisant le réseau internet (suite)", *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2008, p. 621

[256] Cour de Cassation, Chambre criminelle, el 7 de febrero de 2007, núm. 06-87753

[257] Cour de Cassation, Chambre criminelle, el 4 de junio de 2008, núm. 08-81045

[258] Cour de Cassation, Chambre criminelle, el 30 de abril de 2014, núm. 13-88162

[259] J. Francillon, "Cyberdélinquance et provocations policières", *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2014, p. 577

[260] J. Buisson, "Contrôle de l'éventuelle provocation policière : création d'un site pédo-pornographique un policier, même étranger", *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2008, p. 663. Sin embargo, si la identificación del delincuente va seguida de la vigilancia de sus acciones en Internet y se demuestra que la persona consultó varios sitios similares, la duda podría haberse despejado. Esta jurisprudencia anima entonces a las autoridades policiales a reunir más pruebas.

Dos otras decisiones, de otras salas de la Corte de Casación, tratan del delito provocado. El fiscal pidió a un policía que actuara como amigo de la víctima para negociar y obtener pruebas de un delito de extorsión. La Corte subraya que el agente utilizaba un seudónimo y que algunas de las conversaciones telefónicas tuvieron lugar por su iniciativa[261]. Sobre esta base, considera el proceso desleal y las pruebas inadmisibles[262]. Dos años después, el mismo caso fue resuelto una segunda vez por la asamblea plenaria de la Corte. La decisión no menciona los criterios utilizados por la otra sala de la Corte y considera que el proceso fue leal, incluso cuando el agente se puso en contacto con los delincuentes, ya que estos tenían un plan muy detallado, cuya comisión no dependía de la acción del agente[263].

Por lo tanto, es evidente que la Corte de Casación sigue esforzándose por establecer criterios que proporcionen un régimen coherente de la lealtad de la prueba. De momento, la jurisprudencia actual crea inestabilidad jurídica en torno a dicho principio, lo que resulta en una falta de delimitación clara entre los poderes lícitos del agente encubierto en Internet y la prohibición del delito provocado.

Al presentar la regulación de las diligencias tecnológicas consideradas en España y en Francia, se puede deducir que estas son, de manera general, muy similares, dado que se acoplan al estado tecnológico en el momento de sus reformas. Sin embargo, el estudio comparado permite poner de manifiesto algunas diferencias y faltas nacionales, con el fin de orientar potencialmente al legislador en futuras reformas. Ahora bien, las legislaciones española y francesa tienen que conformarse ambas a un mismo marco supranacional: el convenio europeo sobre derechos humanos.

[261] G. Pitti, “L’affaire de la sextape : on ne dribble pas le principe de loyauté des preuves !”, *Gazette du Palais*, el 19 de septiembre de 2017, núm. 31, p. 18
[262] Cour de Cassation, Chambre criminelle, el 11 de julio de 2017, núm. 17-80313
[263] Cour de Cassation, Assemblée plénière, el 9 de diciembre de 2019, núm. 18-86767, ¶ 27–31

III. DILIGENCIAS TECNOLÓGICAS: CONFORMIDAD A LA JURISPRUDENCIA DEL TEDH

En 1994, a nivel internacional, universitarios subrayaron que si la evolución de la criminalidad necesitaba ofrecer nuevos poderes de investigación, esos poderes debían "*equilibrarse con una adecuada protección de los derechos humanos y la privacidad*"[264]. En el plano jurisdiccional, el TEDH ya había planteado estas cuestiones diez años antes, y desarrolló una jurisprudencia muy amplia sobre la regulación de las diligencias de investigación[265], precisamente de diligencias tecnológicas[266] (o, como el tribunal las llama, medidas de vigilancia secretas[267]). Según dicha jurisprudencia, estas deben ser evaluadas en relación con el derecho a la vida privada[268]. De hecho, conforme con jurisprudencia clásica, el tribunal amplió el concepto de privacidad para incluir las interceptaciones telefónicas[269], pero también, cualquier tipo de datos obtenidos y conservados durante una investigación[270], ya que

[264] Association internationale de droit pénal, "XV^{ème} congrès international de droit pénal (Rio de Janeiro, 4 – 10 septembre 1994)", *Revue internationale de droit pénal*, ERES, 2015, vol. 86, núm. 2015/1, ¶ 16–19

[265] TEDH, *Klass y otros c. Alemania*, el 6 de septiembre de 1978, núm. 5029/71 ; TEDH, *Malone c. Reino Unido*, el 2 de agosto de 1984, núm. 8691/79

[266] Mayoritariamente en cuanto a interceptaciones de las comunicaciones (tanto por la policía como por los servicios de inteligencia, siempre que sean secretas) y geolocalización. Es necesario subrayar que el tribunal considera que la geolocalización, y en general la obtención de datos de localización, constituye una injerencia menor para el derecho a la vida privada, en comparación con los datos de imagen o sonido, TEDH, *Uzun c. Alemania*, el 2 de septiembre de 2010, núm. 35623/05, ¶ 52. La jurisprudencia también resolvió casos sobre dispositivos de escucha encubierta o grabación de vídeo, TEDH, *Allan c. Reino Unido*, el 5 de noviembre de 2002, núm. 48539/99 ; TEDH, *P.G. y J.H. c. Reino Unido*, el 25 de septiembre de 2001, núm. 44787/98 ; TEDH, *Vetter c. Francia*, *op. cit.* nota 8; interceptación masiva de comunicaciones, TEDH, *Liberty y otros c. Reino Unido*, el 1 de julio de 2008, núm. 58243/00 ; TEDH, *Big Brother Watch y otros c. Reino Unido (1)*, el 13 de septiembre de 2018, 58170/13, 62322/14 and 24960/15 ; TEDH, *Centrum För Rättvisa c. Suecia (2)*, el 25 de mayo de 2021, núm. 35252/08; divulgación de datos por parte de los proveedores de servicios en línea, TEDH, *Benedik c. Eslovenia*, el 24 de abril de 2018, núm. 62357/14 ; TEDH, *Ringler c. Austria*, el 12 de mayo de 2020, núm. 2309/10

[267] La doctrina francesa también utiliza la expresión de medidas "clandestinas", véase J.-C. Saint-Pau, "Les investigations numériques et le droit au respect de la vie privée", *Actualité juridique Pénal*, Dalloz, 2017, p. 321

[268] Artículo 8 del convenio europeo de derechos humanos

[269] TEDH, *Klass y otros c. Alemania*, *op. cit.* nota 265, ¶ 41 ; TEDH, *Malone c. Reino Unido*, *op. cit.* nota 265, ¶ 64

[270] TEDH, *Amann c. Suiza*, el 18 de octubre de 2011, núm. 27798/95, ¶ 65 ; TEDH, *Leander c. Suecia*, el 26 de marzo de 1987, núm. 9248/81, ¶ 48

la "*vida privada es un término amplio no susceptible de definición exhaustiva*"[271]. Por lo tanto, las diligencias tecnológicas suponen una injerencia en el derecho a la vida privada.

Para asegurarse de que su legislación se ajusta al artículo 8 del CPHR, los países deberían tener en cuenta esta jurisprudencia, y no esperar a una condena para modificarla. Estas condenas son particularmente fáciles de obtener, ya que el tribunal interpretó ampliamente la noción de víctima[272]. Así, el tribunal "*acepta […] que un individuo pueda […] pretenderse víctima de una violación ocasionada por la simple existencia de medidas secretas o de una legislación que permita estas medidas, sin tener que alegar que tales medidas le han sido, en efecto, aplicadas a él*"[273]. Precisamente, el tribunal, para considerar a una persona como víctima, estudiará "*la disponibilidad de cualquier recurso a nivel nacional y el riesgo de que se apliquen medidas secretas de vigilancia*" a esa persona[274].

Para legitimar la injerencia a la vida privada, los Estados deben justificar que la diligencia "*esté prevista por la ley*", basada en objetivos legítimos y es necesaria "*en una sociedad democrática*"[275]. Generalmente, el segundo criterio no se estudia, dado que se considera justificadas la creación y la implementación de diligencias tecnológicas para "*la defensa del orden y la prevención de las infracciones penales*"[276]. Además, el primer y el tercero criterios son generalmente juntados en el estudio llevado a cabo por el tribunal[277]. El tribunal suele estudiar el marco nacional desde la perspectiva del primer criterio, lo que significa que la ley debe incluir disposiciones específicas[278]. Estas disposiciones tienen que ser más claras y

[271] TEDH, *Benedik c. Eslovenia*, *op. cit.* nota 266, ¶ 100. Se subrayar que el concepto de vida privada incluye los datos obtenidos en el espacio público, TEDH, *P.G. y J.H. c. Reino Unido*, *op. cit.* nota 266, ¶ 56 ; TEDH, *Peck c. Reino Unido*, el 28 de enero de 2003, núm. 44647/98, ¶ 59

[272] Artículo 34 del convenio europeo de derechos humanos

[273] TEDH, *Klass y otros c. Alemania*, *op. cit.* nota 265, ¶ 34. Para las medidas llevadas a cabo por los servicios de inteligencia, el TEDH exige la posibilidad de presentar una denuncia ante los tribunales sin necesidad de notificación si una persona sospecha que se ha vulnerado su derecho a la intimidad (en particular, la interceptación de sus comunicaciones), TEDH, *Kennedy c. Reino Unido*, el 18 de mayo de 2010, núm. 26839/05, ¶ 167.

[274] TEDH, *Kennedy c. Reino Unido*, *op. cit.* nota 273, ¶ 124

[275] Artículo 8.2 del convenio europeo de derechos humanos

[276] Artículo 8.2 del convenio europeo de derechos humanos

[277] Para una clara fusión de estos dos criterios, véase TEDH, *Roman Zakharov c. Rusia*, el 4 de diciembre de 2015, núm. 47143/06, ¶ 236

[278] El tribunal considera si existe una base legal, su accesibilidad y su previsibilidad, que es el punto que está más desarrollado, TEDH, *Kruslin c. Francia*, *op. cit.* nota 8, ¶ 27 ; TEDH, *Kopp c. Suiza*, el 25 de marzo de 1998, núm. 13/1997/797/1000, ¶ 55. En cuanto a la accesibilidad, algunos autores

detalladas a medida que se mejoren los dispositivos técnicos utilizados en las diligencias tecnológicas: el tribunal subrayó desde el principio que su jurisprudencia evolucionaría con el marco técnico[279]. Los requisitos, para que las diligencias tecnológicas se ajusten al artículo 8 del convenio europea y a la jurisprudencia del TEDH, pueden agruparse en tres categorías: alcance de la diligencia, procedimiento de la diligencia y protección de los datos obtenidos.

1. Alcance de la diligencia

En primer lugar, la ley debe regular el alcance de las diligencias tecnológicas. Dicho ámbito puede dividirse en tres componentes: "*(1) la naturaleza de los delitos […]; (2) la definición de las categorías de personas [que pueden ser afectadas]; (3) la duración máxima de la ejecución de la medida*"[280]. Estos límites son coherentes con la prohibición de "*conservación generalizada e indiferenciada de los datos*" desarrollada por el Tribunal de Justicia de la Unión Europea[281]. Así, la regulación de las diligencias tecnológicas debe prever su ámbito personal, material y temporal.

franceses han criticado la escasa calidad de la redacción de los textos en las técnicas de investigación digital y su inestabilidad debido al gran número de enmiendas, E. De Marco, "La captation des données", *en* K. Blay-Grabarczyk et al. (eds.), *Le nouveau cadre législatif de la lutte contre le terrorisme à l'épreuve des droits fondamentaux*, Institut Universitaire Varenne, Collection "Colloques & Essais" núm. 44, 2017, pp. 99–100 ; C. Lazerges, "Dédoublement de la procédure pénale et garantie des droits fondamentaux", *en* B. Bouloc, F. Alt-Maes (eds.), *Les droits et le droit: mélanges dédiés à Bernard Bouloc*, Dalloz, 2007, p. 589

[279] TEDH, *Kruslin c. Francia*, *op. cit.* nota 8, ¶ 33 ; TEDH, *Kopp c. Suiza*, *op. cit.* nota 278, ¶ 72

[280] TEDH, *Centrum För Rättvisa c. Suecia (2)*, *op. cit.* nota 266, ¶ 249 ; TEDH, *Huvig c. Francia*, *op. cit.* nota 8, ¶ 34 ; TEDH, *Valenzuela Contreras c. España*, el 30 de julio de 1998, núm. 58/1997/842/1048, ¶ 46 ; TEDH, *Weber y Saravia c. Alemania*, el 29 de junio de 2006, núm. 54934/00, ¶ 95 ; TEDH, *Amann c. Suiza*, *op. cit.* nota 270, ¶ 56–58 ; TEDH, *Roman Zakharov c. Rusia*, *op. cit.* nota 277, ¶ 243, 250

[281] Véase por ejemplo, TJUE, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs c. Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées ; y Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX c. Conseil des ministres*, el 6 de octubre de 2020, C-511/18, C-512/18 y C-520/18, ¶ 141 ; TJUE, *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service*, el 6 de octubre de 2020, C-623/17, ¶ 82

A. Ámbito personal

El ámbito personal de las diligencias tecnológicas contempla las personas que pueden ser objeto de las medidas. Lógicamente, la categoría principal serían las personas investigadas, lo cual está muy claro en la legislación española sobre interceptación de comunicaciones y captación de comunicaciones orales[282]: los terminales interceptados "*han de ser aquellos habitual u ocasionalmente utilizados por el investigado*"[283]; las comunicaciones captadas deben ser llevadas a cabo por el investigado[284]. La afectación de otras personas solamente será posible, en el primer caso, cuando "*1.º exista constancia de que el sujeto investigado se sirve de aquella para transmitir o recibir información, o 2.º el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad*"[285]; o cuando estén comunicándose con el investigado en el segundo caso[286]. Sin embargo, la ley extiende la medida al dispositivo de la víctima en caso de "*grave riesgo para su vida o integridad*"[287]. Por el contrario, las categorías de personas afectadas por un registro informático en Francia son muy amplias: el ámbito personal se extiende a todas las "*personas que parezcan haber participado en el delito o que estén en posesión de documentos, información u objetos relacionados con el mismo*"[288]. Similarmente, el agente encubierto puede intercambiar "incluso con personas que puedan ser autores de delitos"[289], pero entonces no solamente con estas.

