TESIS DOCTORAL

VIGILANCIA E INVESTIGACIÓN POLICIAL EN EL CIBERESPACIO
ASPECTOS PROCESALES DEL CIBERPATRULLAJE

Doctorando	Manuel Jesús Távora Serra
Programa	Doctorado en Derecho
Departamento	Departamento de Derecho Procesal
	Universidad de Sevilla
Fecha	20 de julio de 2022
Dirección	Dra. María del Pilar Martín Ríos
	Prof. Titular de Universidad

ABREVIATURAS, SIGLAS Y ACRÓNIMOS

AAP	Auto de la Audiencia Provincial
ALECRIM	Anteproyecto de Ley de Enjuiciamiento Criminal de 2020
AP	Audiencia Provincial
ARPANET	*Advanced Research Projects Agency Network*
ATS	Auto del Tribunal Supremo
CDFUE	Carta de Derechos Fundamentales de la Unión Europea
CdPT	Conclusiones de la Presidencia del Consejo de Tampere
CB	Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001
CE	Constitución española
CEDH	Convenio Europeo de Derechos Humanos
CNI	Centro Nacional de Inteligencia
CP	Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal
DACE	Datos asociados a comunicaciones electrónicas
EOMF	Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal
FFCCSE	Fuerzas y Cuerpos de Seguridad del Estado
FJ	Fundamento Jurídico
INTERPOL	Organización Internacional de Policía Criminal
LEC	Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil
LECrim	Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal
LGT	Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
LO	Ley Orgánica
LOFCS	Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad
LOPD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
LOPJ	Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial

LORTAD	Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.
LRCNI	Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia
LSSI	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
SAP	Sentencia de la Audiencia Provincial de [ciudad]
SITEL	Sistema Integrado de Interceptación de Comunicaciones
STC	Sentencia del Tribunal Constitucional
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
STS	Sentencia del Tribunal Supremo
TIC	Tecnologías de la Información y de la Comunicación
TC	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
TJUE	Tribunal de Justicia de la Unión Europea
UE	Unión Europea
TUE	Tratado de la Unión Europea
TFUE	Tratado de Funcionamiento de la Unión Europea
CBC	Convenio de Budapest sobre la Ciberdelincuencia

A mis padres, por su constante y amable exigencia, su incondicional apoyo y, sobre todo, por creer en mi capacidad mucho más que yo mismo.

ÍNDICE

CAPÍTULO I
INTRODUCCIÓN A LA TESIS DOCTORAL

1. ESPÍRITU DE LA PRESENTE INVESTIGACIÓN

Por lo que se refiere a cualquier trabajo de investigación y, en particular, en lo relativo a tesis doctorales, son multitud los recursos que se han elaborado con la finalidad de auxiliar al investigador en su misión de finalizarlos con éxito. Aunque cada uno desarrolla, en la proporción que haya podido entender como conveniente su autor, los diferentes métodos que pueden aplicarse para desarrollar una investigación doctoral y conseguir que esta cristalice en la tesis, todos coinciden en que cualquier trabajo debe dedicar sus primeras páginas a la función de contextualizar la labor investigadora, exponiendo su finalidad y utilidad, ubicando así al lector en la mejor posición desde la que recibir la exposición de la investigación.

Con el objetivo de levantar dicha carga, y siguiendo autorizadas voces al respecto[1], entendemos que en esta introducción debemos exponer el objeto de la investigación y la finalidad perseguida, la justificación del tema elegido –con una breve referencia al *status quaestionis*–, el método y las fuentes utilizados en el desarrollo de la investigación, y la estructura del propio trabajo de investigación que se presenta. Por último, resultaba igualmente inexcusable la formulación de los muy debidos agradecimientos. En consecuencia, hemos distribuido esos temas en los siguientes apartados.

Finalmente, nos gustaría referirnos a una inspiradora y sintética reflexión que leía hace algún tiempo sobre los diferentes sistemas de pensamiento de nuestro cerebro.[2] Sintéticamente, el autor identificaba una forma de pensamiento rápida y otra forma de pensamiento lenta, cada una con sus correspondientes ventajas y desventajas (la primera, más adaptada a situaciones de urgencia y menos útil para elaborar estrategias a largo plazo; la segunda, menos adecuada para tomar decisiones inmediatas, pero más acertada para reflexionar sobre la realidad de las cosas). El autor señalaba cómo la propia plasticidad cerebral, en el constante esfuerzo de dicho órgano por adaptarse a los parámetros del medio en el que se encontraba, podía determinar el tipo de pensamiento que predominaba

---

[1] CERVERA RODRÍGUEZ, Á., *Cómo elaborar trabajos académicos y científicos: (TFG, TFM, tesis y artículos)*, Alianza, Madrid, 2019.
[2] MAFFEI, L., *Alabanza de la lentitud*, Alianza, Madrid, 2016.

en una persona y llamaba la atención del lector sobre cómo, en nuestra época, al aplicar criterios de mercado, económicos y mercantiles como valores fundamentales en la formación y desarrollo de las personas, se estaba fomentando en los individuos la ejecución de un pensamiento rápido, compulsivo y sometido al imperio de la satisfacción a corto plazo, así como de las peligrosas consecuencias que podía ello traer para una vida ordenada en sociedad, que exige aceptar ciertos compromisos racionales a corto plazo para extraer ventajas en largo plazo.

Para evitar sintetizar aquí una obra que, como resulta de la lectura de sus páginas, es ya una síntesis en sí misma, nos limitaremos a coincidir con el autor cuando llama la atención sobre el tipo de pensamiento que se promueve en la sociedad en que vivimos, y a expresar nuestra intención de que esta tesis doctoral contribuya a ayudar a que nuestra sociedad continúe conociéndose a sí misma y al contexto en el que habita. En ese sentido, entendemos que la materia objeto de nuestra investigación doctoral brindaba dicha posibilidad.

2. OBJETO Y FINALIDAD DE LA INVESTIGACIÓN

El objeto de la investigación doctoral que ahora se plasma en este trabajo es la actividad desarrollada en el medio virtual por las Fuerzas y Cuerpos de Seguridad del Estado en cumplimiento de sus funciones de prevención e investigación de los comportamientos delictivos. En concreto, analizaremos la hipótesis en que dicha actividad se verifica sin control jurisdiccional previo. Es, precisamente, esa nota de ausencia de control jurisdiccional, la que singulariza nuestra investigación y la diferencia de estudios acerca de las diligencias de investigación tecnológica previstas en los artículos 588 *bis* y siguientes LECrim. Estas, ampliamente analizadas por la doctrina, no son objeto de nuestro estudio.

A su vez, dentro del objeto de nuestra investigación, hemos distinguido, por un lado, la actividad de investigación policial que se verifica en un momento anterior a la incoación de un proceso penal –el denominado *ciberpatrullaje*–, y, por otro lado, la actividad de investigación policial que tiene lugar en el marco de un proceso penal ya incoado, pero que continúa sin precisar de autorización judicial previa –que nos hemos atrevido a denominar, en un intento meramente funcional y con el ánimo de diferenciarla de la anterior, como *ciberinvestigación*–.

Fijado el objeto de nuestra investigación, la principal cuestión que hemos perseguido analizar es si, con ocasión del régimen jurídico vigente –en especial, tras la reforma operada 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–, es posible que, en el desarrollo y ejecución de dicha actividad de *ciberpatrullaje* y *ciberinvestigación*, los derechos fundamentales de quienes sean objeto de las mismas (fundamentalmente, quienes ocupen la posición procesal de investigado) resultan afectados.

En la búsqueda de la respuesta a dicha pregunta, ha sido necesario analizar y recopilar las diferentes técnicas de investigación cibernética de que dispone la policía, las posibilidades que otorga la informática en materia de recopilación y tratamiento de datos, y el régimen del deber de colaboración de los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información.

En consecuencia, se despliegan otras utilidades accesorias más allá de la finalidad principal, como el análisis de las técnicas policiales de ciberpatrullaje o ciberinvestigación, la recopilación y publicación de dichas técnicas, y los detalles del referido cumplimiento del deber de colaboración entre prestadores de servicios de la sociedad de la información y los poderes públicos.

3. JUSTIFICACIÓN DE LA MATERIA DE INVESTIGACIÓN

En la actualidad, el desarrollo de las tecnologías de computación y de las telecomunicaciones ha permitido a nuestra sociedad construir y acceder a un medio complementario a la realidad física directamente perceptible, caracterizado fundamentalmente por la inmediatez, la ubicuidad y la universalidad con que los actos en él ejecutados, y sus consecuencias, se verifican.

Ese nuevo medio virtual común, denominado *ciberespacio*, encuentra sus orígenes en el proyecto ARPANET[3]. Supone uno de los elementos más trascendentales de nuestra época y, acaso, de nuestra historia, que influye en todos los ámbitos de la existencia individual y social[4], y provocó, junto con el desarrollo de la informática, un

[3] "ARPANET | Real Academia de Ingeniería", fecha de consulta 20 abril 2020, en http://diccionario.raing.es/es/lema/arpanet.
[4] GONZÁLEZ HURTADO, J. A., "Delincuencia informática: daños informáticos del artículo 264 del Código penal y propuesta de reforma", 2013, Universidad Complutense de Madrid, pp. 17–57, fecha de consulta 21 enero 2020, en https://dialnet.unirioja.es/servlet/tesis?codigo=39078.

desplazamiento de los métodos analógicos en muchos aspectos de la vida moderna, tanto en el ámbito individual y privado como en el social y público.

No en vano, a modo de ejemplo y de acuerdo con el último estudio disponible del INE, "9 de cada 10 personas de 16 a 74 años ha usado internet en los tres últimos meses. El 78,2% de las mujeres y el 77,0% de los hombres utilizan internet a diario. El 46,9% de las personas de 16 a 74 años ha comprado por internet en los tres últimos meses".[5] Esta tendencia ha experimentado un nuevo impulso con ocasión de los condicionantes impuestos por la aparición del covid-19, que también ha obligado a la Administración de Justicia a dar un paso adelante en el empleo de las nuevas tecnologías en el marco del proceso[6].

A pesar de los avances que supone, y en la medida en que los sujetos que actúan en él siguen siendo –por el momento[7]– los mismos que en la realidad material, las modificaciones e influencias no dejan de suponer sino modalidades de conductas ya existentes con anterioridad. A nuestro juicio, en este momento el medio *cibernético* no ha dejado de ser más que un reflejo del medio real, y cuando el sujeto no cambia, tampoco lo hacen sus conductas, que solo se ven adaptadas a las nuevas circunstancias del medio. Prueba de ello es, si se quiere argumentar en este sentido, lo necesario que ha resultado tipificar nuevas modalidades delictivas, pero, en absoluto, reconocer bienes jurídicos distintos de los ya existentes[8].

Ni siquiera el derecho al propio entorno virtual puede entenderse como algo esencialmente nuevo, toda vez que los conflictos que le sirven de objeto ya existían mucho antes de que el ciudadano medio pudiera acceder al *ciberespacio*. De hecho, se construye tal idea sobre los conceptos de derechos fundamentales tradicionales, aplicados al medio relativamente nuevo de la informática[9], aunque haya autores que afirman que el esquema

---

[5] "INE base / Nivel y condiciones de vida (IPC) /Condiciones de vida /Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares / Últimos datos", *INE*, fecha de consulta 24 abril 2020, en https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176741&menu=ultiDatos&idp=1254735976608.

[6] MARTÍN DIZ, F., "Justicia digital post–covid19: El desafío de las soluciones extrajudiciales electrónicas de litigios y la inteligencia artificial", *Revista de Estudios Jurídicos y Criminológicos*, 2, 2020, Universidad de Cádiz, p. 2.

[7] "Müller and Bostrom AI Progress Poll", *AI Impacts*, 2014, fecha de consulta 7 mayo 2020, en https://aiimpacts.org/muller–and–bostrom–ai–progress–poll/.

[8] BARRIO ANDRÉS, M., *Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2ª, Wolters Kluwers, Madrid, 2018, p. 369.

[9] MARTÍN RÍOS, P., "La indemnidad del domicilio informático como posible límite a la digital forensics", en *Giustizia e Costituzione agli albori del XXI Secolo*, Bonomo Editore, Bolonia, Italia, 2017, pp. 1279–1284.

clásico de nuestro Código Penal, fundado en el bien jurídico afectado, ha devenido insuficiente.[10]

En el medio virtual se verifican, por tanto, unas mismas conductas que en el medio material, pero con variaciones debidas al lugar en que se desarrollan. Así, en el medio virtual, como en el tradicional físico, las personas exploran sus inquietudes, persiguen sus fines, construyen vínculos, celebran negocios y procuran generar riqueza, al igual que también transgreden el ordenamiento jurídico, a veces con una intensidad merecedora exclusivamente de la calificación de ilicitud civil del acto, otras veces administrativa, y otras veces delictiva, exactamente igual que en la realidad material. Entre otras muchas variantes, son manifestaciones de dichas conductas delictivas los fraudes con apariencia de operaciones mercantiles, las suplantaciones de identidad, las lesiones del derecho al honor, las conductas de acoso y violencia virtual, etc.

De esa manera, y siguiendo la misma lógica expuesta, el *ciberpatrullaje* no deja de ser una modalidad de una actividad bien conocida por la doctrina respecto de las Fuerzas y Cuerpos de Seguridad del Estado –la de prevenir e investigar la comisión de delitos–, que ha debido adaptarse a las particularidades y exigencias del medio virtual.

De este modo, la doctrina se ha venido refiriendo al *ciberpatrullaje* como aquella actividad de rastreo y sondeo de contenidos que desarrollan habitualmente las Fuerzas y Cuerpos de Seguridad del Estado en el medio *cibernético* abierto –diremos abierto, para evitar precisiones que se desgranarán posteriormente[11]– en cumplimiento de los fines preventivos e investigativos encomendados por el legislador (este matiz entendemos que es fundamental, habida cuenta de la evidente falta de legislación en materia de *ciberpatrullaje* y demás actividad "autónoma" de la policía o del Ministerio Fiscal). Es decir, se trata de la definición de la actividad de patrullaje tradicional, a la que se le han añadido las modificaciones que el medio virtual requiere.

---

[10] VELASCO NÚÑEZ, E., "Crimen organizado, internet y nuevas tecnologías", en *Los retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso Gallego de Derecho Procesal (I Internacional), A Coruña, 2 y 3 de junio de 2011, 2012, pp. 245–282*, 2012, p. 269, fecha de consulta 24 octubre 2020, en https://dialnet.unirioja.es/servlet/articulo?codigo=4036200.

[11] A título de ejemplo, se plantean como supuestos cuanto menos aparentemente problemáticos los casos en los que los delincuentes preparan servidores privados o sitios en la internet profunda, no indexados y con evidente voluntad de impedir el acceso a la policía y, sin embargo, agentes de la policía consiguen que uno de dichos administradores les conceda acceso, ignorando este su condición de policías).