---

[282] Y en materia de captación de imágenes en lugares públicos, artículo 588 quinquies a de la LECrim, que diferencia entre la captación de la imagen del investigado y de otras personas. Véase por ejemplo la sentencia del Tribunal Supremo. Sala Segunda, de lo Penal, el 18 de abril de 2017, núm. 272/2017

[283] Artículo 588 ter b.1 de la LECrim. Anteriormente a la reforma de 2015, la jurisprudencia había considerado que la ausencia de identificación inicial no suponía una indeterminación subjetiva de la autorización, E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 313

[284] Artículo 588 quater b.1 de la LECrim

[285] Artículo 588 ter c de la LECrim

[286] Artículo 588 quater b.1 de la LECrim. Pero la autorización siempre tendrá que especificar el investigado que participará en el encuentro, O. Martín Sagrado, "La necesaria delimitación del ámbito subjetivo y de la duración de la captación de comunicaciones orales", *en* O. Fuentes Soriano, P. Arrabal Platero, M. Alcaraz Ramos (eds.), *Era digital, sociedad y derecho*, Tirant lo Blanch, Monografías, 2020, pp. 510–512

[287] Artículo 588 ter b.2 ¶2 de la LECrim

[288] Artículo 56 ¶1 del Code de procédure pénale. En cuanto al registro remoto, artículo 706-12-1, se critica el alcance personal por no limitarse a la persona sospechosa o a los "*datos a los que la persona sospechosa tiene acceso cuando se identifica en el sistema informático*", B. Roussel, *Les investigations numériques en procédure pénale*, *op. cit.* nota 1, p. 93

[289] Artículo 230-46.1° del Code de procédure pénale

Ahora bien, la legislación española considera de manera general la posibilidad de afectar a terceras personas en la implementación de las diligencias tecnológicas[290]. Los principios de especialidad y de idoneidad suponen que la autorización judicial delimite el ámbito subjetivo de las medidas. Al afectar terceros, se necesitará "*una motivación reforzada*"[291]. El precepto remite a la regulación de cada diligencia en la materia. Sin embargo, la mayoría de las regulaciones nacionales no contemplan la delimitación de las categorías de personas que pueden ser objeto de las diligencias tecnológicas (salvo, por ejemplo, en materia de interceptación de comunicaciones en España, como se ha mencionado[292]). Es especialmente el caso de la geolocalización en ambos países[293], y de la interceptación de las comunicaciones[294], del uso de drones[295], y del acceso a comunicaciones electrónicas[296] en Francia. De manera general, en España, se acepta la "*recogida de arrastre*" de datos de terceros de manera indirecta cuando relacionándose con el investigado[297]. Sin afectar más de lo proporcional a los derechos de terceros, tampoco se puede vaciar de contenido las diligencias tecnológicas[298].

[290] Artículo 588 bis h de la LECrim

[291] I. López-Barajas Perea, "Garantías Constitucionales En La Investigación Tecnológica Del Delito", *op. cit.* nota 10, p. 112

[292] Sin embargo, la doctrina ha propuesto que el concepto aplicable a las interceptaciones sea aplicado a otras diligencias, en particular a las captaciones de comunicaciones orales, E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 460, o a los registros remotos, L. Bachmaier Winter, "Registro remoto de equipos informáticos en la Ley Orgánica 13/2015", *op. cit.* nota 184

[293] Artículo 588 quinquies b de la LECrim y artículo 230-32 del Code de procédure pénale, M. Quéméner, "Fascicule 982 : Géolocalisation dans le cadre pénal - Articles 689 à 693", *JurisClasseur Communication*, LexisNexis, el 3 de julio de 2019, ¶ 29

[294] Artículo 100 del Code de procédure pénale, complementada por la jurisprudencia que subraya que las personas afectadas por la medida no tienen que ser "*sólo aquellas sobre las que existen indicios de culpabilidad*", Cour de Cassation, Chambre criminelle, el 17 de julio de 1990, núm. 90-82614 ; Cour de Cassation, Chambre criminelle, el 26 de noviembre de 1990, núm. 90-84590 ; Cour de Cassation, Chambre criminelle, el 9 de diciembre de 1991, núm. 88-80786, 90-84994

[295] Artículo 230-47 del Code de procédure pénale

[296] Artículo 706-95-1 del Code de procédure pénale

[297] Fiscalía General del Estado, Circular 1/2019 sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal, el 6 de marzo de 2019, pp. 30073–30074. En particular en materia de interceptaciones: Fiscalía General del Estado, Circular 2/2019, *op. cit.* nota 65, pp. 30099–30101

[298] M. Cedeño Hernán, "Las medidas de investigación tecnológica", *op. cit.* nota 13

No obstante, los dos países consideran disposiciones específicas para la investigación de determinadas categorías de personas, lo que también es especialmente estudiado por el TEDH[299]. España considera la restricción de los registros en espacios privados, que se aplicarán a los potenciales registros informáticos llevados a cabo en estos espacios[300]. Se protege de manera amplia las conversaciones y comunicaciones entre los abogados y sus clientes, cuyas grabaciones se tendrán que eliminar[301].

De manera general, Francia desarrolla más las restricciones del ámbito personal de las diligencias tecnológicas. Se restringen los registros en los espacios profesionales de un abogado[302], una empresa de medios de comunicación[303], un médico, un notario, un agente judicial[304], un lugar con elementos "*protegidos por el secreto de la defensa nacional*"[305], y una "*persona que ejerce funciones jurisdiccionales y que tiende a la incautación de documentos probablemente amparados por el secreto de la deliberación*"[306]. En Francia, las restricciones del ámbito personal también van más allá y se prevén en materia de cesión de datos (personas obligadas al secreto profesional[307] y en particular abogados[308]), de interceptación de las comunicaciones y de acceso remoto a las correspondencias electrónicas (miembros del Parlamento, abogados y magistrados[309]). El registro remoto sin conocimiento de la persona interesada excluye los dispositivos relacionados con las categorías de personas mencionadas para tanto los registros informáticos como para las interceptaciones de comunicaciones[310]. Resulta entonces dudoso en relación con la conformidad a la jurisprudencia del TEDH que

[299] TEDH, *Kopp c. Suiza*, *op. cit.* nota 278, ¶ 73 ; TEDH, *Aalmoes y otros c. Países Bajos*, el 25 de noviembre de 2004, núm. 16269/02, p. 24
[300] Estas restricciones del régimen de entrada en espacios privados se refieren a: Parlamento, artículo 548 de la LECrim, lugares religiosos, artículo 549, lugares reales, artículos 555 y 556, representantes de naciones extranjeras, artículos 559 y 560, buques de guerra extranjeros, artículo 561, cónsules extranjeros, artículo 562. Sin embargo, todos esos lugares no se consideran "*registros domiciliarios*", mientras que el artículo sobre el registro informático se limita a esa situación, artículo 588 sexies a
[301] Artículo 118.4 de la LECrim
[302] Artículo 56-1 del Code de procédure pénale
[303] Artículo 56-2 del Code de procédure pénale
[304] Artículo 56-3 del Code de procédure pénale
[305] Artículo 56-4 del Code de procédure pénale
[306] Artículo 56-5 del Code de procédure pénale
[307] Artículo 60-1 del Code de procédure pénale
[308] Artículo 60-1-1 del Code de procédure pénale
[309] Artículos 100-7 y 706-95-3 del Code de procédure pénale
[310] Artículo 706-102-5 ¶ 3 del Code de procédure pénale

similares restricciones no se hayan extendidas en España a las demás diligencias tecnológicas.

Sin embargo, este criterio puede considerarse inapropiado para las diligencias que se enfocan en un objeto o dispositivo específico y no en una persona. Por ejemplo, la regulación francesa de la geolocalización también puede utilizarse para rastrear cualquier tipo de objetos, independientemente de una persona concreta[311]. Otro ejemplo es el marco español sobre registros informáticos que se centra más en el dispositivo concreto que en la persona vinculada a él[312]. Por lo tanto, en material de registros remotos mediante software, las disposiciones francesas y españolas no definen las categorías de personas que pueden enfrentarse a esta medida, sino que la autorización debe limitarse a especificar el dispositivo en cuestión[313]. Aún más amplio, el dispositivo IMSI catcher, en su funcionamiento, ni siquiera selecciona un dispositivo concreto, sino se limita a un espacio geográfico[314]. Un alcance similar se considera para la grabación de imágenes y sonidos en el marco francés, ya que la autorización tiene que especificar lugares y no personas[315]. Una evolución de este criterio del TEDH permitiría tener en cuenta las dificultades de la investigación, cuando a veces un dispositivo aún no está vinculado a una persona física.

311 Artículo 230-32 del Code de procédure pénale, M. Quéméner, "Géolocalisation dans le cadre pénal", *op. cit.* nota 293, ¶ 30

312 Artículo 588 sexies a de la LECrim

313 Artículo 706-102-3 del Code de procédure pénale y artículo 588 septies a.2.a de la LECrim. Se critica la regulación española por no especificar "*si el registro remoto sólo puede acordarse para acceder al ordenador del sospechoso o si puede también autorizarse para registrar el ordenador que, aun siendo de otro sujeto, posiblemente está siendo utilizado por el sospechoso para almacenar datos o para comunicarse*", ni "*si puede autorizarse el registro remoto del ordenador de un tercero, aunque no esté siendo utilizado por el sospechoso, pero en el cual pueden existir datos relevantes para el esclarecimiento del delito*", L. Bachmaier Winter, "Registro remoto de equipos informáticos en la Ley Orgánica 13/2015", *op. cit.* nota 184. Se subraya que la delimitación subjetiva de una diligencia que tanto afecta a la vida privada necesitaría más precisión, I. López-Barajas Perea, "El derecho a la protección del entorno virtual y sus límites", *op. cit.* nota 28, p. 167

314 Aunque, en la normativa francesa, si se interceptan las comunicaciones, deben limitarse a la persona o al dispositivo especificado en la autorización, artículo 706-95-20.II del Code de procédure pénale. También véase el artículo 588 ter l de la LECrim

315 Artículo 706-97 del Code de procédure pénale

Una vez estudiado el ámbito personal de las diligencias tecnológicas, cabe atender a su ámbito material, es decir, los delitos por los que se pueden implementar.

B. Ámbito material

En segundo lugar, el ámbito de aplicación de las diligencias debe definir la naturaleza de los delitos que pueden dar lugar a la autorización de dichas diligencias: "*la condición de previsibilidad no exige que los Estados listen exhaustivamente por su nombre los delitos concretos que pueden dar lugar a la [diligencia]. Sin embargo, se debe detallar suficientemente la naturaleza de los delitos en cuestión*"[316]. Casi todas las diligencias tecnológicas cumplen con este criterio. Sin embargo, determinadas diligencias no fijan un ámbito material explícito, dejando a la persona autorizando la medida el deber de justificar su proporcionalidad. Así, de manera general, en ambos países, los registros informáticos pueden implementarse para cualquier delito[317]. Esta medida se lleva a cabo con el conocimiento de la persona interesada, por lo cual no se consideraría aplicable la jurisprudencia estudiada del TEDH y se tendrá que acudir al artículo 6 del convenio. Más cuestionable resulta en España la ausencia de ámbito material para la geolocalización[318], y la falta de referencia a la aplicación del ámbito material de las interceptaciones de comunicaciones para la incorporación al proceso de datos electrónicos de tráfico o asociados y el acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad.

Al definir el ámbito material, los Estados pueden delimitarlo mediante una lista de delitos. Hay que subrayar que si la lista es exhaustiva, el TEDH prohíbe ampliarla por analogía o por jurisprudencia[319]. Por ejemplo, en España, el ámbito material del agente encubierto en Internet

[316] TEDH, *Kennedy c. Reino Unido*, *op. cit.* nota 273, ¶ 159
[317] Artículo 588 sexies a de la LECrim y artículo 57-1 del Code de procédure pénale
[318] Artículo 588 quinquies b de la LECrim sólo considera los principios de necesidad y proporcionalidad, que deben desarrollarse en la autorización, artículo 588 bis b.2.1° y 2°
[319] TEDH, *Dumitri Popescu c. Rumania*, el 26 de abril de 2007, núm. 71525/01, ¶ 64

se basa en parte en una lista de delitos cometidos en un grupo organizado[320]. En Francia, el código lista los delitos considerados como parte de la criminalidad organizada[321].

De manera diferente, los Estados pueden definir un umbral para fijar el alcance material como nivel de gravedad de la infracción. A este respecto, el TEDH suele exigir un cierto nivel de gravedad, pero una categoría de delito muy amplia no supone una violación del artículo 8 del convenio[322]. Esta flexibilidad del tribunal en ese criterio podría ser muy criticada con respecto al principio de proporcionalidad derivado del criterio de "necesario para una sociedad democrática". Por el contrario, para las técnicas de investigación masiva, el tribunal exige un nivel específico de gravedad de los delitos perseguidos[323]. Parece ser la técnica más utilizada en ambas legislaciones estudiadas: son numerosas las diligencias tecnológicas delimitadas por un nivel de pena. Sin embargo, cuando es utilizado, siempre es un umbral de tres años de prisión como mínimo, aunque sean diligencias tecnológicas diferentes[324], lo que cuestiona la proporcionalidad de la regulación. En particular, este umbral "*no es excesivamente exigente*"[325], lo que a veces puede llegar a comprometer "*directamente el principio de proporcionalidad*"[326].

[320] Artículo 282 bis.4 de la LECrim

[321] Artículos 706-73 y 706-73-1 de la LECrim. Las listas se extienden cada vez más. El primer artículo sufró 18 reformas, y el segundo, seis

[322] El tribunal criticó la legislación de Rusia, donde el carterismo estaba incluido en una amplia lista de delitos que permitían la interceptación de las comunicaciones, TEDH, *Roman Zakharov c. Rusia*, *op. cit.* nota 277, ¶ 244.

[323] TEDH, *Big Brother Watch y otros c. Reino Unido (1)*, *op. cit.* nota 266, ¶ 386. La jurisprudencia del TJUE es más restrictiva al respecto, véase TJUE, *Tele2 Sverige AB c. Post-och telestyrelsen*, el 21 de diciembre de 2016, C-203/15 y C-698/15, ¶ 102 ; TJUE, *Ministerio Fiscal*, el 2 de octubre de 2018, C-207/16, ¶ 54

[324] En España, artículos 588 ter a y 579.1 de la LECrim en materia de interceptación de comunicaciones, y 588 quater b en materia de grabaciones de comunicaciones orales; en Francia, artículo 100 del Code de procédure pénale en materia de interceptación de comunicaciones, artículo 230-32 en materia de geolocalización, artículo 230-47 en materia de uso de drones, artículo 60-1-2 en materia de cesión de datos de tráfico

[325] J. Vegas Torres, "Las medidas de investigación tecnológica", *op. cit.* nota 10 ; F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, p. 67. En el sentido contrario, indicando que excluye gran parte de los delitos menos graves, véase, M. Neupavert Alzola, "Crítica a los presupuestos de adopción de diligencias de investigación tecnológica", *en* F. Bueno de la Mata, I. González Pulido, L.M. Bujosa Vadell (eds.), *Fodertics 9.0: Estudios sobre tecnologías disruptivas y justicia*, Comares, 2021, pp. 366–368

[326] A. Rodríguez Álvarez, "Intervención de las comunicaciones telefónicas y telemáticas y smartphones. Un primer estudio a propósito de la ley orgánica 13/2015, de 5 de octubre, de modificación de la ley de enjuiciamiento criminal", *en* J.M. Asencio Mellado, M. Fernández López (eds.), *Justicia penal y nuevas formas de delincuencia*, Tirant lo Blanch, Monografías, 1a ed., 2017, p. 158

Sin embargo, surgen más dudas cuando las diligencias definen su ámbito material utilizando nociones generales. Según el CEDH, los términos generales (como "delito grave", "orden público" o "seguridad nacional") pueden utilizarse para delimitar la naturaleza de los delitos, pero solamente si esos términos están definidos y pueden determinar un alcance claro[327]. Entonces, dentro de las dos legislaciones estudiadas, se tendrá que atender a la definición de dos términos generales.