Ahora bien, la aplicación de las innovaciones tecnológicas a las conductas tradicionales puede aumentar su intensidad y alcance hasta tal punto que pueda entenderse que ha mutado su condición o que, al menos, sea precisa una regulación específica que garantice su encaje en el marco jurídico. Es lo que sucede con la criminalidad y la investigación policial y sus contrapartidas virtuales: el cibercrimen, por un lado, y el ciberpatrullaje y la ciberinvestigación, por otro.[12]

Así, la magnitud cuantitativa y cualitativa de los daños que originan los *ciberdelito*s es innegable, como lo es su potencialidad global para afectar a la economía y el desarrollo tecnológico de todo el mundo. El coste económico directo y mensurable, computado en función del perjuicio que ocasionara a las víctimas, ya en 2013 se admitía entre los 100.000 y 500.000 millones de dólares[13]. Paralelamente, la Estrategia Nacional de Ciberseguridad de 2019[14] prevé entre sus líneas de acción la de "reforzar las capacidades de investigación y persecución de la cibercriminalidad", estableciendo una serie de medidas a adoptar en dicho marco, como reforzar el marco jurídico para conseguir una mayor eficacia en la respuesta a la cibercriminalidad, especialmente en lo que se refiere a las medidas de investigación, fomentar la colaboración de los ciudadanos –particulares y empresas– con los poderes públicos, potenciar las capacidades de investigación del ciberespacio, procurar a los operadores jurídicos y Fuerzas y Cuerpos de Seguridad del Estado el acceso a medios materiales que les doten de mayores capacidades para la investigación, e impulsar la coordinación institucional y la cooperación policial internacional. Frente a tales pretensiones expansionistas del poder público, entendemos necesario realizar un ejercicio de reflexión que ayude a identificar los límites o condicionantes que deben modularlas.

En añadidura, el progreso de las ciencias aplicadas, en general, y de las Tecnologías de la Información de la Comunicación, en particular, la digitalización de la información, la coordinación de los sistemas y bases de almacenamiento de datos y la difusión del fenómeno internet que ya da lugar, incluso, al internet de las cosas, suscitan cuestiones en materia de investigación policial a un ritmo que desborda el aparato público, que se

---

[12] ORTIZ PRADILLO, J. C., "El impacto de la tecnología en la investigación penal y en los derechos fundamentales", en *Problemas actuales de la justicia penal*, Colex, Madrid, 2013, pp. 317–319.

[13] "The Economic Impact of Cybercrime and Cyber Espionage", fecha de consulta 7 marzo 2020, en https://www.csis.org/analysis/economic–impact–cybercrime–and–cyber–espionage.

[14] "Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.", fecha de consulta 4 mayo 2020, en https://www.boe.es/diario_boe/txt.php?id=BOE–A–2019–6347.

encuentra limitado por los tiempos de su propia burocracia. En este contexto, la necesidad de responder de manera inmediata a la realidad social ha justificado, en ocasiones, que se admita cierta relajación en determinadas garantías, lo que hace resurgir peligrosamente la idea[15] de que las Fuerzas y Cuerpos de Seguridad pueden infringir los derechos fundamentales para investigar con eficiencia y eficacia (extremos de singular importancia para nuestra sociedad contemporánea) en sus funciones de prevención e investigación. Ante el temor a lo novedoso, la reacción instintiva parece ser la restricción de garantías procesales y derechos fundamentales. Las limitaciones a la actuación policial pasan a ser entendidas como un obstáculo para una investigación pública eficaz y eficiente[16].

Lo cierto es que, de manera especialmente destacada en el ámbito del *ciberespacio*, la constante búsqueda de la seguridad nacional por los poderes públicos, persiguiendo una mayor eficiencia en la evitación, persecución y represión de los delitos (en especial, en la lucha contra el terrorismo), parece justificar una creciente actitud invasora en el ámbito de las telecomunicaciones que, consecuentemente, restringe gravemente los derechos fundamentales de los ciudadanos, llegando a apreciarse incluso la existencia de una suerte de toque de queda digital[17].

Existen numerosos ejemplos: el espionaje masivo de las comunicaciones por parte la Agencia de Seguridad Nacional revelado por Snowden[18], otras redes tradicionales de espionaje internacional de las comunicaciones como *Echelon*; programas para la interceptación de mensajes trasmitidos por correo electrónico, como el *Carnivore* del FBI norteamericano; o, incluso, el proyecto europeo *Enfopol*. A todo ello hay que añadir las coincidentes propuestas o aprobaciones de iniciativas legislativas para dar cobertura a tales prácticas, como la *Patriot Act*, en Estados Unidos o la *Investigatory Powers Act*, en

---

[15] ASENCIO MELLADO, J. M., "La STC 97/2019, de 16 de julio. Descanse en paz la prueba ilícita", *Diario La Ley*, 9499, 2019.
[16] *Ibid.*, p. 3.
[17] CABEZUDO RODRÍGUEZ, N., "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal", *I Jornada del Boletín del Ministerio de Justicia: Las reformas del proceso penal*, vol. 2186, 2016.
[18] Revelación que, en última instancia, dio lugar a la STEDH de 25 de mayo de 2021, (Big Brother Watch and Others v. the United Kingdom), en la que la Gran Sala del Tribunal Europeo de Derechos Humanos viene a reconocer que los sistemas de vigilancia masiva son de "vital importancia" para los Estados a la hora de identificar posibles amenazas a su seguridad nacional, pero recordando que deben de contar con protecciones y garantías de extremo a extremo ("end-to-end"), y que las autoridades nacionales deben realizar una evaluación, en cada etapa del proceso, de las medidas a adoptar e implementar en el marco general de los principios de necesidad y proporcionalidad.

Inglaterra, la *Loi relative au renseignement* en Francia, o la *Gesetz zur Beschränkung des Brief–, Post– und Fernmeldegeheimnisses*, en Alemania.

Todo ello ha dado forma a un nuevo paradigma calificado como de "sociedad del riesgo", en el que se abandona la idea del "Estado del bienestar" para adoptar la del "Estado de la seguridad", con la consiguiente expansión, no ya de la jurisdicción penal –que también–, sino de los poderes investigadores del Estado.[19] Tendencia esta que ha trascendido, incluso, al modelo económico vigente, llegando a identificarse como capitalismo de la vigilancia[20] o capitalismo de control[21], conceptos que exploraremos con más detenimiento en el penúltimo apartado de nuestra tesis doctoral.

De este modo, de igual forma que la tecnología y el ciberespacio acentúan las capacidades lesivas de la cibercirminalidad, así ocurre con la función de vigilancia policial. Entendemos que esta mera circunstancia justifica, por sí sola, la pertinencia del estudio que es objeto de esta investigación doctoral, en la medida en que se trata de analizar de qué modo la actividad de prevención e investigación policial se ha amoldado al *ciberespacio*. Pero es que además, por el objeto al que se refiere (actividad pública no protegida de los usuarios), por el medio en el que se desarrolla (red abierta o de público acceso) y por el modo en que se verifica (técnicas no perceptiblemente invasivas), creemos que el *ciberpatrullaje* (es decir, las actividades de rastreo y sondeo de la red con finalidad de prevención e investigación del delito) plantea cuestiones trascendentales que es necesario abordar: su naturaleza, su cobertura normativa, su objeto, el modo en que se ejecutan, las buenas prácticas que han de desplegarse en su realización, y las garantías de que han de recubrirse, especialmente en lo que se refiere al conflicto con los derechos fundamentales de aquellos *cibernautas* que fueran objeto de las actividades de *ciberpatrullaje.*

En ese sentido, tal vez quepa destacar lo paradójico que resulta el hecho de que una actividad que, en teoría, no necesita de la previa autorización judicial puede llegar a comprometer –en una medida nada despreciable– los derechos fundamentales de los ciudadanos.