En primer lugar, las legislaciones utilizan en varios conceptos la noción de delitos cometidos en el entorno digital[328]. En España, resulta de la jurisprudencia del Tribunal Supremo al interpretar la noción de delito grave: dicha gravedad no solamente se considera por la pena, sino que puede tener en cuenta "*la incidencia del uso de las tecnologías de la información*"[329]. Dicho concepto no se cuestiona en la doctrina francesa, pero sí sufre críticas de la doctrina española[330]. Este ámbito material, de por sí mismo, no se considera que puede justificar la adopción de una diligencia tecnológica, sino que se debe probar "*la mayor dificultad de esclarecer el delito en caso de que no se adopten medidas de investigación tecnológica*"[331], considerar "*la posible impunidad de la conducta si no se utiliza este instrumento de investigación, sino también la potencialidad lesiva del tipo penal por la amplificación que*

[327] TEDH, *Big Brother Watch y otros c. Reino Unido (2)*, el 25 de mayo de 2021, 58170/13, 62322/14 y 24960/15, ¶ 368–371. On the contrary, a failure to define the concept supposes a violation of Artículo 8, TEDH, *Iordachi y otros c. Moldavia*, el 10 de febrero de 2009, núm. 25198/02, ¶ 46. For the definitions, the TEDH does not take into account only the law, but also preparatory works, TEDH, *Centrum För Rättvisa c. Suecia (2)*, *op. cit.* nota 266, ¶ 287

[328] Artículo 588 ter a de la LECrim en materia de interceptación de comunicaciones, y artículo 588 septies a en materia de registro remoto: "*delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación*". Artículo 230-46 del Code de procédure pénale en materia de agente encubierto en Internet, artículo 100¶ 3 en materia de interceptación de comunicaciones: delitos "*cometidos a través de comunicaciones electrónicas*"

[329] C. Sanchís Crespo, "Puesta al día de la instrucción penal: la interceptación de las comunicaciones telefónicas y telemáticas", *La ley penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, 2017, núm. 125, p. 3 ; Tribunal Supremo. Sala Segunda, de lo Penal, el 3 de febrero de 2006, núm. 104/2006

[330] F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, p. 193

[331] L. Bachmaier Winter, "Registro remoto de equipos informáticos en la Ley Orgánica 13/2015", *op. cit.* nota 184. El autor considera este ámbito material particularmente desproporcional en materia de registro remoto. En el mismo sentido, I. López-Barajas Perea, "El derecho a la protección del entorno virtual y sus límites", *op. cit.* nota 28, p. 164

supone el uso de medios informáticos"[332]. Se critica en particular la ausencia de un mínimo de pena para complementar un término tan genérico[333], como se hace en Francia: no se consideran todos los delitos, sino solamente los delitos graves y menos graves con pena de prisión.

En segundo lugar, las dos legislaciones definen ciertos ámbitos materiales por la noción de "criminalidad organizada"[334]. Se define a nivel internacional en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional de 2000 (Convención de Palermo), ratificado por España como Francia. Considera la noción de "*grupo delictivo organizado*" como "*un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves […] con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material*"[335]. Esta definición se adoptó posteriormente en el Consejo de Europa[336]. La definición de la UE es casi idéntica, pero rebaja el umbral a una asociación de dos o más personas[337].

En España, las nociones están claramente definidas. La diligencia de ciber infiltración se basa en la noción de "delincuencia organizada", definida como: "*la asociación de tres o más personas para realizar, de forma permanente o reiterada*"[338] delitos especificados. La

---

[332] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 542

[333] L. Bachmaier Winter, "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *Boletín del Ministerio de Justicia*, Ministerio de Justicia, 2017, vol. 71, núm. 2195, p. 15

[334] Artículos 588 ter a y 579.1.2° de la LECrim en materia de interceptación de comunicaciones, artículo 588 quater b.2.a.2° en materia de captación de comunicaciones orales, artículo 588 septies a.1.a en materia de registro remoto, artículo 282 bis.4 en materia de agente encubierto en Internet; artículos 706-73, 706-73-1 y 706-74 del Code de procédure pénale

[335] Artículo 2.a del convenio de Palermo. Sigue definiendo el "*delito grave*" ("*conducta que constituya un delito punible con una privación de libertad máxima de al menos cuatro años o con una pena más grave*", artículo 2.b) y el "*grupo estructurado*" ("*grupo no formado fortuitamente para la comisión inmediata de un delito y en el que no necesariamente se haya asignado a sus miembros funciones formalmente definidas ni haya continuidad en la condición de miembro o exista una estructura desarrollada*", artículo 2.c)

[336] Comité de Ministros, "Recommendation Rec(2001)11 concerning guiding principles on the fight against organised crime", Consejo de Europa, el 19 de septiembre de 2001

[337] Decisión Marco 2008/841/JAI del Consejo, de 24 de octubre de 2008 , relativa a la lucha contra la delincuencia organizada, artículo 1.1

[338] Artículo 282 bis.4 de la LECrim. La definición fue introducida en 1999, antes de la Convención de Palermo, por la Ley Orgánica 5/1999 de modificación de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la acción investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves. Antes no se podía encontrar ninguna definición del concepto, aunque se

interceptación de las comunicaciones[339] y la captación de comunicaciones orales[340] se basan en la noción de "grupo u organización criminal", definida como "*la agrupación formada por más de dos personas con carácter estable o por tiempo indefinido, que de manera concertada y coordinada se repartan diversas tareas o funciones con el fin de cometer delitos*"[341]. Aunque puede dificultar una buena comprensión de la ley tener dos nociones muy similares, ambas están bien definidas.

En Francia, la noción de "grupo organizado" se define como una circunstancia agravante, como "*cualquier agrupación formada o cualquier acuerdo establecido con vistas a la preparación, caracterizada por uno o varios hechos materiales, de uno o varios delitos*"[342]. Esta definición es menos detallada, sin información sobre el número de personas implicadas, la base temporal del grupo y la naturaleza de los delitos que se preparan. Por lo tanto, la noción es criticada por la doctrina[343]. Dado que la Corte de Casación no proporciona una definición más detallada, las jurisdicciones se basaron en varios criterios, como una pluralidad de individuos en relación con el propósito de cometer el delito, actos preparatorios coordinados o una organización estructurada[344]. Debido a la falta de criterios bien determinados, la existencia o ausencia de la circunstancia queda en manos del fiscal[345] y casi no es controlado por la Corte de Casación[346]. Además, la circunstancia del crimen organizado

utilizaba en el Código penal como circunstancia agravante de ciertos delitos. Sin embargo, esta definición se consideraba limitada a la técnica de infiltración, J.L. De la Cuesta, "Organised Crime Control Policies in Spain", *op. cit.* nota 249, pp. 796–797. En el año 2000, la ley integra el concepto de "asociaciones ilícitas", pero éste es muy diferente al vinculado a la "delincuencia organizada", véase artículo 515 del Código penal.

339 Artículos 588 ter a y 579.1.2°de la LECrim

340 Artículo 588 quater b.2.a.2° de la LECrim

341 Artículo 570 bis del Código penal

342 Artículo 132-71 del Code pénal

343 C. Lazerges, "La dérive de la procédure pénale", *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2003, p. 644 ; E. Vergès, "La notion de criminalité organisée après la loi du 9 mai 2004", *Actualité juridique Pénal*, Dalloz, 2004, p. 181 ; T. Godefroy, "The Control of Organised Crime in France: A Fuzzy Concept but a Handy Reference", *en* C. Fijnaut, L. Paoli (eds.), *Organised crime in Europe: concepts, patterns and control policies in the European Union and beyond*, Springer, Studies of organized crime núm. 4, 1a ed., 2006, p. 763 ; C. Guerrier, "« Loppsi 2 » et l'utilisation des nouvelles technologies", *Revue Le Lamy Droit de l'immatériel*, el 1 de octubre de 2010, núm. 64 ; C. Lazerges, "Le déclin du droit pénal : l'émergence d'une politique criminelle de l'ennemi", *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2016, p. 649

344 E. Vergès, "La notion de criminalité organisée après la loi du 9 mai 2004", *op. cit.* nota 343, p. 181

345 C. Guerrier, "« Loppsi 2 » et l'utilisation des nouvelles technologies", *op. cit.* nota 343

346 E. Vergès, "La notion de criminalité organisée après la loi du 9 mai 2004", *op. cit.* nota 343, p. 181. However, in 2016, the court seemed to consider two criteria for the notion, that "*presupposes the*

no convence a muchos profesionales[347], que se basará más en la gravedad del delito que en la complejidad de los hechos[348]. Por lo tanto, la noción no parece ajustarse a la condición de previsibilidad del TEDH.

Una vez estudiados los ámbitos personales y materiales, queda por averiguar la conformidad de las legislaciones nacionales a los criterios desarrollados en cuanto al ámbito temporal.

C. Ámbito temporal

El alcance temporal se deja principalmente a "*la discreción de las autoridades nacionales pertinentes*"[349]. Sin embargo, una ley previsible debe indicar claramente "*el período tras el cual expirará una [diligencia], las condiciones en las que se puede renovar una orden y las circunstancias en las que debe ser cancelada*"[350]. El ámbito temporal se divide entonces en tres componentes.

En primer lugar, la ley tiene que definir la duración máxima de la medida[351]. En España, de manera general, se considera que las diligencias tecnológicas "*no podrán exceder del*

premeditation of the offences and a structured organization of its members," Cour de Cassation, Chambre criminelle, el 22 de junio de 2016, núm. 16-81834

[347] T. Godefroy, "The Control of Organised Crime in France", *op. cit.* nota 343, p. 763

[348] El Conseil Constitutionnel se basa en este último criterio para aplicar el principio de proporcionalidad, por ejemplo cuando censuró la extensión a cualquier delito de todas las técnicas especiales de investigación dentro de la instrucción, Conseil constitutionnel, *Loi de programmation 2018-2022 et de réforme pour la justice*, el 21 de marzo de 2019, 2019-778 DC, ¶ 161–166. Sin embargo, hay que subrayar que la motivación del Consejo también se basa en la falta de control por parte del juez de las libertades y la custodia dentro de la investigación de flagrancia y la investigación preliminar. Por lo tanto, estas técnicas podrían extenderse a delitos, sin que se den las circunstancias de un grupo de delincuencia organizada, si la técnica fuera controlada por un juez y no por un fiscal. Un interrogante similar surge de la censura por parte del Consejo de la extensión de la interceptación de las comunicaciones a la investigación de flagrancia y a las investigaciones preliminares, que se consideraba para cualquier delito castigado con un máximo de al menos tres años de prisión, *Ibid.* ¶ 138–147

[349] TEDH, *Kennedy c. Reino Unido*, *op. cit.* nota 273, ¶ 161, aunque el tribunal reconoce que "*la duración global de cualquier medida de interceptación [debe] depender de la complejidad y duración de la investigación en cuestión*".

[350] TEDH, *Roman Zakharov c. Rusia*, *op. cit.* nota 277, ¶ 250 ; TEDH, *Klass y otros c. Alemania*, *op. cit.* nota 265, ¶ 52

[351] Sin embargo, dicha técnica legislativa se critica en España por no ser lo suficientemente flexible, en particular en relación con la gravedad de los hechos, C. San Miguel Caso, "Los nuevos medios de

tiempo imprescindible para el esclarecimiento de los hechos"[352], que resulta ser un "*concepto jurídico indeterminado*"[353]. Afortunadamente, la ley precisa una duración numeral para algunas diligencias tecnológicas. Las interceptaciones de comunicaciones y la captación de datos de seguimiento son limitadas a tres meses[354]. El límite temporal es más reducido para los registros remotos (un mes)[355], "*por la extremada intrusión de esta diligencia en la vida privada del investigado*"[356]. Los mismos límites temporales (uno o cuatro meses según el procedimiento) se establecen en Francia para la casi totalidad de las diligencias: la interceptación de comunicaciones, la geolocalización, el uso de drones, la captación de sonidos e imágenes, la captación de datos informáticos y el uso del *IMSI catcher*[357]. Considerando que los límites temporales son muy similares, dicho criterio se podría regular de manera armonizada para todas las diligencias.

Por el contrario, otras diligencias no fijen un límite temporal numeral[358]. La diligencia española sobre la captación de comunicaciones orales se limita a un encuentro concreto y no perdura en el tiempo: un nuevo encuentro necesitará una nueva autorización[359]. Sin embargo, se resalta, como ya se ha mencionado, que dicho concepto no se define, por lo cual su conformidad con el criterio de previsibilidad es cuestionable. Similarmente, la regulación de los registros informáticos no fija una duración a la diligencia, ya que no se supone que duren en el tiempo, sino que el acceso a los datos interviene en un periodo concreto y limitado[360].

---

investigación de los delitos en el sistema de las garantías procesales", *en* F. Bueno de Mata (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*, Comares, 2016, p. 268 ; F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, pp. 44–47. Por el contrario, en Francia, se puede modificar la duración de la medida para investigaciones contra delincuencia organizada. Sin embargo, dicha posición doctrinal es obviamente contraria a la jurisprudencia del TEDH

[352] Artículo 588 bis e.1 de la LECrim

[353] E. Gómez Soler, "La utilización de dispositivos técnicos de captación de la imagen de seguimiento y de localización", *op. cit.* nota 144, p. 124

[354] Artículos 588 ter g y 588 quinquies c de la LECrim

[355] Artículo 588 septies c de la LECrim

[356] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, pp. 510–512

[357] Artículos 100-2, 230-33, 230-48, 706-95-16 y 706-95 del Code de procédure pénale. Como excepción, como el *IMSI catcher* sirve para interceptar comunicaciones, dicho uso se limita a 48 horas, artículo 706-95-20.II

[358] Hay que precisar que no se requiere límite temporal cuando se requiere la cesión de datos. Sin embargo, se podría considerar la implementación de límites temporales máximos dentro de los cuales los operadores tienen que contestar

[359] Artículo 588 quater e de la LECrim

[360] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 384

Pero cuando se incautan los dispositivos, el acceso posterior a los datos podría incluir datos recibidos después del registro físico. Se cuestiona entonces la necesidad de establecer un límite temporal al acceso de los datos. También, la diligencia francesa de acceso a distancia a las correspondencias electrónicas no establece un límite de tiempo. Hay que recordar que no se trata de un registro: los policías obtienen códigos de acceso a un ciberespacio privado, al que técnicamente se puede acceder todos los días. Teniendo en cuenta que interfiere en el derecho a la intimidad, debería definirse un ámbito temporal. La diligencia del agente encubierto en Internet no fija un límite temporal en ninguno de los dos países[361], aunque la infiltración clásica explicita que la identidad supuesta se otorga por seis meses en España[362] y que se limite a cuatro meses en Francia[363]. En la LECrim, tampoco se considera límite temporal para la captación de imágenes en lugares o espacios públicos, lo que se podría justificar por la injerencia muy limitada a la vida privada.

También, el TEDH comprueba también si la ley ordena que la autorización de la diligencia fije su duración concreta[364]. Dicha duración debe incluirse explícitamente dentro de la autorización en el ámbito español[365]. Sin embargo, en Francia, esta precisión solamente se menciona explícitamente para la interceptación de las comunicaciones[366]. Una decisión de la Corte de Casación consideró que "*la duración por la que se autoriza la diligencia constituye una garantía esencial contra el riesgo de una violación desproporcionada del derecho a la privacidad*"[367]. Pero este criterio no aparece en ninguna otra decisión, por lo cual no se puede considerar que la jurisprudencia haga previsible este criterio.

[361] Lo que se critica en la doctrina española, F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, p. 122
[362] Artículo 282 bis.1 de la LECrim
[363] Artículo 706-83 del Code de procédure pénale
[364] TEDH, *Kruslin c. Francia*, *op. cit.* nota 8, ¶ 35
[365] Artículo 588 bis c.3.e de la LECrim, y en la solicitud, artículo 588 bis b.2.7°
[366] Artículos 100-1 y 706-95 del Code de procédure pénale. No hay precisión sobre este tema en los artículos 706-95-13 y 230-33 (incluso la circular sobre la geolocalización no lo considera, Ministère de la Justice, Circulaire du 1er avril 2014 de présentation de la loi n°2014-372 relative à la géolocalisation, Francia, el 28 de marzo de 2014.
[367] Cour de Cassation, Chambre criminelle, el 9 de enero de 2018, núm. 17-82946

En segundo lugar, en cuanto a la prórroga de la diligencia, la ley tiene que ser precisa en cuanto al límite temporal y las razones de la(s) prórroga(s)[368]. En España, la prórroga debe ser justificada tanto por el órgano solicitante como por el órgano autorizando la medida[369]. Además, todas las diligencias tienen una duración máxima, incluso después de las prórrogas, para las que fijan un límite temporal numeral[370]. En general[371], en Francia, las diligencias autorizadas en el marco de la investigación de flagrancia o preliminar solamente pueden renovarse una vez[372]; mientras que durante la instrucción, el código considera una duración total máxima[373]. El código suele considerar que la autorización de prórroga debe seguir las mismas condiciones de forma, sin dar más detalles. Se nota aquí que las prórrogas pueden llegar a una duración máxima de 18 meses[374] o de dos años[375], en ambos países, lo que la doctrina considera desproporcionado.

Hay que subrayar que el cómputo de los plazos supuso un problema de interpretación en España (pero no en Francia). Se cuestionó si el plazo de la diligencia comenzaba al día de su autorización o al día de su efectivo comienzo (después de la implementación de los

[368] TEDH, *Szabó y Vissy c. Hungría*, el 12 de enero de 2016, núm. 37138/14, ¶ 74

[369] Artículos 588 bis e.2 y 3 y 588 bis f de la LECrim. En particular, se deben valorar en función de los resultados obtenidos, J. Vegas Torres, "Las medidas de investigación tecnológica", *op. cit.* nota 10. El desarrollo de la investigación permite confirmar el principio de necesidad, los resultados, su idoneidad, y la gravedad del delito, su proporcionalidad, Fiscalía General del Estado, Circular 2/2019, *op. cit.* nota 65, p. 30108. En definitiva, se requiere "*motivación más reforzada*," F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, p. 79. La doctrina argumenta que la denegación de prórroga tendría que suponer el cese de la diligencia, ya que ya no concurren los principios justificantes de la injerencia a la vida privada, A. Rodríguez Álvarez, "Intervención de las comunicaciones telefónicas y telemáticas y smartphones", *op. cit.* nota 326, p. 171

[370] Véase los artículos 588 ter g, 588 quinquies c y 588 septies c de la LECrim. Se critica que las prórrogas en materia de interceptación de comunicaciones tengan que ser de igual duración, C. Sanchís Crespo, "Puesta al día de la instrucción penal", *op. cit.* nota 329, p. 7

[371] La geolocalización se limita a un año o a dos años en caso de investigación contra delincuencia organizada, artículo 230-33 del Code de procédure pénale; y el uso del *IMSI catcher* para interceptar comunicaciones sólo puede renovarse una vez, artículo 706-95-20.II

[372] Véase los artículos 230-33.1°, 706-95-16.1° y 706-95 del Code de procédure pénale

[373] Dos años para la captación de imágenes y sonidos, el *IMSI catcher* y la captación de datos informáticos, artículo 706-95-16 del Code de procédure pénale; un año o dos años en caso de investigación contra delincuencia organizada para la interceptación de comunicaciones, artículo 100-2

[374] E. Gómez Soler, "La utilización de dispositivos técnicos de captación de la imagen de seguimiento y de localización", *op. cit.* nota 144, p. 134 ; F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, p. 149

[375] F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, p. 61

dispositivos, por ejemplo). El Tribunal Constitucional[376] y el Tribunal Supremo[377] interpretaron la LECrim según la primera opción, con el fin de aportar seguridad jurídica[378]. Se critica dicha interpretación en particular en materia de registros remotos, cuando la instalación de los dispositivos tarda o cuando el investigado no ha activado los programas que permiten entrar en el sistema[379].

Por último, el órgano que dio la autorización debe poder cesarla en cualquier momento, especialmente si los motivos originales han desaparecido. La LECrim lo menciona explícitamente[380]. Por el contrario, el código francés no contempla explícitamente la posibilidad de poner fin a las diligencias antes de la finalización de la duración establecida en la autorización[381]. Por lo tanto, la regulación procesal penal francesa parece ser particularmente cuestionable con respecto a la jurisprudencia del TEDH sobre el alcance temporal de las diligencias tecnológicas.

Una vez que se haya estudiado los diferentes ámbitos que delimitan a las diligencias tecnológicas, para los cuales ya se han anotados elementos de no conformidad con la jurisprudencia del TEDH, se requiere valorar el procedimiento de control de dichas diligencias.

---

[376] Tribunal Constitucional, el 18 de julio de 2005, núm. 205/2005 ; I. López-Barajas Perea, "Garantías Constitucionales En La Investigación Tecnológica Del Delito", *op. cit.* nota 10, p. 111

[377] Tribunal Supremo. Sala Segunda, de lo Penal, el 22 de enero de 2014, núm. 7/2014 ; J. Vegas Torres, "Las medidas de investigación tecnológica", *op. cit.* nota 10

[378] Fiscalía General del Estado, Circular 2/2019, *op. cit.* nota 65, p. 30107. Para una opinión contraria, abogando por cómputos individualizados, véase, F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, pp. 79–80,

[379] L. Bachmaier Winter, "Registro remoto de equipos informáticos en la Ley Orgánica 13/2015", *op. cit.* nota 184

[380] Artículos 588 bis e.1 y 588 bis j de la LECrim. Entonces, "*tres serían las circunstancias que determinarán el cese de la medida […]: 1ª La desaparición de las circunstancias que justificaron su adopción […] 2ª La evidencia de que a través de la medida no se están obteniendo los resultados pretendidos […] 3ª El transcurso del plazo*", E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, pp. 458–459

[381] Salvo en el caso de la captación de imágenes y de sonidos, del *IMSI catcher* y de la captación de datos informáticos, el órgano autorizante puede cesar la diligencia en cualquier momento, pero el artículo no detalla por qué, artículo 706-95-14 del Code de procédure pénale; similarmente para el uso de drones, artículo 230-50

1. Procedimiento de la diligencia

La ley debe detallar las modalidades y los órganos que revisan las diligencias tecnológicas. Como subrayó el TEDH, la "*vigilancia puede sufrir un control en tres niveles: cuando se ordena, mientras es desarrollada y después cuando ella cesa*."[382] Por lo general, el tribunal se centra en el control inicial (A), y luego agrupa los controles que se desarrollan durante la implementación de la diligencia y posteriormente (B).

A. Control inicial

El control inicial de las diligencias tecnológicas supone una intervención antes de la implementación de la diligencia. Este tema se dividirá en dos partes: el órgano encargado del control y las modalidades del mismo (en particular, el alcance del control y el contenido de la autorización)[383].

En primer lugar, el TEDH "*estima en principio deseable que el control sea confiado a un juez en un campo donde los abusos son potencialmente propiciados en casos individuales y podrían entrañar consecuencias perjudiciales para la sociedad democrática en su conjunto*"[384]. Sin embargo, el TEDH destacó que, aunque es deseable, no es obligatorio[385]. El criterio más importante es la independencia del órgano de supervisión[386]. En Francia, los fiscales no se consideran autoridades judiciales, ya que no son independientes del poder ejecutivo[387]. En

[382] TEDH, *Klass y otros c. Alemania*, *op. cit.* nota 265, ¶ 55
[383] TEDH, *Roman Zakharov c. Rusia*, *op. cit.* nota 277, p. 257
[384] TEDH, *Klass y otros c. Alemania*, *op. cit.* nota 265, ¶ 56
[385] Aunque, se considera muy importante en la doctrina, véase P. Beauvais, "La nouvelle surveillance pénale", *en* J. Alix et al. (eds.), *Humanisme et justice: mélanges en l'honneur de Geneviève Giudicelli-Delage*, Dalloz, 2016, p. 273
[386] Por ejemplo, para un organismo de supervisión no judicial, véase TEDH, *Weber y Saravia c. Alemania*, *op. cit.* nota 280, ¶ 117. Por el contrario, el TEDH considera que un órgano de supervisión de carácter político viola el artículo 8, véase TEDH, *Szabó y Vissy c. Hungría*, *op. cit.* nota 368, ¶ 75–76.
[387] TEDH, *Moulin c. Francia*, el 23 de noviembre de 2010, núm. 37104/06, ¶ 59; En consecuencia, en lo que respecta a la geolocalización, la jurisprudencia de la Cour de Cassation evolucionó, para hacerse coherente con la exigencia del TEDH. En primer lugar, el tribunal aceptó la posibilidad de que un fiscal autorice dicha diligencia, Cour de Cassation, Chambre criminelle, el 22 de noviembre de 2011, núm. 11-84308. Dos años después, el tribunal ordena que la autorización sea emitida por un magistrado

España, los fiscales aún se encuentran en una "*situación de dependencia orgánica y estatutaria*"[388] frente al poder ejecutivo. Por lo cual, la mayoría de las diligencias tienen que ser autorizadas por un juez[389].

Sin embargo, todavía existen algunas dudas. En caso de emergencia, en Francia, los agentes de policía pueden colocar dispositivos de geolocalización[390]. Un procedimiento similar se contempla en el marco español[391]. Dentro del marco español, se dispensa de autorización en caso de urgencia para el registro de dispositivos informáticos[392]; también se considera interceptaciones de comunicaciones ordenadas por el Ejecutivo, en caso de urgencia, en materia de lucha contra bandas armadas o delitos de terrorismo[393]. Durante un periodo de tiempo muy breve y en caso de emergencia, estos procedimientos podrían considerarse proporcionados y necesarios para la prevención y persecución de delitos. Sin embargo, la doctrina española pone de relieve la ausencia de "*parámetros predeterminados para acotar la urgencia*", dado que se tiene que valorar *ex ante*, con independencia del éxito de la medida[394].

independiente, es decir, no por un fiscal, Cour de Cassation, Chambre criminelle, el 22 de octubre de 2013, *op. cit.* nota 175 ; Cour de Cassation, Chambre criminelle, el 22 de octubre de 2013, *op. cit.* nota 175

[388] F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, p. 30

[389] Juez de libertades y custodia o juez de instrucción en Francia; juez de instrucción en España

[390] Medida que debe ser confirmada por el juez en un plazo de 24 horas, artículo 230-35 del Code de procédure pénale. Hay que subrayar que si el agente de policía tiene que informar al magistrado inmediatamente, la ley no establece un plazo específico

[391] Artículo 588 quinquies b.4 de la LECrim. Dentro de las guías de la Fiscalía General del Estado, se considera que "*La urgencia existirá en aquellos casos en los que se disponga de un plazo de tiempo para la colocación del dispositivo que no permita acudir a la autoridad judicial para solicitar la autorización*", Fiscalía General del Estado, Circular 4/2019, *op. cit.* nota 140, p. 30154.

[392] Artículo 588 sexies c.4 de la LECrim. Se critica el plazo para que el juez resuelva sobre la diligencia implementada con urgencia, que es más largo que para la interceptación de comunicaciones y la geolocalización, E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 485

[393] Artículo 588 ter d.3 de la LECrim

[394] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, pp. 423–427. La urgencia se considera como un concepto jurídico indeterminado que contribuye a "*oscurecer los requisitos de superación del juicio de proporcionalidad*", E. Gómez Soler, "La utilización de dispositivos técnicos de captación de la imagen de seguimiento y de localización", *op. cit.* nota 144, p. 134. Otro concepto jurídico indeterminado regula la implementación con urgencia del registro de dispositivos informáticos: se requiere un "*interés constitucional legítimo*", I. López-Barajas Perea, "El derecho a la protección del entorno virtual y sus límites", *op. cit.* nota 28, pp. 142–143

Se critica ampliamente[395], considerando que el control inicial del juez es una de la "*decisiones más medulares*" de protección frente a la injerencia a los derechos fundamentales[396].

Otros procedimientos podrían enfrentarse a la censura del TEDH[397]: España no exige ninguna autorización para el uso del *IMSI catcher*[398] o la captación de imágenes en lugares públicos[399]; y, en Francia, la geolocalización está autorizado durante los primeros ocho días por el fiscal[400].

En segundo lugar, el órgano controla clásicamente los ámbitos material, personal y temporal. Como ya se ha mencionado, el contenido de las autorizaciones francesas está muy poco detallado en la ley[401]. En general, se limita a considerar que la motivación debe basarse en hechos jurídicos y materiales[402]. Por el contrario, en España[403], el contenido de la autorización, y por consiguiente del examen de la solicitud, debe ser más detallado. Por un

[395] M.E. Laro-González, "El dron al servicio de las diligencias de investigación", *op. cit.* nota 160, pp. 278–279 ; A. Rodríguez Álvarez, "Diligencia de registro de dispositivos y 'smartphones'", *en* F. Bueno de Mata (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*, Comares, 2016, p. 261

[396] C. Sanchís Crespo, "Puesta al día de la instrucción penal", *op. cit.* nota 329, p. 5. Se critica aún más que la jurisprudencia parece extender los supuestos de urgencia a otras diligencias tecnológicas, Tribunal Supremo. Sala Segunda, de lo Penal, el 20 de abril de 2016, *op. cit.* nota 148 ; E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 454

[397] Sin embargo, esta censura no es flagrante, ya que el TEDH suele considerar el marco jurídico en su conjunto teniendo en cuenta otras salvaguardias

[398] Artículo 588 ter l de la LECrim, el control sólo es posterior, cuando los investigadores solicitan una interceptación de las comunicaciones gracias a los datos obtenidos

[399] Aunque la jurisprudencia del TEDH ha indicado que también podía considerarse como una injerencia a la vida privada, TEDH, *P.G. y J.H. c. Reino Unido*, *op. cit.* nota 266 ; TEDH, *Peck c. Reino Unido*, *op. cit.* nota 271

[400] Artículo 230-33 del Code de procédure pénale

[401] Salvo para la interceptación de comunicaciones, ya que el artículo 100-1 del Code de procédure pénale desarrolla algunos de los elementos que deben incluirse; y para la captación de datos informáticos, artículo 706-102-3. Para una crítica sobre esto último, véase E. De Marco, "La captation des données", *op. cit.* nota 278, p. 103

[402] Artículos 230-33 y 706-95-13 del Code de procédure pénale. El código sólo menciona la necesidad de motivar la autorización sin hacer referencia a los hechos legales y materiales, artículo 706-95-1. Sin embargo, para la grabación de comunicaciones orales, la Cour de Cassation pidió autorizaciones más detalladas, Cour de Cassation, Chambre criminelle, el 6 de enero de 2015, núm. 14-85448 ; T. Meindl, "Articles 706-73 à 706-106", *op. cit.* nota 113, ¶ 59 ; P. Collet, "Le renforcement progressif des garanties applicables à deux mesures intrusives : la géolocalisation et la sonorisation", *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2021, p. 29. Por el contrario, Saint-Pau considera que sí se requieren los principios de necesidad y proporcionalidad, pero define el primero como la necesidad de que se dicte dentro de un procedimiento penal, lo que no se ajusta a las otras definiciones de este principio, J.-C. Saint-Pau, "Les investigations numériques et le droit au respect de la vie privée", *op. cit.* nota 267, p. 321

[403] Artículo 588 bis c de la LECrim

lado, la ley detalla el contenido específico del documento. Por otro lado, las autorizaciones deben basarse en los principios, ya mencionados, "*de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida*"[404]. Comparando los dos marcos jurídicos, el procedimiento español parece mucho más previsible y cualitativo.