---

[19] JIMÉNEZ MEJÍA, D., "La crisis de la noción material de bien jurídico en el derecho penal del riesgo", *Nuevo Foro Penal*, 82, 2014, Universidad EAFIT, p. 3.
[20] ZUBOFF, S., *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, PublicAffairs, Estados Unidos, 2019.
[21] LLOVERAS SOLER, J. M., "Capitalismo de control", *Alternativas económicas*, 80, 2020, SGEL: Sociedad General Española de Librería, p. 10.

A nuestro juicio, la correcta delimitación conceptual, primero, y normativa, después, de la actividad de *ciberpatrullaje* constituye una cuestión fundamental, no sólo por la propia actualidad de nuestra sociedad y la cada vez mayor inmersión del quehacer diario de los ciudadanos en el medio *cibernético*, sino también porque, en lo que se refiere a nuestro ordenamiento procesal penal, se tiende a la progresiva reducción del protagonismo del juez de instrucción en lo que se refiere a la investigación de los hechos –sin perjuicio de su posición de garante de los derechos fundamentales– con el consiguiente incremento de la actividad investigadora de la Policía Judicial y del Ministerio Fiscal.

A ese respecto, hay que recordar que la Policía Judicial ha visto reforzadas sus funciones, especialmente con las reformas operadas por la Ley 38/2002, de 24 de octubre, de reforma parcial de la Ley de Enjuiciamiento Criminal, sobre procedimiento para el enjuiciamiento rápido e inmediato de determinados delitos y faltas, y de modificación del procedimiento abreviado, y la Ley Orgánica 8/2002, de 24 de octubre, complementaria de la Ley de reforma parcial de la Ley de Enjuiciamiento Criminal, sobre procedimiento para el enjuiciamiento rápido e inmediato de determinados delitos y faltas, y de modificación del procedimiento abreviado[22].

Igualmente, la Ley 41/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal y el fortalecimiento de las garantías procesales, atribuye un papel más activo al Ministerio Fiscal en la investigación de los hechos, tanto en el transcurso de la fase de instrucción –desarrollando las competencias que ya tenía atribuidas en los artículos 306, 309 *bis* y 319 LECrim–, al reconocerle en exclusiva o de modo compartido con el resto de las partes personadas la facultad de interesar la conversión del procedimiento de simple a complejo o las prórrogas ordinaria y excepcional de los plazos de conformidad con el artículo 324 LECrim, como en lo relativo a la terminación anticipada del procedimiento a través del incidente por aceptación de decreto, previsto en el Título III *bis* LECrim[23]. Todas estas reformas evidencian la tendencia a situar al juez de instrucción como garante de los derechos fundamentales,

[22] Muy especialmente, en el procedimiento para el enjuiciamiento rápido de determinados delitos, regulado en los artículos 770 a 772 y 796 LECrim, que exigen un comportamiento muy activo por parte de la Policía Judicial.

[23] CABEZUDO RODRÍGUEZ, N., "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal", cit., p. 3.

haciendo recaer todo el peso de la iniciativa instructora en el Ministerio Fiscal, que también ostentaría la dirección de la actividad de la Policía Judicial.

Tales cuestiones suponen, a nuestro humilde entender, que no se pueda negar que el *ciberpatrullaje* sea una realidad merecedora de estudio, no sólo por la novedad que reviste en nuestra práctica procesal e investigadora, sino también por tratarse de una actividad sobre la que es difícil practicar un control previo. En particular, esta dificultad que presenta para su fiscalización debe enmarcarse, además, en el contexto facilitado por la STC 97/2019, de 16 de julio, en la que se aprecia una acusada tendencia a la relajación de la garantía de la ilicitud de la prueba obtenida con vulneración de los derechos fundamentales, que deja de estar implícita en cada derecho fundamental para incluirse en el marco del derecho a un proceso justo, abriendo la puerta al estudio de cada caso concreto y una suerte de juicio de proporcionalidad *ex post*. No se trata de una cuestión menor, habida cuenta de la trascendencia que tendría el hecho de que, en la práctica del *ciberpatrullaje*, se hubieran obtenido evidencias de modo ilícito.

A todo lo anterior habrá que añadir, como elemento diferenciador, la nota de la internacionalidad, pues el *ciberpatrullaje* constituye una auténtica manifestación de la posibilidad de actuación global y organizada de las Fuerzas y Cuerpos de Seguridad de los diferentes Estados. A este respecto, existen, como veremos, varios instrumentos supranacionales destinados a homogeneizar y coordinar la capacidad de actuación de dichos cuerpos.

Asimismo, debemos recordar que el medio virtual ha incorporado modificaciones sociales a un ritmo vertiginoso (aunque las nuevas modalidades delictivas y la necesidad de extraer elementos indiciarios de delito de soportes informáticos son sólo una manifestación más de la nueva dimensión a la que se ha visto abocada nuestra realidad social), muy superior a la ya de por sí demorada capacidad del ordenamiento jurídico para adaptarse a la realidad social, de manera que nuestro ordenamiento jurídico ha quedado completamente desbordado, apareciendo lagunas que es necesario colmar.

A ese respecto, el voluntarismo judicial, sobradamente reconocido por la doctrina e incluso por la jurisprudencia europea, ha quedado sustituido, finalmente, con ocasión

de la Ley Orgánica 13/2015, de 5 de octubre[24], por la expresión del legislador, que ha reaccionado más tarde que pronto (y de un modo no exento de reproches, tanto nacionales como internacionales), ante la realidad innegable de que sus preceptos no cumplían con la exigencia de contar con una previsión legal suficiente que amparase las actividades de investigación de las Fuerzas y Cuerpos de Seguridad, Ministerio Fiscal y Poder Judicial ordenada a la obtención lícita de pruebas.

En fin, el entorno tecnológico se plantea como un escenario de conflictos de notable trascendencia, habida cuenta de la dimensión superior de los intereses que eventualmente pueden entrar en colisión: de un lado, nos hallamos con el ejercicio de la libertad –referida en términos generales– por parte de los ciudadanos, así como con las legítimas expectativas de privacidad en los individuos cuya idiosincrasia se ve afectada, de un modo u otro, por el medio virtual; de otro, encontramos el interés público que persigue la constante protección del orden público y, más en concreto, de otros bienes jurídicos igualmente relevantes, frente a comportamientos antisociales o que nieguen su valor. Las tesis abstencionistas, que concebían internet como un espacio que podía mantenerse expedito de toda intervención pública, han quedado superadas frente a la constatación de que se trata, en definitiva, de comportamientos humanos y, por tanto, precisan de un tratamiento jurídico particular y consecuente con sus reseñables peculiaridades.

Puesto que en el proceso penal resultan afectados derechos fundamentales de los sujetos implicados, deben exigirse una serie de garantías que limiten las actividades de investigación que se desarrollan en la fase de instrucción. Tras constatarse la existencia de dos intereses (el de la búsqueda de la verdad y correspondiente sanción de las conductas punibles, por un lado, y el del respeto a los intereses y garantías fundamentales de los ciudadanos que no deberían verse afectados por una investigación penal, por otro)[25], se hace imprescindible la búsqueda de un equilibrio entre ambos, servicio al que, en definitiva, nos hemos encomendado.

---

[24] CALVO LÓPEZ, D., "Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (apartados K) a M) del art. 588 ter de la LECrim)", en *Jornadas de Especialistas celebradas en el Centro de Estudios Jurídicos de Madrid*, Madrid, 2017.