Por último, en el ámbito del control inicial, el TEDH comprueba que el procedimiento incluye una autorización específica para la entrada en espacios cerrados, especialmente para instalar los dispositivos técnicos[405]. En España, la instalación de dispositivos de grabación de audio en espacios privados necesita una autorización explícita[406], pero no se considera similar concepto para la geolocalización y los registros remotos. Por el contrario, en Francia, la instalación y la desinstalación se consideran para cada técnica que necesita dichos procedimientos[407].

Una vez el control inicial efectuado, las diligencias tecnológicas no se implementan sin más controles posteriores, sino que suponen controles intermedios durante su implementación y después de su finalización.

B. Controles intermedios y finales

En cuanto al control posterior de las diligencias tecnológicas, el TEDH exige la regulación de tres elementos en la ley: "*las modalidades de control de la aplicación de las [diligencias], los eventuales mecanismos de notificación y los recursos previstos por el derecho nacional*"[408].

En primer lugar, hay que supervisar la implementación de la diligencia autorizada. Al igual que para la supervisión inicial, debe estudiarse quién y cómo se realiza la supervisión continua

[404] Artículo 588 bis a de la LECrim, a los cuales ya que añadir el principio de legalidad
[405] TEDH, *Vetter c. Francia*, *op. cit.* nota 8, ¶ 27
[406] Artículo 588 quater a de la LECrim
[407] Artículos 230-34, 706-96-1 y 706-102-5 del Code de procédure pénale
[408] TEDH, *Roman Zakharov c. Rusia*, *op. cit.* nota 277, ¶ 238 ; TEDH, *Centrum För Rättvisa c. Suecia (2)*, *op. cit.* nota 266, ¶ 249

y/o final. En España, el juez de instrucción fija la forma y la frecuencia a la cual los investigadores deben informarle, y dicho control interviene en todo caso al final de la medida[409]. En Francia, durante la instrucción, las disposiciones generales establecen que el juez de instrucción debe comprobar todos los datos obtenidos[410]; la investigación preliminar es controlada por el fiscal[411]. Además, para cada diligencia, el código subraya que el magistrado controla la medida[412].

En cuanto al cómo, uno de los medios para controlar la diligencia tecnológica que menciona particularmente el TEDH es dejar constancia de la misma[413]. En España, el registro de las operaciones se exige indirectamente para algunas de las diligencias[414], pero no para la identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes y los registros remotos[415]. Se considera de mayor relevancia el acceso por el juez a las grabaciones[416], y su entrega rápida para evitar "*las posibilidades de*

[409] Artículo 588 bis g de la LECrim; se detalla dicha disposición para la interceptación de las comunicaciones, artículo 588 ter f, y la captación de las comunicaciones orales, artículo 588 quater d. Dicho requisito ya se exigía en la jurisprudencia anterior a la reforma de 2015. El incumplimiento de los plazos no produce la nulidad de la diligencia "*siempre que el Juez de Instrucción haya tenido información y conocimiento del resultado de las intervenciones*", Fiscalía General del Estado, Circular 1/2019, *op. cit.* nota 297, p. 30079. Problemáticamente, se considera el control judicial de la diligencia de infiltración clásica, pero no explícitamente del control del agente encubierto en Internet, artículo 282 bis

[410] Artículo 81¶5 del Code de procédure pénale

[411] Artículo 75¶2 del Code de procédure pénale

[412] *IMSI catcher*, captación de comunicaciones orales, captación de datos informáticos, artículo 706-95-14¶1 del Code de procédure pénale; interceptación de comunicaciones, artículos 100¶1 y 706-95¶1; acceso a correspondencias electrónicas, artículo 706-95-3¶1; geolocalización, artículo 230-37; uso de drones, artículo 230-50; agente encubierto en Internet, artículo 230-46¶3. Sin embargo, esta última disposición no especifica quién controla la medida cuando sólo la autoriza el fiscal, lo que significa que podría no haber una revisión judicial previa ni continua

[413] TEDH, *Kennedy c. Reino Unido*, *op. cit.* nota 273, ¶ 165 ; TEDH, *Roman Zakharov c. Rusia*, *op. cit.* nota 277, ¶ 272

[414] Interceptación de comunicaciones, artículo 588 ter f de la LECrim, *in fine*; captación de comunicaciones orales, artículo 588 quater d, *in fine*; geolocalización, artículo 588 quinquies c, *in fine*. En cuanto al último concepto, la doctrina precisa que se debe entregar los soportes y las copias al finalizar la diligencia, y no las investigaciones al completo, E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 483

[415] El régimen jurídico de los registros en espacios privados también contempla la necesidad de dejar constancia de las operaciones, artículo 572 de la LECrim, pero no es explícito si se aplica a los registros informáticos. No se exige explícitamente para el agente encubierto en Internet

[416] Sin embargo, se critica que los agentes de policía hacen necesariamente una selección de lo grabado, sin que hubiera "*una diferenciación entre los agentes que escuchan y los que investigan, de modo que los primeros, encargados de seleccionar, escogieran el contenido delictivo de las comunicaciones sin estar mediatizados*", C. Sanchís Crespo, "Puesta al día de la instrucción penal", *op. cit.* nota 329, p. 7. En particular, la jurisprudencia ha indicado que no se requiere que el juez de instrucción oiga "*íntegramente las grabaciones*", J. Vegas Torres, "Las medidas de investigación tecnológica", *op. cit.* nota 10. Sin embargo, el contenido íntegro de las grabaciones siempre deberá

manipulación del material"[417]. En Francia, se solicita explícitamente para casi todas las diligencias[418]. Sin embargo, para las operaciones de acceso, copia a los datos almacenados u obtenidos, es solamente una posibilidad: las disposiciones no consideran el registro de las operaciones realizadas[419].

En segundo lugar, la notificación es un factor muy relevante, ya que "*si no se le informa de las medidas tomadas sin su conocimiento, el interesado no puede generalmente, en principio, constatar retrospectivamente la legalidad de la actuación*"[420]. En España, el secreto de las diligencias tecnológicas es automático y se considera explícitamente[421]. En general, se abandona al menos diez días antes del final de la investigación, para que las partes puedan tomar nota de las diligencias, de los documentos y soportes[422]. Específicamente para la interceptación de comunicaciones[423], el código prevé explícitamente la información de las partes en el procedimiento y la notificación a otras personas interesadas. Sin embargo, excepcionalmente, se denegará acceso a las grabaciones por las partes cuando "*sea imposible, exija un esfuerzo desproporcionado o puedan perjudicar futuras investigaciones*", lo que se critica por "*la vaguedad del precepto [y] la inexigencia de que el juez motive una decisión en este sentido*"[424]. Se considera que, aún no esté previsto explícitamente, dicho concepto se tendría que aplicar a la captación de comunicaciones orales[425], por lo que se

estar disponible, E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 458

[417] Fiscalía General del Estado, Circular 4/2019, *op. cit.* nota 140, p. 30144

[418] Interceptación de comunicaciones, artículos 100-4 y artículo 100-5 del Code de procédure pénale; geolocalización, artículos 230-38 y 230-39; registros, artículo 56; *IMSI catcher*, captación de comunicaciones orales, captación de datos informáticos, artículo 706-95-18; uso de drones, artículo 230-52

[419] Artículos 706-95-1 y 706-95-2 del Code de procédure pénale

[420] TEDH, *Klass y otros c. Alemania*, *op. cit.* nota 265, ¶ 57. El tribunal también reconoció la necesidad de aplazar la notificación hasta que no obstaculice la eficacia de la medida, *Ibid.* ¶ 58

[421] Artículo 588 bis d de la LECrim

[422] Artículo 302 de la LECrim

[423] Artículo 588 ter i de la LECrim

[424] A. Rodríguez Álvarez, "Intervención de las comunicaciones telefónicas y telemáticas y smartphones", *op. cit.* nota 326, p. 175

[425] M. Díaz Martínez, "La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos", *op. cit.* nota 123, p. 111 ; Fiscalía General del Estado, Circular 3/2019, *op. cit.* nota 116, p. 30134

subraya la no conformidad de la LECrim en este criterio[426]. En Francia, en general, los actos de la investigación son secretos[427]. Todas las operaciones mencionadas anteriormente se incluirán en el expediente, que estará abierto a la consulta de las partes una vez finalizada la investigación[428]. Por lo tanto, no hay ninguna disposición relativa a la notificación a terceros o a una notificación antes del final de la investigación.

En tercer lugar, los recursos que ofrece la ley contra las decisiones de autorización de las diligencias tecnológicas durante su implementación no suelen ser estudiados por el TEDH dentro de la conformidad al artículo 8. Es un tema estrechamente vinculado al artículo 13 del convenio europeo de derechos humanos sobre el derecho a un recurso efectivo. El tribunal se basa a veces en el estudio de este criterio derivado del artículo 8 para no comprobar la conformidad con el artículo 13[429]. Aunque no está incluido la jurisprudencia sobre el artículo 13 en el ámbito del estudio, hay que subrayar que todas las autorizaciones españolas[430] y la mayor parte de las autorizaciones francesas relativas a las diligencias tecnológicas no están abiertas a recurso[431]. Por lo tanto, los recursos solamente se desarrollarán después de la aplicación de la técnica, en relación con la notificación, si procede[432].

[426] Dicha falta es sorprendente considerando que dicho criterio se exigía por jurisprudencia antes de la reforma de 2015, Fiscalía General del Estado, Circular 2/2019, *op. cit.* nota 65, p. 30109
[427] Artículo 11 del Code de procédure pénale. Se fortalece el secreto de la geolocalización para proteger a la víctima, con un régimen específico para que la persona sospechosa pueda recurrir la decisión, artículos 230-40 y 230-41
[428] B. Bouloc, G. Stefani, G. Levasseur, *Procédure pénale*, *op. cit.* nota 18, ¶ 819–820
[429] TEDH, *Malone c. Reino Unido*, *op. cit.* nota 265, ¶ 91 ; TEDH, *Liberty y otros c. Reino Unido*, *op. cit.* nota 266, ¶ 73 ; TEDH, *Centrum För Rättvisa c. Suecia (2)*, *op. cit.* nota 266, ¶ 376
[430] Para poder recurrir, la ley tiene que preverlo explícitamente, artículo 217 de la LECrim, lo que la ley no prevé para las diligencias tecnológicas
[431] Interceptación de comunicaciones, artículo 100¶2 del Code de procédure pénale; geolocalización, artículo 230-33¶3; *IMSI catcher*, captación de comunicaciones orales, captación de datos informáticos, artículo 706-95-13; uso de drones, artículo 230-49¶2. Por el contrario, las decisiones de acceso a los datos almacenados se consideran jurisdiccionales, por lo que el fiscal podría recurrirlas, artículos 706-95-1 a 706-95-3 y artículo 185
[432] Lo cual es criticado por la doctrina, véase M. Touillier, “Les droits de la défense dans les procédures d’exception : une évolution « vent dessus, vent dedans »”, *Actualité juridique Pénal*, Dalloz, 2016, p. 119; y el artículo 170 del Code de procédure pénale

Ya se ha subrayado varias potenciales o claras faltas de conformidad con los criterios de la jurisprudencia del TEDH en ambos países. A los criterios relativos al alcance de la diligencia y a su control, hay que añadir la protección de los datos obtenidos.

2. Protección de los datos obtenidos

Por último, el TEDH establece varios criterios relativos a la protección de los datos personales obtenidos. En primer lugar, significa que el Estado debe contar con una ley que detalle el "*procedimiento que debe seguirse para examinar, utilizar y almacenar los datos obtenidos*"[433], en general, una ley que trata de la protección de los datos personales en el marco de las funciones de las autoridades policiales y judiciales[434]. Dentro de la Unión Europea, los Estados tenían que transponer la directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. La directiva ha sido transpuesta a tiempo por Francia[435]. Por el contrario, España fue condenada por el TJUE por la no transposición de la directiva[436], y adoptó unos meses después su transposición [437].

En segundo lugar, la ley debe especificar el contenido del tratamiento de datos. El tribunal considera que estos criterios están estrechamente relacionados con la obligación de conservar los registros de las operaciones[438].

---

[433] TEDH, *Roman Zakharov c. Rusia*, *op. cit.* nota 277, ¶ 231
[434] TEDH, *Liberty y otros c. Reino Unido*, *op. cit.* nota 266, ¶ 69 ; TEDH, *Centrum För Rättvisa c. Suecia (2)*, *op. cit.* nota 266, ¶ 312
[435] Artículos 87 a 114, de la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, después de su reforma por la Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles
[436] TJUE, *European Commission c. Kingdom of Spain*, el 25 de febrero de 2021, C-658/19
[437] 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
[438] TEDH, *Centrum För Rättvisa c. Suecia (2)*, *op. cit.* nota 266, ¶ 310–311, see *supra*, 0

El primer criterio es la calidad de los datos, que debe ser comprobada y su almacenamiento debe ser seguro. La ley francesa considera ambos[439], así como la regulación española[440].

El segundo criterio tiene en cuenta la utilización o selección de los datos, especialmente para fines distintos de los definidos en la autorización. Por lo tanto, la ley debe detallar "*las precauciones que deben tomarse al comunicar los datos a otras partes*,"[441] lo que se considera en ambas legislaciones[442]. El principio general es que "*las informaciones y los documentos obtenidos […] no pueden servir a otros fines*"[443]. Por lo tanto, los datos no pertinentes deben ser destruidos, y los datos no deben ser utilizados en otro procedimiento. La LECrim no contempla la supresión de los datos no relevantes. La regulación española acepta el uso de los datos en otro procedimiento (siempre que sea legítima la injerencia), y la continuación de la diligencia para la investigación del delito descubierto bajo autorización judicial[444]. Estos hallazgos casuales no se regulan específicamente para las diligencias tecnológicas, sino que se remiten a un concepto en materia de apertura de la correspondencia escrita y telegráfica, por lo cual se critica la falta de regulación adaptada. En particular, la ley no considera el descubrimiento de un delito por el que no forme parte del ámbito material de la diligencia y el uso de dicha información en este otro procedimiento[445]. Aunque el código francés[446] no

[439] Artículos 4.4° y 6°, 97 y 99 de la Loi n°78-17
[440] Artículos 10 y 37 de la Ley Orgánica 7/2021
[441] TEDH, *Roman Zakharov c. Rusia*, *op. cit.* nota 277, ¶ 231
[442] Artículo 91 de la Loi n°78-17, aunque el artículo se limita a la transferencia de datos para otros fines, y no, por ejemplo, a otras autoridades policiales con el mismo fin general de reprimir delitos; artículo 11 de la Ley Orgánica 15/1999 de manera muy amplia. A este respecto, cabe señalar que la regulación de las transferencias internas es mucho más sencilla que para las transferencias internacionales. El TEDH también considera el intercambio de datos con otros países, TEDH, *Centrum För Rättvisa c. Suecia (2)*, *op. cit.* nota 266, ¶ 318
[443] TEDH, *Klass y otros c. Alemania*, *op. cit.* nota 265, ¶ 52
[444] Artículos 588 bis i y 579 bis de la LECrim. La extensión de la regulación de los hallazgos casuales a las diligencias tecnológicas proviene de la jurisprudencia anterior, M. Díaz Martínez, "La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos", *op. cit.* nota 123, p. 108. Bueno de Mata distingue los hallazgos casuales conectados con la prueba matriz, para los cuales se requiere una extensión de la autorización en función del principio de necesidad; y los que no tienen relación con dicha prueba, que necesitan la apertura de un proceso paralelo dentro de un contexto de flagrancia, "*que permitiría a la policía judicial recabar la prueba sin una autorización judicial previa*", F. Bueno de Mata, *Las Diligencias de investigación penal en la cuarta revolución industrial*, *op. cit.* nota 67, pp. 32–34
[445] M. Cedeño Hernán, "Las medidas de investigación tecnológica", *op. cit.* nota 13
[446] Existen disposiciones específicas cuando los datos se transmiten a través de la PNIJ, véase los artículos R40-42 a R40-56 del Code de procédure pénale

contempla la supresión de datos no relevantes, los datos conservados en el expediente ("*procès-verbal*") deben ser aquellos "*útiles para la demostración de la verdad*"[447]. Entonces, se supone que es una selección de datos relevantes. Del mismo modo, el código francés no regula la utilización de los datos obtenidos en otro procedimiento, y solamente precisa, para determinadas diligencias, que el descubrimiento de otros delitos no anula la diligencia[448].

Por último, el criterio que parece más importante para el TEDH es la regulación de "*las circunstancias en que las grabaciones pueden o deben ser borradas o destruidas*"[449], precisamente, "*a partir del momento en el cual no representen utilidad para el fin buscado*"[450]. En España, la destrucción de los datos originales[451] es obligatoria después del término del procedimiento (por orden del tribunal), y, para las copias[452], cinco años[453] "*desde que la pena se haya ejecutado*[454] *o cuando el delito o la pena hayan prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado*"[455]. Sin embargo, las copias se pueden conservar, a juicio del tribunal, sin que la regulación

[447] Interceptación de comunicaciones, artículo 100-5 del Code de procédure pénale; geolocalización, artículo 230-39; uso de drones, artículo 230-52; *IMSI catcher*, captación de comunicaciones orales, captación de datos informáticos, artículo 706-95-18, que precisa que "*En el expediente del procedimiento no podrán conservarse imágenes relativas a la vida privada distintas de las infracciones contempladas en los autos que autorizan la medida*" (dicha disposición podría haberse ampliado a todas las diligencias tecnológicas). No se contempla ninguna disposición similar para el acceso a las correspondencias electrónicas

[448] Geolocalización, artículo 230-37 del Code de procédure pénale; *IMSI catcher*, captación de comunicaciones orales, captación de datos informáticos, artículo 706-95-14; acceso a las correspondencias electrónicas, artículo 706-95-3. Sin embargo, "*Las operaciones no pueden, bajo pena de nulidad, tener otra finalidad que la de investigar y constatar los delitos a los que se refieren las decisiones del magistrado*", acceso a las correspondencias electrónicas (artículo 706-95-3), *IMSI catcher*, captación de comunicaciones orales, captación de datos informáticos (artículo 706-95-14). La falta de coherencia del código en este tema es especialmente flagrante

[449] TEDH, *Roman Zakharov c. Rusia*, *op. cit.* nota 277, ¶ 231

[450] TEDH, *Klass y otros c. Alemania*, *op. cit.* nota 265, ¶ 52

[451] Se critica que dicho concepto no sea ampliado a los datos obtenidos durante un procedimiento implementado con urgencia de forma indebida, E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 550

[452] Dicha diferencia para los datos digitales es importante en cuanto a los metadatos, C. Sanchís Crespo, "Puesta al día de la instrucción penal", *op. cit.* nota 329, pp. 7–8

[453] Se critica la larga duración prevista en relación con la duración de los elementos mencionados, E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* nota 28, p. 368

[454] Se cuestiona saber si se refiere al cumplimiento de la condena o desde el inicio de la ejecución. Además, no se considera el fin del cumplimiento de la condena por muerte del condenado o la concesión del indulto, A. Rodríguez Álvarez, "Intervención de las comunicaciones telefónicas y telemáticas y smartphones", *op. cit.* nota 326, p. 179

[455] Artículo 588 bis k.2 de la LECrim

precise ningún límite temporal en este caso ni los motivos de dicha decisión[456]. En Francia, la destrucción de los datos debe ser exigida por el fiscal, al término de la prescripción de la acción pública[457]. Sin embargo, no existe ninguna disposición al respecto para el acceso a las correspondencias electrónicas en Francia, ni para los datos recabados por los agentes encubiertos en Internet en ambos países[458].

[456] Artículo 588 bis k.2 de la LECrim *in fine*. "*Una posibilidad sería, por ejemplo, la proximidad cierta o muy probable de otra investigación por hechos relacionados o la existencia de un proceso pendiente con esas características*", C. Sanchís Crespo, "Puesta al día de la instrucción penal", *op. cit.* nota 329, pp. 7–8

[457] Interceptación de comunicaciones, artículo 100-6 del Code de procédure pénale; geolocalización, artículo 230-43; uso de drones, artículo 230-53; *IMSI catcher*, captación de comunicaciones orales, captación de datos informáticos, artículo 706-95-19. Se ha criticado que la destrucción no depende del resultado del procedimiento, C. Guerrier, "« Loppsi 2 » et l'utilisation des nouvelles technologies", *op. cit.* nota 343

[458] No obstante, en general, el interesado puede solicitar la destrucción de los datos basándose en el artículo 23 de la Ley Orgánica 7/2021 y el artículo 106.I.4° de la Loi n°78-17

IV. CONCLUSIONES

Las diligencias tecnológicas pertenecen a los poderes más soberanos de ambos Estados y permiten definir, dentro de su territorio, el alcance de las medidas intrusivas para la investigación de delitos. Por lo tanto, su regulación es una competencia, principalmente, estatal. No se armoniza a nivel supranacional, y si se da el caso, es mínimo y para facilitar la cooperación internacional. Sin embargo, a pesar de dicha autonomía de los Estados, este estudio comparado permite subrayar una similitud muy fuerte entre las diligencias tecnológicas disponibles en España y Francia. Las mismas diligencias son reguladas, aunque, a veces, con un nombre o alcance diferente. Se regulan los registros informáticos (presenciales y a distancia), la interceptación de comunicaciones, la captación de comunicaciones orales y de imágenes, la cesión de datos por los operadores de servicios[459], el acceso a metadatos a través de dispositivos técnicos[460], la geolocalización, los registros remotos sin conocimiento de las personas interesadas[461], y la ciber infiltración (o agente encubierto por Internet). Además, la regulación española regula de manera específica la captación de imágenes en lugares públicos; en Francia, se introdujo en enero 2022 un concepto específico para el uso de drones, o generalmente la captación de imágenes en lugares públicos mediante dispositivos aéreos. Dicha similitud puede justificarse por la regulación tardía de las diligencias tecnológicas, que siempre se acopla a las tecnologías disponibles en vez de prever más allá.

La regulación española desarrolla casi todas las diligencias tecnológicas en una parte específica de la LECrim (salvo la ciber infiltración), facilitando su lectura y coherencia. Por el contrario, la regulación francesa sobre diligencias tecnológicas se encuentra desbaratada en numerosas partes del código de enjuiciamiento criminal, resultando en regímenes muy diferentes y cuya lectura y comprensión es dificultosa.

[459] Explícitamente, en España, para la identificación de usuarios y dispositivos
[460] Y, en Francia, la interceptación de comunicaciones a través de dichos dispositivos
[461] Aunque en Francia se divide en dos conceptos: el acceso a distancia a las correspondencias electrónicas, y la captación de datos informáticos

Hay que notar que la implementación efectiva de las diligencias supone, además de su legalidad, la disponibilidad de los dispositivos necesarios, la formación adecuada de las autoridades policiales y judiciales, y tomar en cuenta de sus costes. Aunque queda fuera del ámbito de este estudio, la eficacia de la investigación penal no se limita a consideraciones jurídicas.

Al enfrentar los regímenes de dichas diligencias tecnológicas a la jurisprudencia del TEDH en materia de protección de la vida privada, se considera que las regulaciones se acoplan de manera general a los criterios establecidos. Sin embargo, al entrar en detalle en los regímenes, se pueden subrayar numerosas faltas o disconformidades que cuestionan la validez de ambos sistemas jurídicos frente al marco supranacional.

En cuanto al alcance de las diligencias, son pocas las que fijan un ámbito personal estrictamente delimitado. Por un lado, la legislación española considera de manera general la posible afectación a terceros, exigiendo una motivación reforzada. Dicho concepto sería de ideal adopción en Francia. Por otro lado, la regulación francesa desarrolla ampliamente la captación de los datos conexos a personas especialmente protegidas o sometidas a secretos profesionales, lo que no se recoge de manera armonizada en España: se limita a determinadas diligencias (registros domiciliarios, principalmente) y a categorías de personas muy limitadas (abogados, principalmente). Sin embargo, dicho criterio se enfrenta a la evolución de la tecnología y carece de sentido para la implementación de determinadas diligencias o es en la práctica imposible de averiguar antes de dicha implementación.

Los ámbitos materiales de las diligencias son muy similares en ambos países, fijando un umbral general y muy amplio de delitos penados por tres años de prisión como mínimo. Se puede criticar este criterio general por no adaptarse al nivel de injerencia a cada diligencia. De manera general, las diligencias tecnológicas españolas disponen de un ámbito material más amplio que en Francia. En particular, varias de ellas se limitan a determinados delitos listados como de especial gravedad por su comisión de manera organizada, como al acceso a metadatos por *IMSI catcher*, la captación de sonidos e imágenes en lugares privados y los

registros remotos sobre dispositivos informáticos. Sin embargo, determinadas diligencias no fijan un ámbito material, cuestionando su conformidad con el convenio europeo de derechos humanos, como la geolocalización o el acceso a metadatos en España. Además, cuando se fija un ámbito material mediante términos generales, dicha conformidad se plantea también por falta de definición precisa de dichos términos (en particular, la noción de delincuencia organizada en Francia y de delitos cometidos en el entorno digital en ambos países).

En cuanto al ámbito temporal, la gran mayoría de las diligencias fijan límites precisos. Sin embargo, en particular en Francia, dichos límites son armonizados, en vez de adaptarse al nivel de injerencia de cada diligencia[462]. Sin embargo, en España, se cuestiona la conformidad del ámbito temporal de las captaciones de comunicaciones orales, ya que no se fija límite numeral, sino que se delimitan a encuentros específicos, cuya implementación en la práctica puede resultar compleja. Otras diligencias no fijan un ámbito temporal, dado que se consideran como limitadas en el tiempo por naturaleza, como los registros o el acceso a distancia y sin conocimiento de la persona interesada a sus correspondencias electrónicas. Sin embargo, el entorno digital es dinámico y podría plantearse la cuestión del ámbito temporal en relación con dispositivos incautados o accesos multiplicados a dichas correspondencias. Además, la LECrim prevé la necesaria fijación de la duración de la medida en la autorización judicial de la diligencia, mientras en Francia solamente se considera en materia de interceptación de comunicaciones. En cuanto a las prórrogas, sus duraciones se consideran desproporcionadas por la doctrina. En cuanto al cesa de la medida, la legislación francesa no considera la posibilidad de poner fin a las diligencias en cualquier momento.

El control de las diligencias tecnológicas mediante una autorización inicial se conforma mayoritariamente a los criterios del TEDH. Sin embargo, cabe mencionar que el fiscal aún tiene un papel importante en Francia como órgano autorizante, aunque no se considera como un juez independiente. En España, algunas diligencias, como el uso del *IMSI catcher* o la captación de imágenes en lugares públicos, no requieren autorización, aunque pueden

[462] Similar comentario puede hacerse en cuanto a las prórrogas

suponer una injerencia en la vida privada. Además, la ausencia de control inicial en situación de urgencia plantea cuestiones de conformidad frente a la falta de delimitación de dicho concepto. También, este control parece más detallado en España, ya que se basa en principios rectores y que la ley desarrolla ampliamente el contenido de la autorización. Por el contrario, la legislación española regula de manera incompleta autorizaciones específicas para la entrada en lugares privados para la instalación de dispositivos técnicos[463]. En cuanto a los controles posteriores, ambas legislaciones prevén controles intermediarios y controles por el órgano autorizante, así como la constancia de las operaciones en el expediente[464]. Por el contrario, la regulación de la notificación a las partes o personas interesadas es muy incompleta, limitada a determinadas diligencias. Se debe entonces acudir a las reglas generales sobre el secreto de la investigación, que no se acopla específicamente a las injerencias que resultan de las diligencias tecnológicas.

Por fin, la protección de los datos obtenidos se lleva a cabo mayoritariamente a través de la transposición de la directiva 680/2016, mediante exigencias de calidad de los datos y de seguridad de su conversación. Además, el uso de los datos obtenidos debe limitarse al ámbito material delimitado en la autorización: ambas legislaciones de protección de datos personales detallan y limitan las posibles transferencias de los datos a otras partes. Estos datos incluso deben limitarse a los pertinentes. La LECrim no considera la limitación de los datos obtenidos por la implementación de las diligencias tecnológicas, mientras que el régimen francés lo hace de manera limitada, sin fijar criterios precisos. También, la LECrim desarrolla la regulación de los hallazgos casuales, lo que no hace la regulación francesa. Finalmente, las leyes consideran la destrucción de los datos y copias[465], aunque se puede seguir conservando bajo criterios imprecisos en España.

La regulación de las diligencias tecnológicas nunca será definitiva: se acopla a la evolución de las técnicas y tendrá que conformarse con la jurisprudencia del TEDH que se desarrolla

[463] En materia de geolocalización y de registros remotos
[464] Salvo, en Francia, para las operaciones de acceso y copia a los datos almacenados u obtenidos
[465] Salvo para los datos recabados por los agentes encubiertos en Internet, ni para el acceso a distancia a las correspondencias electrónicas en Francia

cada vez más. Es necesario que el legislador amplíe las medidas a la disposición de las autoridades policiales y judiciales con el fin de mejorar la detección e investigación de delitos. Sin embargo, tanto en España como en Francia, la regulación principalmente responde a subsanar las lagunas mencionadas por los profesionales y la doctrina. Eso limita la eficacia de su implementación, ya que pocas veces se considera potenciales evoluciones futuras. Además, dichas regulaciones no toman en cuenta todas las exigencias del marco supranacional de la protección de derechos fundamentales. Aunque los regímenes de las diligencias tecnológicas se conforman en su globalidad a los criterios del TEDH, se puede llegar a cuestionar la conformidad de numerosos elementos y detalles de cada diligencia. A la hora de reformar las leyes de enjuiciamiento criminal en materia de diligencias tecnológicas, los legisladores podrían entonces ayudarse del derecho comparado con el fin de examinar las buenas prácticas desarrolladas en otros países, especialmente con los que existe amplia cooperación policial y judicial. También les ayudarían a estudiar en profundidad los criterios fijados por el TEDH, que son de suma importancia para determinar un régimen coherente en la regulación de las diligencias tecnológicas, a la vez unitario y adaptado a los niveles de injerencia al derecho a la vida privada.

V. BIBLIOGRAFÍA

1. Libros y manuales

BOULOC B., STEFANI G., LEVASSEUR G., *Procédure pénale*, Dalloz, Précis, 27a ed., 2020.
BUENO DE MATA F., *Las Diligencias de investigación penal en la cuarta revolución industrial: principios teóricos y problemas prácticos*, Thomson Reuters Aranzadi, Aranzadi derecho penal núm. 1151, Primera edición, 2019, 2019.
OTAMENDI ZOZAYA F., *Las últimas reformas de la ley de enjuiciamento criminal una visión práctica tras un año de vigencia*, Dykinson, 2017.
VELASCO NÚÑEZ E., SANCHÍS CRESPO C., *Delincuencia informática: tipos delictivos e investigación: con jurisprudencia tras la reforma procesal y penal de 2015*, Tirant lo Blanch, 2019.
ZAFRA ESPINOSA DE LOS MONTEROS R., *El policía infiltrado: los presupuestos jurídicos en el proceso penal español*, Tirant lo Blanch, 2010.
MELÓN MUÑOZ A. (ed.), *Procesal penal 2021*, Francis Lefebvre, Memento práctico, 2020.