[25] NADAL GÓMEZ, I., "El Régimen de los hallazgos casuales en la Ley 13/2015, de modificación de la ley de Enjuiciamiento criminal", *Revista General de Derecho Procesal*, 40, 2016, Iustel, p. 22.

4. METODOLOGÍA EMPLEADA Y LÓGICA INTERNA DE LA INVESTIGACIÓN

En nuestra investigación hemos perseguido superar la perspectiva de una tesis doctoral que suponga única y exclusivamente una recopilación de la doctrina más autorizada que pueda existir sobre la materia objeto de investigación.

Hemos procedido de ese modo por dos motivos fundamentales: el primero, el respeto que nos merece el concepto mismo de investigación doctoral, en la que, entendemos, el investigador adquiere un especial compromiso por enriquecer el acervo científico de una forma que vaya más allá de la depuración y cohesión de fuentes doctrinales (por más útil y loable que puedan resultar este tipo de trabajos, de los que también tiene buena parte esta investigación). En segundo término, el escaso número de fuentes doctrinales que abordan el estudio del ciberpatrullaje nos ha obligado a consentirnos, forzosamente, una mínima originalidad.

Así, en nuestra investigación, nos hemos servido de las siguientes fuentes de información: i) manuales, monografías y artículos doctrinales: con carácter principal, pues, a pesar de que queramos evitar hacer una mera recopilación, hemos tenido que apoyarnos y formarnos con la doctrina que existe sobre la materia; ii) legislación vigente, en tanto que carecería de sentido, dado el programa de doctorado en el que se inserta esta investigación, no atender al marco normativo nacional e internacional; iii) pronunciamientos judiciales y de otros organismos, pues hemos procurado atender a la praxis de nuestros tribunales –en donde el derecho procesal se materializa– y a la de otros organismos, tanto nacionales como internacionales; iv) conferencias, charlas y coloquios, en los que hemos procurado asistir y participar, cuanto menos, por vía telemática; v) otros materiales escritos, como reflexiones de algunas personalidades en materia de privacidad, hojas de ruta y declaraciones de intenciones de compañías y fundaciones vinculadas materialmente al ámbito de trabajo de la investigación, etc.; vi) entrevistas con profesionales del sector, personalidades y especialistas en la materia, sea de manera presencial o telemática; vii) datos recabados en materia de las actividades de ciberpatrullaje, así como de los portales de transparencia de las principales sociedades de servicios de información vinculadas por el deber de colaboración.

Especialmente interesante hubiera resultado poder contar con información obtenida de primera mano a través de los Fuerzas y Cuerpos de Seguridad del Estado. No obstante, estos han expresado la imposibilidad de trasladarnos información al respecto.

5. ESTRUCTURA DE LA TESIS DOCTORAL Y CONCLUSIÓN CENTRAL

El presente trabajo de investigación está dividido en seis bloques, orientados todos ellos a la persecución de la finalidad referida: analizar si existe riesgo de vulneración de los derechos fundamentales de los investigados con ocasión de la actividad autónoma de las Fuerzas y Cuerpos de Seguridad del Estado en materia de ciberpatrullaje.

En el capítulo I, que es el que nos ocupa, desarrollamos la introducción de la investigación, en los términos expuestos al principio, procurando introducir al lector en el trabajo realizado, así como justificar el objeto de la investigación y presentar el estado de la cuestión.

En el capítulo II nos referimos a varias cuestiones introductorias que consideramos de trascendental importancia para abordar el objeto de investigación. Así, nos referimos a los conceptos de ciberespacio y ciberdelincuencia, a los diferentes niveles de acceso y publicidad existentes en internet, a las notas características de la ciberinvestigación, a los caracteres de la prueba digital, al contenido de la reforma operada por la Ley Orgánica 13/2015 y a los derechos fundamentales que pueden resultar afectados con ocasión de dicha adopción, con especial énfasis en la actualidad de la prueba ilícita, según los pronunciamientos más recientes de nuestro Tribunal Constitucional, así como al reciente Anteproyecto de LECrim de 2020.

En el capítulo III nos ocupamos directamente de la actividad de *ciberpatrullaje* de las Fuerzas y Cuerpos de Seguridad del Estado, esto es, la actividad de carácter preprocesal que realizan en el marco de prevención delictiva en el ciberespacio. Así, nos referimos al concepto de ciberpatrullaje y su previsión en el ordenamiento jurídico, a la figura de la inteligencia sobre fuentes abiertas, al conjunto de técnicas o recursos conocidos que emplea para ello y, finalmente, a la cooperación supranacional en dicha materia.

En el capítulo IV estudiamos con detenimiento las diligencias de investigación tecnológica que, aunque no constituyen una investigación de fuentes abiertas –lo que constituye, en términos estrictos, la figura del *ciberpatrullaje*– pueden desarrollarse por la Policía Judicial y el Ministerio Fiscal de manera autónoma, sin necesidad de autorización judicial, o con carácter previo a una autorización judicial, que legitimaría la injerencia tras su verificación en supuestos de urgencia. Distinguimos entre aquellas diligencias que pueden realizar de manera autónoma, en todo caso, de aquellas otras que pueden

realizar sin autorización judicial exclusivamente en supuestos de urgencia. Analizamos también –aun someramente, por exceder del objeto prioritario de estudio– la figura del agente encubierto informático y los hallazgos casuales.

En el capítulo V, nos referiremos a las figuras de la retención de datos y del deber de colaboración que pesa sobre prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, para prestar toda la asistencia e información que sean precisos al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial.

Finalmente, en un capítulo diferenciado recopilamos y exponemos las conclusiones extraídas de la investigación y apuntamos posibles líneas de investigación futura.

6. AGRADECIMIENTOS

Queremos finalizar esta introducción formulando nuestro más sincero y debido agradecimiento a todas aquellas personas que han hecho posible la realización de esta tesis doctoral, sin cuyo impulso, constancia y entendimiento este fruto no habría sido posible.

También tenemos que agradecérselo a quienes promovieron la presentación de solicitud de admisión en el programa de doctorado, gracias al cual hemos descubierto un mundo entero de posibilidades nuevas y cuestiones sin resolver.

Igualmente, hay que expresar nuestro agradecimiento a quienes soportaron mis vaivenes, y a quienes contribuyeron a la formación y el mantenimiento en mi persona de la voluntad de hacer el doctorado.

En especial, a quienes mantuvieron conversaciones al respecto, a quienes atendieron dudas sencillas y complejas, a quienes se mostraron flexibles y comprensivos cuando era necesario, y firmes el resto del tiempo. También, a quienes valoraron la esencia de la investigación, prestaron las herramientas necesarias y la vieron escribirse.

Especialmente, a la profesora Dra. Dª. Pilar Martín Ríos, por su amable tutela e ilustre dirección, y al profesor Dr. D. José de los Santos Martín Ostos, por recomendarme ante ella.

Finalmente, a quienes tengan la deferencia de evaluarla.

A todos ellos, gracias.

CAPÍTULO II
LA ACTIVIDAD INVESTIGADORA EN EL CIBERESPACIO: CUESTIONES INTRODUCTORIAS

En este apartado queremos presentar algunos conceptos que se han revelado como fundamentales para avanzar en la investigación. De esa manera, no constituyen elemento central del trabajo, pero sí suponen una base sobre la que el mismo ha sido construido y dirigido, y que en todo caso resultan esenciales para situar la problemática que hemos tratado de abordar.

1. EL CIBERESPACIO Y LA DELINCUENCIA

Como hemos visto, el *ciberespacio* es un medio que surge con la propia existencia de internet, posibilita la conectividad universal y facilita el libre flujo de información, servicios e ideas, estimula el emprendimiento y el crecimiento socioeconómico, y transforma a escala global y a un ritmo vertiginoso[26] los procesos productivos, especialmente con las nuevas herramientas de inteligencia artificial, robótica, *big data*, *blockchain* e *internet of things*.

No obstante, sus implicaciones van más allá de la dimensión tecnológica e influyen en la vida social hasta el punto de ser origen de propuestas de nuevos modelos sociales, políticos y éticos. De esta forma, son múltiples las facetas que presenta el ciberespacio y, en consecuencia, múltiples también las perspectivas que pueden desplegarse sobre el mismo.

De esta manera, y sin ir más lejos, en la estrategia nacional de ciberseguridad, el *ciberespacio* se entiende como "un campo de batalla donde la información y la privacidad de los datos son activos de alto valor en un entorno de mayor competición geopolítica, reordenación del poder y empoderamiento del individuo"[27], saltando a la vista así el énfasis público en el entendimiento del ciberespacio como un espacio de soberanía, con recursos disponibles para ser explotados e intereses merecedores de protección.

---

[26] Según datos disponibles en Eurostat, el 89% de la población europea utiliza internet, según consulta disponible en https://ec.europa.eu/eurostat/databrowser/view/tin00028/default/table?lang=en, fecha de consulta 16 de junio de 2022.

[27] "Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.".

De igual modo, tampoco escapa a nadie, por su condición de nuevo medio para el desarrollo de la sociedad, que el ciberespacio alberga también nuevas formas de criminalidad, que ha venido recibiendo la denominación de *cibercriminalidad*. En relación con las conductas delictivas, el ciberespacio, a su vez, se caracteriza por su inherente ausencia de soberanía, su débil ejercicio de la jurisdicción, la facilidad de acceso a los comportamientos delictivos y la dificultad de atribución de la autoría de las conductas que en él se desarrollan.

La magnitud cuantitativa y cualitativa de los daños que originan los *ciberdelito*s es innegable, como lo es su potencialidad global para afectar sobre la economía y el desarrollo tecnológico de todo el mundo. Debe tenerse en cuenta que esta capacidad no es una mera consecuencia de la interconexión global de hoy en día entre las economías, mercados y culturas, sino que es un elemento intrínseco a la propia naturaleza de una actividad ilícita que se desarrolla en un medio para el que el diámetro de nuestro planeta, al completo, apenas puede suponer unos milisegundos de diferencia. Es completamente lógico que acciones que tienen la capacidad de afectar a todo el planeta tengan que desplegar efectos de escala mundial.

Desde otra perspectiva, el Comité del Convenio sobre Cibercrimen del Consejo de Europa se hace eco de la incidencia de este fenómeno delictivo sobre la privacidad, la dignidad e integridad de las personas, la libertad de expresión, las instituciones, la estabilidad democrática, y demás bienes, principios e intereses considerados de especial protección en los Estados de Derecho modernos[28]. En España, la creciente preocupación por este fenómeno ha impulsado la creación del Consejo Nacional de Ciberseguridad, con funciones de coordinación en esta materia a nivel estatal[29].

La doctrina, apoyándose en estudios realizados por diversas instituciones, ya ha distinguido un doble impacto de la ciberdelincuencia. Por un lado, encontraríamos el coste económico directo y mensurable, computado en función del perjuicio que ocasionara a las víctimas, que ya en 2013 se admitía entre los 100.000 y 500.000 millones de

[28] Informe explicativo disponible en https://rm.coe.int/16802fa403#:~:text=El%20Convenio%20tiene%20como%20finalidad,para%20la%20investigaci%C3%B3n%20y%20el, fecha de consulta 16 de enero de 2020.

[29] Creado mediante la Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad.

dólares[30]. Por otro lado, incluso con mayor trascendencia a la hora de determinar el impacto real de las formas de cibercriminalidad en nuestra sociedad, también se atiende a los efectos indirectos, como son las interrupciones de los servicios, la disminución de la confianza de las actividades en línea, el coste de protección de las redes, de seguros y de trabajos de recuperación de ataques informáticos, así como el daño reputacional a la marca de la empresa atacada. Los costes del cibercrimen crecen un 15% anual a nivel global y ya genera más beneficios que el narcotráfico, según Interpol[31]. Junto a lo anterior, quizás sería debido reconocer, igualmente, que un nuevo mercado de productos y servicios, el de la seguridad informática, surge por la propia existencia del peligro del cibercrimen y los ciberataques[32].

En todo caso, ya en 2013, los usuarios de internet en la UE expresaban su preocupación por la seguridad cibernética. En una encuesta realizada a más de 27.000 personas de los Estados miembros de la UE, el 76 %[33] consideraba que en el último año había aumentado el riesgo de ser víctima de un delito informático y, si bien el 70 % de los usuarios de internet en toda la UE confiaban en su capacidad para realizar operaciones bancarias o compras en línea, únicamente en torno al 50 % optaban realmente por hacerlo.

Muchos incidentes podrían prevenirse si los usuarios adoptasen una serie de medidas sencillas y poco costosas. En particular, el 87 % de los encuestados evitaba desvelar datos personales en línea, el 52% seguía sin considerarse informado sobre los riesgos de la ciberdelincuencia, y el 12 % había sido víctima de ataques en su correo electrónico o red social. Paralelamente, ya entonces había aumentado el número de usuarios que accedían a internet a través de *smartphones* o *tablets*. En palabras de la comisaria de Asuntos

---

[30] "The Economic Impact of Cybercrime and Cyber Espionage", disponible en The Economic Impact of Cybercrime and Cyber Espionage | Center for Strategic and International Studies (csis.org), fecha de consulta 16 de enero de 2020.

[31] Como se indica en https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbH1czUwMDAytDA3MzRVK0stKs7Mz7M1MjAyMjAzNAYJZKZVuuQnh1QWpNqmJeYUpwIAuQrogzUAAAA=WKE, fecha de consulta 14 de julio de 2022.

[32] En 2021 fue valorado en 150.370 millones de dólares, y se espera un valor estimado de 317.020 millones de dólares, según datos disponibles en https://www.mordorintelligence.com/industry-reports/cyber-security-market#:~:text=Market%20Overview,personal%20data%20from%20cyber%2Dattacks, fecha de consulta 16 de junio de 2020. Rosa Díez Moles, directora general del INCIBE, ha destacado que es un mercado en auge en nuestro país, con un crecimiento anual de más de un 8%, lo que supone una gran oportunidad de negocio que nos puede situar en primera línea, sólo detrás de USA y China, tal y como se indica en https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbH1czUwMDAytDA3MzRVK0stKs7Mz7M1MjAyMjAzNAYJZKZVuuQnh1QWpNqmJeYUpwIAuQrogzUAAAA=WKE, fecha de consulta 14 de julio de 2022.

[33] "Una nueva encuesta revela las inquietudes de los ciudadanos de la UE ante la ciberdelincuencia", en https://ec.europa.eu/commission/presscorner/detail/es/IP_13_1130, fecha de consulta 7 marzo 2020.

de interior[34]: "las amenazas informáticas evolucionan continuamente, socavando la confianza en el mundo digital: surgen nuevos puntos vulnerables, nuevos métodos delictivos, nuevos entornos para delinquir y nuevas víctimas. Estamos decididos a seguir desarrollando nuevas herramientas, nuevos sistemas de cooperación y nuevas medidas para luchar contra ellas […] la ciberdelincuencia sigue afectando negativamente a nuestra economía. Es necesaria la cooperación de todos los actores para dar una respuesta eficaz a este fenómeno, a fin de garantizar que tanto los ciudadanos como las empresas aprovechen al máximo las posibilidades que ofrecen las tecnologías digitales."