A. Capítulos de libros

ALBA CLADERA F., GARCÍA MARTÍNEZ G., "Blanqueo de capitales y agente encubierto en internet", *en* BUENO DE MATA F. (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*, Comares, 2016, pp. 191–201.
ALEJANDRA SUÁREZ M., "Diligencias de investigación tecnológicas. La licitud de la actividad probatoria de un dron", *en* BUENO DE LA MATA F., GONZÁLEZ PULIDO I., BUJOSA VADELL L.M. (eds.), *Fodertics 9.0: Estudios sobre tecnologías disruptivas y justicia*, Comares, 2021, pp. 393–403.
BACHMAIER WINTER L., "Registro remoto de equipos informáticos en la Ley Orgánica 13/2015: algunas cuestiones sobre el principio de proporcionalidad", *en* CEDEÑO HERNÁN M. (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1a ed., 2017.
BEAUVAIS P., "La nouvelle surveillance pénale", *en* ALIX J. et al. (eds.), *Humanisme et justice: mélanges en l'honneur de Geneviève Giudicelli-Delage*, Dalloz, 2016, pp. 259–274.
BENSOUSSAN A., LEPAGE A., QUEMENER M., "Loyauté de la preuve et nouvelles technologies : entre exigences processuelles et efficacité répressive", *Les transformations de la justice pénale: cycle de conférences 2013 à la Cour de cassation*, 2014.
BRIGANT J.-M., "Mesures d'investigation face au défi numérique en droit français", *en* FRANSSEN V., FLORE D., STASIAK F. (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019.
BUENO DE MATA F., "Peculiaridades probatorias del DRON como diligencia de investigación tecnológica", *en* BUENO DE LA MATA F., DÍAZ MARTÍNEZ M., LÓPEZ-BARAJAS PEREA I. (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, pp. 169–204.
BUENO DE MATA F., "El agente encubierto en Internet como instrumento para la lucha contra el 'child grooming' y el 'sexting'", *en* BUENO DE MATA F. et al. (eds.), *Cambio de paradigma en la prevención y erradicación de la violencia de género*, Editorial Comares, Estudios de Derecho constitucional, 2017, pp. 3–16.
CEDEÑO HERNÁN M., "Las medidas de investigación tecnológica. Especial consideración de la captación y grabación de conversaciones orales mediante dispositivos electrónicos", *en* CEDEÑO HERNÁN M. (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1a ed., 2017.
DE JORGE PÉREZ C., "El escondite virtual y el nuevo agente encubierto", *en* BUENO DE MATA F. (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*, Comares, 2016, pp. 245–253.
DE LA CUESTA J.L., "Organised Crime Control Policies in Spain: A 'Disorganised' Criminal Policy for 'Organised' Crime", *en* FIJNAUT C., PAOLI L. (eds.), *Organised crime in Europe: concepts, patterns and control policies in the European Union and beyond*, Springer, Studies of organized crime núm. 4, 1a ed., 2006, p. 795.
DE MARCO E., "La captation des données", *en* BLAY-GRABARCZYK K. et al. (eds.), *Le nouveau cadre législatif de la lutte contre le terrorisme à l'épreuve des droits fondamentaux*, Institut Universitaire Varenne, Collection "Colloques & Essais" núm. 44, 2017, p. 88.
DÍAZ MARTÍNEZ M., "La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos", *en* BUENO DE LA MATA F., DÍAZ MARTÍNEZ M., LÓPEZ-BARAJAS PEREA I. (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, pp. 85–112.

DONOSO ABARCA L., “Legitimidad de los sistemas de videovigilancia activa como medida de investigación tecnológica”, *en* BUENO DE MATA F., GONZÁLEZ PULIDO I., BUJOSA VADELL L. (eds.), *Fodertics 8.0: estudios sobre tecnologías disruptivas y justicia*, Comares, 2020, pp. 245–257.
DURÁN BERNARDINO M., “El método comparado en los trabajos de investigación”, *en* MARCHAL ESCALONA N., MUÑOZ GONZÁLEZ M.C., MUÑOZ GONZÁLEZ S. (eds.), *El Derecho Comparado en la Docencia y la Investigación*, Dykinson, S.L., 2017, p. 48.
FRÍGOLS I BRINES E., “La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías”, *en* BOIX REIG J., JAREÑO LEAL Á. (eds.), *La protección jurídica de la intimidad*, Iustel, 2010, pp. 37–92.
GODEFROY T., “The Control of Organised Crime in France: A Fuzzy Concept but a Handy Reference”, *en* FIJNAUT C., PAOLI L. (eds.), *Organised crime in Europe: concepts, patterns and control policies in the European Union and beyond*, Springer, Studies of organized crime núm. 4, 1a ed., 2006, p. 763.
GÓMEZ SOLER E., “La utilización de dispositivos técnicos de captación de la imagen de seguimiento y de localización. Cuando la práctica forense no puede esperar”, *en* BUENO DE LA MATA F., DÍAZ MARTÍNEZ M., LÓPEZ-BARAJAS PEREA I. (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, pp. 113–134.
JUANATEY DORADO C., DOVAL PAIS A., “Límites de la protección penal de la intimidad frente a la grabación de conversaciones o imágenes”, *en* BOIX REIG J., JAREÑO LEAL Á. (eds.), *La protección jurídica de la intimidad*, Iustel, 2010, pp. 127–170.
LARO-GONZÁLEZ M.E., “El dron al servicio de las diligencias de investigación”, *en* BUENO DE MATA F., GONZÁLEZ PULIDO I., BUJOSA VADELL L. (eds.), *Fodertics 8.0: estudios sobre tecnologías disruptivas y justicia*, Comares, 2020, pp. 273–284.
LAZERGES C., “Dédoublement de la procédure pénale et garantie des droits fondamentaux”, *en* BOULOC B., ALT-MAES F. (eds.), *Les droits et le droit: mélanges dédiés à Bernard Bouloc*, Dalloz, 2007, pp. 573–590.
LÓPEZ ORTEGA J.J., “La utilización de medios técnicos de observación y vigilancia en el proceso penal”, *en* BOIX REIG J., JAREÑO LEAL Á. (eds.), *La protección jurídica de la intimidad*, Iustel, 2010, pp. 261–334.
LÓPEZ-BARAJAS PEREA I., “El derecho a la protección del entorno virtual y sus límites. El registro de los sistemas informáticos”, *en* BUENO DE LA MATA F., DÍAZ MARTÍNEZ M., LÓPEZ-BARAJAS PEREA I. (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, pp. 135–168.
MARGUENAUD J.-P., “La réécriture du droit criminel français sous la dictée de la cour européenne des droits de l’homme”, *en* ALIX J. et al. (eds.), *Humanisme et justice: mélanges en l’honneur de Geneviève Giudicelli-Delage*, Dalloz, 2016, pp. 923–938.
MARTÍN SAGRADO O., “La necesaria delimitación del ámbito subjetivo y de la duración de la captación de comunicaciones orales”, *en* FUENTES SORIANO O., ARRABAL PLATERO P., ALCARAZ RAMOS M. (eds.), *Era digital, sociedad y derecho*, Tirant lo Blanch, Monografías, 2020, pp. 507–516.
MARTÍNEZ SANTOS A., “Las grabaciones obtenidas a través de sistemas de videovigilancia en el proceso penal: derechos fundamentales afectados y tipología de supuestos”, *en* CEDEÑO HERNÁN M. (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1a ed., 2017.
NEUPAVERT ALZOLA M., “Crítica a los presupuestos de adopción de diligencias de investigación tecnológica”, *en* BUENO DE LA MATA F., GONZÁLEZ PULIDO I., BUJOSA VADELL L.M. (eds.), *Fodertics 9.0: Estudios sobre tecnologías disruptivas y justicia*, Comares, 2021, pp. 361–370.
PÉREZ ZÚÑIGA J.M., “La importancia del método comparado en la investigación y la docencia”, *en* MARCHAL ESCALONA N., MUÑOZ GONZÁLEZ M.C., MUÑOZ GONZÁLEZ S. (eds.), *El Derecho Comparado en la Docencia y la Investigación*, Dykinson, S.L., 2017, p. 56.
RIZO GÓMEZ B., “La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la 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”, *en* ASENCIO MELLADO J.M., FERNÁNDEZ LÓPEZ M. (eds.), *Justicia penal y nuevas formas de delincuencia*, Tirant lo Blanch, Monografías, 1a ed., 2017, pp. 97–123.
RODRÍGUEZ ÁLVAREZ A., “Intervención de las comunicaciones telefónicas y telemáticas y smartphones. Un primer estudio a propósito de la ley orgánica 13/2015, de 5 de octubre, de modificación de la ley de enjuiciamiento criminal”, *en* ASENCIO MELLADO J.M., FERNÁNDEZ LÓPEZ M. (eds.), *Justicia penal y nuevas formas de delincuencia*, Tirant lo Blanch, Monografías, 1a ed., 2017, pp. 149–182.
RODRÍGUEZ ÁLVAREZ A., “Diligencia de registro de dispositivos y ‘smartphones’”, *en* BUENO DE MATA F. (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*, Comares, 2016, pp. 255–263.

SAN MIGUEL CASO C., “Los nuevos medios de investigación de los delitos en el sistema de las garantías procesales”, *en* BUENO DE MATA F. (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*, Comares, 2016, pp. 265–274.
SERRA CRISTÓBAL R., “La vigilancia de datos y de comunicaciones digitales en la lucha por la seguridad nacional: especial referencia a las previsiones legislativa de España”, *en* FLORES GIMÉNEZ F., RAMÓN CHORNET C. (eds.), *Análisis de los riesgos y amenazas para la seguridad*, Tirant lo Blanch, Derechos humanos, 1a ed., 2017, pp. 105–136.
VALIÑO CES A., “El agente encubierto informático y la ciberdelincuencia. El intercambio de archivos ilícitos para la lucha contra los delitos de pornografía infantil”, *en* BUENO DE MATA F. (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*, Comares, 2016, pp. 275–285.
VALLÉS CAUSADA L., “Utilidad de los datos conservados de las comunicaciones electrónicas para la resolución de emergencias”, *en* BUENO DE LA MATA F., DÍAZ MARTÍNEZ M., LÓPEZ-BARAJAS PEREA I. (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, pp. 49–84.
VEGAS TORRES J., “Las medidas de investigación tecnológica”, *en* CEDEÑO HERNÁN M. (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1a ed., 2017.
VILLAMARÍN LÓPEZ M.L., “La nueva figura del agente encubierto online en la lucha contra la pornografía infantil. Apuntes desde la experiencia en Derecho Comparado”, *en* CEDEÑO HERNÁN M. (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1a ed., 2017.

2. Tesis

BOOS R., *La lutte contre la cybercriminalité au regard de l’action des États*, Tesis doctoral, Université de Lorraine, 2016.
ROUSSEL B., *Les investigations numériques en procédure pénale*, Tesis doctoral, Université de Bordeaux, Université de Bordeaux, el 7 de julio de 2020.

3. Artículos

AGUSTINA J.R., “Sobre la utilización oculta de GPS en investigaciones criminales y detección de fraudes laborales: análisis jurisprudencial comparado en relación con el derecho a la intimidad”, *La ley penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, 2013, núm. 102, p. 2.
ASSOCIATION INTERNATIONALE DE DROIT PENAL, “XV^{ème} congrès international de droit pénal (Rio de Janeiro, 4 – 10 septembre 1994)”, *Revue internationale de droit pénal*, ERES, 2015, vol. 86, núm. 2015/1, pp. 147–170.
BACHMAIER WINTER L., “Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015”, *Boletín del Ministerio de Justicia*, Ministerio de Justicia, 2017, vol. 71, núm. 2195, pp. 1–36.
BOUCHET M., “Les drones face aux enjeux de droit pénal et de libertés fondamentales”, *Dalloz IP/IT*, Dalloz, 2022, p. 299.
BUISSON J., “Contrôle de l’éventuelle provocation policière : création d’un site pédo-pornographique un policier, même étranger”, *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2008, p. 663.
COLLET P., “Le renforcement progressif des garanties applicables à deux mesures intrusives : la géolocalisation et la sonorisation”, *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2021, p. 29.
CUADRADO SALINAS C., “Registro informático y prueba digital: estudio y análisis comparado de la ciberinvestigación criminal en Europa (1)”, *La ley penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, 2014, núm. 107, p. 3.
DUMONT J., FOMBONNE J.-C., “Fascicule 20 : Interceptions des correspondances émises par la voie de communications électroniques - Articles 100 à 100-7”, *JurisClasseur Procédure pénale*, LexisNexis, el 18 de mayo de 2020.
FERNÁNDEZ RODRÍGUEZ J.J., “Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente”, *Revista Española de Derecho Constitucional*, el 14 de diciembre de 2016, núm. 108, pp. 93–122, DOI:10.18042/cepc/redc.108.03.
FRANCILLON J., “Provocation à la commission d’actes de pédophilie organisée par un service de police étranger utilisant le réseau internet (suite)”, *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2008, p. 621.