En todo caso, la ciberdelincuencia como fenómeno social tiene innegables consecuencias, lo que obliga a no desatender su trascendencia, que aumenta conforme la globalización y la intercomunicación se asientan.

Los primeros escenarios de la delincuencia organizada se focalizan en el fraude en el comercio electrónico y en la banca electrónica, como instrumentos más rápidos para obtener beneficios. Inicialmente, el fraude en el comercio electrónico se centró en duplicar portales de venta que inducían a engaño a las víctimas que abonaban dinero por productos que no recibían. La vida útil de las falsas web era muy breve, suficiente para engañar a unas pocas víctimas que denunciaban el fraude. La incidencia del fraude fue escasa e imputable a delincuentes esporádicos que actuaban de forma independiente. Posteriormente, se adoptó la técnica denominada como *carding*, la compra de productos abonándolos con tarjetas de crédito falsas. Los defraudadores posteriormente revendían los objetos del fraude, a precios muy bajos, para obtener beneficios. La gran mayoría de estos fraudes se dirigieron contra comercios de productos informáticos, de telefonía móvil, con gran salida en el mercado, y billetes de transportes (tren, avión, barco)[35].

A medida que la red se ha hecho más participativa, los usuarios han aprovechado las ventajas que esta les ofrece, y el mundo de las subastas y ventas entre particulares ha experimentado un gran crecimiento[36]. Como no puede ser de otra forma, los delincuentes se han trasladado al nuevo escenario de ventas entre particulares, donde la entrega del

---

[34] *Ibid.*

[35] BARRIO ANDRÉS, M., *Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 10.

[36] Según datos facilitados por la Fiscalía General del Estado, en España tuvieron lugar en 2020 más de 16.900 procedimientos judiciales por ciberdelincuencia, un valor que representa un incremento de un 28,69% con respecto a 2019, como se puede comprobar en https://es.statista.com/temas/3166/ciberdelitos-en-espana/#dossierKeyfigures, fecha de consulta 16 de junio de 2022.

producto casi siempre está supeditada a un previo pago, y el fraude se centra sobre las estafas del vendedor hacia el comprador.

El servicio de banca electrónica que ofrecen las entidades bancarias a sus clientes supone comodidad e inmediatez en las gestiones para los usuarios que hacen uso de él, pero presenta una vulnerabilidad importante, la autenticación del usuario. Inicialmente, los usuarios se identificaban con un sistema de autenticación primario, es decir, con algo que se sabe, un *login* y un *password*, un nombre de usuario y una contraseña. Si esta es conocida por terceros, pueden usurpar nuestra identidad y realizar toda aquella operativa que el banco ofrezca. Ese fue el inicio del fraude bancario. Los delincuentes enviaban correos electrónicos a multitud de usuarios, simulando proceder de la entidad bancaria y requiriendo la conexión al banco para actualizar las contraseñas. Este engaño para hacerse con los datos de identidad online de la banca electrónica se bautizó como *phishing*, del que han surgido varias modalidades:

- *Pharming*, técnica de phishing que consiste en derivar las conexiones a banca electrónica actuando sobre los servidores de resolución de nombres de dominio o DNS. En esencia, consiste en que cuando al navegador web se le indica una dirección web de un banco concreto, en vez de acudir al banco adecuado acude a la que el *pharmer* le ha indicado. Esta resolución falsa de nombres de dominio, que lleva a la víctima a la página web falsa, se puede hacer en «local», actuando sobre el propio ordenador de la víctima a través de un programa malicioso, o en «red», actuando sobre los servidores de DNS, ordenadores que están en la red con la función de indicar el «camino» adecuado para acceder a las páginas web solicitadas.

- *Vishing*, técnica basada en la tecnología de Voz sobre IP (VoIP) que permite hablar por teléfono a través de la red de Internet. Se manipulan ordenadores para que actúen como auténticas centralitas telefónicas, dando una respuesta similar a una central de banco, a través de la cual solicitan al usuario víctima los datos de identidad bancaria o datos de tarjetas de crédito. La forma de inducir al usuario a que efectúe llamada al número de telefonía por VoIP es mediante el envío de mensajes SMS en los que alerta de gastos no realizados, incluyendo en el mensaje el supuesto número para reclamaciones, que no es otro que el de la centralita de VoIP.

- *Smishing*, o *phishing* a través de mensajes SMS de telefonía móvil. Se realiza un spam de SMS supuestamente remitidos desde la entidad bancaria reclamando respuesta por esa misma vía de datos bancarios.

- *Whaling* o *whale phishing* (*phishing* de ballenas). Es una variante de phishing mucho más preparada y dirigida a altos ejecutivos, políticos o empresarios a los que se supone que tienen disponibilidad de cantidades más altas de dinero o manejan información más sensible, y por ellos son objetivos más rentables.

- *Hishing* o *hardware phishing*. Es el *phishing* a través de productos *hardware* que se comercializan con una vulnerabilidad que permite el acceso fácil al equipo de la víctima o que el propio hardware lleva incorporado en su *firmware* el programa malicioso que permite el robo de información bancaria y su remisión a un servidor bajo control de *phisher*.

El crecimiento del *phishing*, derivado de la rentabilidad del delito, tanto en criterios económicos como de impunidad, hace proliferar los grupos organizados que aterrizan en este escenario delictivo. El incremento de grupos en torno al *phishing* les obliga a buscar, entre los ambientes *hackers*, individuos capaces capaz de cubrir sus necesidades. En el entorno del mundo *hacker*, a través de foros o canales temáticos de fraude se empieza a comercializar las herramientas de *phishing*, los troyanos que roban información de las víctimas. Por otro lado, debido a la permanente respuesta del mundo de la seguridad informática y bancaria, el *hacker* está obligado a una constante innovación. Todo el *malware* que desarrolla tiene una vida limitada hasta que es descubierto.

Consecuencia de esta amplia actividad de desarrollo de *malware*, las bandas organizadas empiezan a dejar de tener *hackers* a su servicio, para empezar a contratar servicios que estos venden. Y el *hacker*, de esta forma, se desvincula del hecho delictivo concreto y sólo ofrece el instrumento. El más claro ejemplo de esto es la venta de kits de *phishing* en la que un usuario cualquiera, sin conocimientos avanzados de informática puede adquirir en el mercado del *malware*, un kit que sólo ha de configurar y poner en funcionamiento, para empezar a infectar equipos y obtener información de sus usuarios. Incluso en los acuerdos de servicio por el kit, informan que el desarrollador no se hace responsable del mal uso del programa

También debemos referirnos, siquiera en términos básicos, a las diversas técnicas utilizadas por los ciberdelincuentes para alcanzar sus fines. Aunque estas técnicas están en constante desarrollo, sí se pueden clasificar en función de su núcleo operativo:

- Técnicas de anonimato, como el uso de datos personales falsos imposibles de comprobar, o el empleo de *proxys* o servicios VPN[37], mail anónimo, cibercafés, redes wifi–ajenas carentes de seguridad y programas de encriptación y estenografía.

- *Malware, spyware o adware*[38] que sirven para controlar sistemas ajenos o crear redes de equipos infectados que sirvan a los fines de los ciberdelincuentes, así como diccionarios y programas que emplean la fuerza bruta para colapsar servicios o atacar encriptaciones.

- Técnicas de ingeniería social con la finalidad de suplantar identidades, descubrir contraseñas o utilizar productos bancarios.