FRANCILLON J., “Cyberdélinquance et provocations policières”, *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2014, p. 577.
FUCINI S., “Vidéosurveillance sur la voie publique durant l’enquête : conditions d’autorisation”, *Dalloz Actualité*, Dalloz, el 6 de enero de 2021.
FUCINI S., “Vidéosurveillance sur la voie publique durant l’enquête : conditions de réalisation”, *Dalloz Actualité*, Dalloz, el 18 de enero de 2019.
GUERRIER C., “« Loppsi 2 » et l’utilisation des nouvelles technologies”, *Revue Le Lamy Droit de l’immatériel*, el 1 de octubre de 2010, núm. 64.
HARBOTTLE QUIRÓS F., “El agente encubierto informático: Reflexiones a partir de la experiencia española”, *Revista Judicial, Poder Judicial de Costa Rica*, 2021, núm. 131, pp. 123–140.
LAZERGES C., “La dérive de la procédure pénale”, *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2003, p. 644.
LAZERGES C., “Le déclin du droit pénal : l’émergence d’une politique criminelle de l’ennemi”, *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2016, p. 649.
LEPAGE A., “Provocation sur Internet - La distinction entre provocation à la preuve et provocation à la commission d’une infraction à l’épreuve d’Internet”, *Communication Commerce électronique*, septiembre de 2014, núm. 9.
LÓPEZ-BARAJAS PEREA I., “Garantías constitucionales en la investigación tecnológica del delito: previsión legal y calidad de la ley”, *Revista de Derecho Político*, Universidad Nacional de Educacion a Distancia (UNED), 2017, núm. 98, pp. 91–119, 29 páginas.
MAISTRE DU CHAMBON P., “La régularité des « provocations policières » : l’évolution de la jurisprudence”, *La Semaine Juridique Edition Générale*, LexisNexis, el 27 de diciembre de 1989, núm. 51, p. doctr. 3422.
MEINDL T., “Fascicule 20 : Procédure applicable à la criminalité et la délinquance organisées – Poursuite. Instruction. Jugement. Assistants spécialisés – Dispositions dérogatoires de procédure – Articles 706-73 à 706-106”, *JurisClasseur Procédure pénale*, LexisNexis, el 31 de enero de 2020.
ORTIZ PRADILLO J.C., “Europa: auge y caída de las investigaciones penales basadas en la conservación de datos de comunicaciones electrónicas”, *Revista General de Derecho Procesal*, Iustel, 2020, núm. 52, p. 7.
ORTIZ PRADILLO J.C., “Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos fundamentales en el proceso penal”, *Diario La Ley*, Wolters Kluwer, 2021, núm. 9955, p. 1.
PERRIER J.-B., “Le fair-play de la preuve pénale”, *Actualité juridique Pénal*, Dalloz, 2017, p. 436.
PITTI G., “L’affaire de la sextape : on ne dribble pas le principe de loyauté des preuves !”, *Gazette du Palais*, el 19 de septiembre de 2017, núm. 31, p. 18.
QUEMENER M., “Fascicule 20 : La preuve numérique dans un cadre pénal - Articles 427 à 457”, *JurisClasseur Procédure pénale*, LexisNexis, el 18 de abril de 2019.
QUEMENER M., “Les dispositions liées au numérique de la loi du 3 juin 2016 renforçant la lutte contre le crime organisé et le terrorisme”, *Dalloz IP/IT*, 2016, p. 431.
QUEMENER M., “Fascicule 1110 : Infiltrations numériques”, *JurisClasseur Communication*, LexisNexis, el 3 de julio de 2019.
QUEMENER M., “Les spécificités juridiques de la preuve numérique”, *Actualité juridique Pénal*, Dalloz, 2014, p. 63.
QUEMENER M., “Fascicule 982 : Géolocalisation dans le cadre pénal - Articles 689 à 693”, *JurisClasseur Communication*, LexisNexis, el 3 de julio de 2019.
RAYÓN BALLESTEROS M.C., “Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015”, *Anuario Jurídico y Económico Escurialense*, Real Colegio Universitario “Escorial-María Cristina”, 2019, núm. 52, pp. 179–203.
SAINT-PAU J.-C., “Les investigations numériques et le droit au respect de la vie privée”, *Actualité juridique Pénal*, Dalloz, 2017, p. 321.
SANCHÍS CRESPO C., “Puesta al día de la instrucción penal: la interceptación de las comunicaciones telefónicas y telemáticas”, *La ley penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, 2017, núm. 125, p. 1.
TOUILLIER M., “Les droits de la défense dans les procédures d’exception : une évolution « vent dessus, vent dedans »”, *Actualité juridique Pénal*, Dalloz, 2016, p. 119.
VALAT J.-P., “Prise de photos ou enregistrement vidéo : que peut faire un enquêteur ?”, *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2022, p. 399.
VARGAS GALLEGO A.I., “Algunos apuntes sobre la interceptación de las comunicaciones telefónicas”, *Revista de Jurisprudencia El Derecho*, el 16 de diciembre de 2020, núm. 8.

VELASCO NUÑEZ E., “Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías”, *Revista de Jurisprudencia*, el 1 de febrero de 2011, núm. 4, p. 1.
VELASCO NÚÑEZ E., “Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica”, *Diario La Ley*, el 4 de noviembre de 2013, núm. 8183.
VERGES E., “Loyauté et licéité, deux apports majeurs à la théorie de la preuve pénale”, *Recueil Dalloz*, 2014, p. 407.
VERGES E., “La notion de criminalité organisée après la loi du 9 mai 2004”, *Actualité juridique Pénal*, Dalloz, 2004, p. 181.
VLAMYNCK H., “Le point sur la captation de l’image et des paroles dans l’enquête de police”, *Actualité juridique Pénal*, Dalloz, 2011, p. 574.
VLAMYNCK H., “La loyauté de la preuve au stade de l’enquête policière”, *Actualité juridique Pénal*, Dalloz, 2014, p. 325.

4. Jurisprudencia

A. Jurisprudencia europea

TEDH, *Kruslin c. Francia*, el 24 de abril de 1990, núm. 11801/85.
TEDH, *Huvig c. Francia*, el 24 de abril de 1990, núm. 11105/84.
TEDH, *Lambert c. Francia*, el 24 de agosto de 1998, núm. 88/1997/872/1084.
TEDH, *Matheron c. Francia*, el 29 de marzo de 2005, núm. 57752/00.
TEDH, *Vetter c. Francia*, el 31 de mayo de 2005, núm. 59842/00.
TEDH, *Wisse c. Francia*, el 20 de diciembre de 2005, núm. 71611/01.
TEDH, *Ben Faiza c. Francia*, el 8 de febrero de 2018, núm. 31446/12.
TEDH, *Prado Bugallo c. España*, el 18 de febrero de 2003, núm. 58496/00.
TEDH, *Klass y otros c. Alemania*, el 6 de septiembre de 1978, núm. 5029/71.
TEDH, *Malone c. Reino Unido*, el 2 de agosto de 1984, núm. 8691/79.
TEDH, *Uzun c. Alemania*, el 2 de septiembre de 2010, núm. 35623/05.
TEDH, *Allan c. Reino Unido*, el 5 de noviembre de 2002, núm. 48539/99.
TEDH, *P.G. y J.H. c. Reino Unido*, el 25 de septiembre de 2001, núm. 44787/98.
TEDH, *Liberty y otros c. Reino Unido*, el 1 de julio de 2008, núm. 58243/00.
TEDH, *Big Brother Watch y otros c. Reino Unido (1)*, el 13 de septiembre de 2018, 58170/13, 62322/14 y 24960/15.
TEDH, *Centrum För Rättvisa c. Suecia (2)*, el 25 de mayo de 2021, núm. 35252/08.
TEDH, *Benedik c. Eslovenia*, el 24 de abril de 2018, núm. 62357/14.
TEDH, *Ringler c. Austria*, el 12 de mayo de 2020, núm. 2309/10.
TEDH, *Amann c. Suiza*, el 18 de octubre de 2011, núm. 27798/95.
TEDH, *Leander c. Suecia*, el 26 de marzo de 1987, núm. 9248/81.
TEDH, *Peck c. Reino Unido*, el 28 de enero de 2003, núm. 44647/98.
TEDH, *Kennedy c. Reino Unido*, el 18 de mayo de 2010, núm. 26839/05.
TEDH, *Roman Zakharov c. Rusia*, el 4 de diciembre de 2015, núm. 47143/06.
TEDH, *Kopp c. Suiza*, el 25 de marzo de 1998, núm. 13/1997/797/1000.
TEDH, *Valenzuela Contreras c. España*, el 30 de julio de 1998, núm. 58/1997/842/1048.
TEDH, *Weber y Saravia c. Alemania*, el 29 de junio de 2006, núm. 54934/00.
TEDH, *Aalmoes y otros c. Países Bajos*, el 25 de noviembre de 2004, núm. 16269/02.
TEDH, *Dumitri Popescu c. Rumania*, el 26 de abril de 2007, núm. 71525/01.
TEDH, *Big Brother Watch y otros c. Reino Unido (2)*, el 25 de mayo de 2021, 58170/13, 62322/14 y 24960/15.
TEDH, *Iordachi y otros c. Moldavia*, el 10 de febrero de 2009, núm. 25198/02.
TEDH, *Szabó y Vissy c. Hungría*, el 12 de enero de 2016, núm. 37138/14.
TEDH, *Moulin c. Francia*, el 23 de noviembre de 2010, núm. 37104/06.

TJUE, *Digital Rights Ireland Ltd (C-293/12), Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl e.a. (C-594/12) c. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána y Irlanda*, el 8 de abril de 2014, C-293/12 y C-594/12.
TJUE, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d’accès à Internet associatifs c. Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l’Intérieur, Ministre*

des Armées ; y Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX c. Conseil des ministres, el 6 de octubre de 2020, C-511/18, C-512/18 y C-520/18.
TJUE, *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service*, el 6 de octubre de 2020, C-623/17.
TJUE, *Tele2 Sverige AB c. Post-och telestyrelsen*, el 21 de diciembre de 2016, C-203/15 y C-698/15.
TJUE, *Ministerio Fiscal*, el 2 de octubre de 2018, C-207/16.
TJUE, *European Commission c. Kingdom of Spain*, el 25 de febrero de 2021, C-658/19.

B. Jurisprudencia española

Tribunal Supremo. Sala Segunda, de lo Penal, el 26 de noviembre de 2014, núm. 850/2014.
Tribunal Supremo. Sala Segunda, de lo Penal, el 1 de junio de 2017, núm. 400/2017.
Tribunal Supremo. Sala Segunda, de lo Penal, el 15 de julio de 2016, núm. 652/2016.
Tribunal Supremo. Sala Segunda, de lo Penal, el 16 de mayo de 2014, núm. 421/2014.
Tribunal Supremo. Sala Segunda, de lo Penal, el 27 de junio de 2018, núm. 311/2018.
Tribunal Supremo. Sala Segunda, de lo Penal, el 20 de abril de 2016, núm. 329/2016.
Tribunal Supremo. Sala Segunda, de lo Penal, el 22 de junio de 2007, núm. 562/2007.
Tribunal Supremo. Sala Segunda, de lo Penal, el 7 de julio de 2016, núm. 610/2016.
Tribunal Supremo. Sala Segunda, de lo Penal, el 9 de mayo de 2008, núm. 236/2008.
Tribunal Supremo. Sala Segunda, de lo Penal, el 28 de mayo de 2008, núm. 292/2008.
Tribunal Supremo. Sala Segunda, de lo Penal, el 5 de julio de 2007, núm. 767/2007.
Tribunal Supremo. Sala Segunda, de lo Penal, el 14 de julio de 2010, núm. 752/2010.
Tribunal Supremo. Sala Segunda, de lo Penal, el 7 de febrero de 2019, núm. 65/2019.
Tribunal Supremo. Sala Segunda, de lo Penal, el 18 de abril de 2017, núm. 272/2017.
Tribunal Supremo. Sala Segunda, de lo Penal, el 3 de febrero de 2006, núm. 104/2006.
Tribunal Supremo. Sala Segunda, de lo Penal, el 22 de enero de 2014, núm. 7/2014.

Tribunal Constitucional, el 22 de septiembre de 2014, núm. 145/2014.
Tribunal Constitucional, el 29 de noviembre de 1984, núm. 114/1984.
Tribunal Constitucional, el 9 de octubre de 2006, núm. 281/2006.
Tribunal Constitucional, el 20 de mayo de 2002, núm. 123/2002.
Tribunal Constitucional, el 18 de julio de 2005, núm. 205/2005.

C. Jurisprudencia francesa

Cour de Cassation, Chambre criminelle, el 6 de abril de 2022, 21-84.092.
Cour de Cassation, Chambre criminelle, el 7 de mayo de 2019, 18-85.596.
Cour de Cassation, Chambre criminelle, el 21 de marzo de 2007, 06-89.444.
Cour de Cassation, Chambre criminelle, el 8 de diciembre de 2020, 20-83.885.
Cour de Cassation, Chambre criminelle, el 11 de diciembre de 2018, 18-82.365.
Cour de Cassation, Chambre criminelle, el 22 de octubre de 2013, núm. 13-81949.
Cour de Cassation, Chambre criminelle, el 22 de octubre de 2013, núm. 13-81945.
Cour de Cassation, Chambre criminelle, el 14 de enero de 2014, núm. 13-84909.
Cour de Cassation, Chambre criminelle, el 27 de febrero de 1996, núm. 95-81366.
Cour de Cassation, Chambre criminelle, el 7 de febrero de 2007, núm. 06-87753.
Cour de Cassation, Chambre criminelle, el 4 de junio de 2008, núm. 08-81045.
Cour de Cassation, Chambre criminelle, el 30 de abril de 2014, núm. 13-88162.
Cour de Cassation, Chambre criminelle, el 11 de julio de 2017, núm. 17-80313.
Cour de Cassation, Assemblée plénière, el 9 de diciembre de 2019, núm. 18-86767.
Cour de Cassation, Chambre criminelle, el 17 de julio de 1990, núm. 90-82614.
Cour de Cassation, Chambre criminelle, el 26 de noviembre de 1990, núm. 90-84590.
Cour de Cassation, Chambre criminelle, el 9 de diciembre de 1991, núm. 88-80786, 90-84994.
Cour de Cassation, Chambre criminelle, el 22 de junio de 2016, núm. 16-81834.
Cour de Cassation, Chambre criminelle, el 9 de enero de 2018, núm. 17-82946.
Cour de Cassation, Chambre criminelle, el 22 de noviembre de 2011, núm. 11-84308.
Cour de Cassation, Chambre criminelle, el 6 de enero de 2015, núm. 14-85448.

Conseil d'Etat, *French Data Network et autres*, el 21 de abril de 2021, núm. 397844, 397851, 393099, 394922, 424717, 424718.

Conseil constitutionnel, *Ligue des droits de l'homme [Perquisitions et saisies administratives dans le cadre de l'état d'urgence]*, el 19 de febrero de 2016, 2016-536 QPC.
Conseil constitutionnel, *Loi de programmation 2018-2022 et de réforme pour la justice*, el 21 de marzo de 2019, 2019-778 DC.

CNIL, *Délibération portant avis sur un projet de décret modifiant le décret n°2015-1700 du 18 décembre 2015 relatif à la mise en œuvre de traitements de données informatiques captées en application de l'article 706-102-1 du code de procédure pénale (demande d'avis n°18004354)*, el 26 de septiembre de 2019, núm. 2019-119.

5. Documentos institucionales

Fiscalía General del Estado, Circular 1/2019 sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal, el 6 de marzo de 2019.
Fiscalía General del Estado, Circular 2/2019 sobre interceptación de comunicaciones telefónicas y telemáticas, el 6 de marzo de 2019.
Fiscalía General del Estado, Circular 3/2019 sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, el 6 de marzo de 2019.
Fiscalía General del Estado, Circular 4/2019 sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, el 6 de marzo de 2019.
Fiscalía General del Estado, Circular 5/2019 sobre sobre registro de dispositivos y equipos informáticos, el 6 de marzo de 2019.

Ministère de la Justice, Circulaire du 1er avril 2014 de présentation de la loi n°2014-372 relative à la géolocalisation, Francia, el 28 de marzo de 2014.
GROUPE DE TRAVAIL INTERMINISTERIEL SUR LA LUTTE CONTRE LA CYBERCRIMINALITE, *Protéger les Internautes - Rapport sur la cybercriminalité*, Francia, febrero de 2014.
CYBERLEX, CENTRE EXPERT CONTRE LA CYBERCRIMINALITE FRANÇAIS, "Code de procédure pénale et lutte contre la cybercriminalité : propositions pour une efficacité juridique renforcée", el 24 de enero de 2018.

COMISIÓN EUROPEA, "Commission Staff working document - Impact assessment report accompanying the document Proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse", UE, el 11 de mayo de 2022, SWD(2022) 209 final.
EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE, "European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment", Consejo de Europa, el 4 de diciembre de 2018.
COMITE DE MINISTROS, "Recommendation Rec(2001)11 concerning guiding principles on the fight against organised crime", Consejo de Europa, el 19 de septiembre de 2001.

6. Páginas internet

BURKE M., "Amazon's Alexa may have witnessed alleged Florida murder, authorities say", *NBC News*, el 2 de noviembre de 2019, en línea https://www.nbcnews.com/news/us-news/amazon-s-alexa-may-have-witnessed-alleged-florida-murder-authorities-n1075621 (recuperado el 12 de octubre de 2022).