- Explotación de *bugs* mediante *exploits* específicamente diseñados para aprovechar las vulnerabilidades existentes en los diferentes programas.

- Técnicas de denegación de servicio, empleadas para interrumpir las funciones ofrecidas por los sistemas informáticos que se desea atacar.

Son igualmente destacables las denominadas *blended threats*, que son ataques novedosos que procuran integrar todas las características de las diferentes técnicas de ataque, con el fin de alcanzar la máxima posibilidad de éxito.[39]

A estas alturas, no debemos dejar de recordar en este punto el carácter relativo del término delincuencia. En efecto, muchas de las técnicas que enumeramos son también empleadas por activistas en Estados con regímenes más autoritarios y limitativos en materia de libertad de expresión, y constituyen elemento indispensable para dichas personas para asegurarse un mínimo anonimato que les proteja de la represalia pública. En estos casos, dichos activistas podrían merecer también, desde la óptica del ordenamiento

[37] Ofertados por compañías radicadas en países que no obligan a prestadores de servicios a trasladar datos a las autoridades, en una clara semejanza al régimen de los paraísos fiscales.
[38] Como son los virus, gusanos, troyanos, rastreadores, bombas lógicas, *botnets, exploits, droppers, rootkits, y ddos.*
[39] QUEVEDO GONZÁLEZ, J., *Investigación y prueba del ciberdelito*, Sepín, Madrid, 2017, p. 65.

jurídico en dichos Estados, el calificativo de "cibercriminales", a pesar de que su conducta pueda tener un componente fundamentalmente de protesta política.

2. LA CIBERCRIMINALIDAD EN ESPAÑA

En España, el Instituto Nacional de Tecnologías de la Comunicación (INTECO), ha realizado diversos estudios del estado de la sociedad de la información en el escenario español, entre los que destacan el *Estudio sobre la seguridad de la información y "eConfianza" de los hogares españoles* y el *Estudio sobre incidencias y necesidades de seguridad en las pequeñas y medianas empresas españolas*[40].

Particularmente interesante resulta el *Estudio sobre la Cibercriminalidad en España*, elaborado anualmente por el Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad del Ministerio del Interior. En particular, en su capítulo 2 (Informe de la sociedad de la Información) trata de trazar y esquematizar un perfil de la sociedad española enlazado al uso de las tecnologías e internet.

En su última entrega, correspondiente al año 2020[41], los datos aportados, procedentes de la Encuesta del Instituto Nacional de Estadística (INE), permiten extraer varias conclusiones. Para empezar, en relación con los hogares y porcentaje de vivienda que tiene o no tiene acceso a internet, los estudios revelan que el porcentaje de viviendas que poseen ordenador y las que disponen de acceso a internet se ha incrementado en 2020 con respecto al año 2019, siguiendo de esta forma la tendencia general experimentada en la serie histórica que se representa (2011–2020). Además, se puede observar que los índices sobre las viviendas que poseen o no dispositivos de esta naturaleza, así como la existencia de que estas estén conectadas a internet, es más elevado, en ambos casos, cuanto mayor es la población de la localidad en la que se ubican los hogares.

Asimismo, en relación con el perfil del ciudadano ante la sociedad de la información, resulta que, los grupos de edad más temprana son los que más hacen uso de las tecnologías. En este sentido, el 99,8 % de los jóvenes, entre 16 a 24 años, afirman haber accedido a la Red en los últimos tres meses, porcentaje que se reduce a un 69,7% entre las personas con edades comprendidas entre los 65 y 74 años. Si bien, la mayoría de los porcentajes de los rangos de edad que comprende este análisis han experimentado un

[40] Disponible en https://docplayer.es/4243695-Estudio-sobre-la-seguridad-de-la-informacion-y-la-e-confianza-de-los-hogares-espanoles.html, fecha de consulta 16 de junio de 2022.
[41] GUTIÉRREZ, J. L. Y OTROS, "Estudio sobre la Cibercriminalidad en España", p. 18.

incremento con respecto a 2019, siendo el incremento más acusado en la edad de 65 a 74 años. Se iguala, además y por segunda vez en la serie histórica, el porcentaje de uso de internet entre mujeres y hombres.

De igual modo, en cuanto al perfil del menor de edad ante la sociedad de la información, es de destacar el porcentaje de los menores de edad (10 a 15 años) que han utilizado un ordenador y han accedido a internet en los tres últimos meses, que se sitúa en el 91,5% y 94,5, respectivamente. En cuanto a la distinción por sexos, las niñas tienen porcentajes marginalmente más altos que los niños, en lo que se refiere al uso de ordenador (92,3% frente al 90,8%) y acceso a internet (95,7% frente al 93,4%). Por grupos o rangos de edad, son las personas con edades comprendidas entre los 25 y 34 años las que realizan más compras a través de internet (73,2%). Por otro lado, las personas de 65 a 74 años muestran que sólo el 20,5% realiza compras por internet.

El informe también se refiere al perfil de las personas que compran por internet. Así pues, se puede apreciar que desde el año 2011 el comercio electrónico se ha llegado casi a triplicar, puesto que el 53,8 % de las personas encuestadas en 2020 reconocen haber realizado alguna compra empleando esta vía, mientras que en el año 2011 solo lo hacían el 18,6%. Por sexo, los hombres muestran mayores cifras porcentuales que las mujeres (54,3% frente al 53,4%), aunque esta diferencia con el paso de los años se viene reduciendo paulatinamente.

Asimismo, el referido *Estudio sobre la Cibercriminalidad en España* también contiene algunos datos estadísticos en materia de cibercriminalidad, obtenidos a partir del Sistema Estadístico de Criminalidad (SEC), que se compone de la Base de Datos que registra las actuaciones policiales, regido a su vez por la Instrucción núm. 1/2013, de la Secretaría de Estado de Seguridad, sobre la Estadística Nacional de Criminalidad.

En el periodo comprendido entre 2016 a 2020, ha tenido lugar un aumento de los delitos informáticos. De esta forma, podemos apreciar que, en 2020, se ha conocido un total de 287.963 hechos, lo que supone un 31,9% más con respecto al año anterior. De esta cifra, el 89,6 % corresponde a fraudes informáticos (estafas) y el 4,9% a amenazas y coacciones. Actualmente, la importancia de la Cibercriminalidad va creciendo año tras año, como se demuestra con el aumento del número de hechos conocidos. Otro efecto imposible de obviar es el peso proporcional que adquiere en el conjunto de la criminalidad, pues se ha pasado de un 4,6% en el año 2016 al 16,3% en el año 2020. En relación

al porcentaje de hechos esclarecidos, en el año 2020, este supone el 14,0% del total de los hechos conocidos. Por otra parte, los detenidos e investigados han alcanzado la cifra de 11.280, de los que el 73,3% corresponden a personas de sexo masculino; teniendo lugar, principalmente, por la comisión de fraudes informáticos, delitos de amenazas y coacciones, y delitos sexuales. La mayoría de las detenciones/investigaciones de personas de sexo femenino se han llevado a cabo por fraudes informáticos, amenazas y coacciones, y por el delito de falsificación informática.

La distribución de la ciberdelincuencia, desde el punto de vista geográfico, a lo largo de 2020, sitúa a Cataluña, Madrid, Andalucía y Comunitat Valenciana entre las Comunidades Autónomas que concentran más infracciones penales en este ámbito. A nivel provincial, se encuentran a la cabeza Madrid, Barcelona, Valencia, Illes Balears, Bizkaia y Sevilla.

En 2020, las victimizaciones que han sido registradas por las Fuerzas y Cuerpos de Seguridad suman un total de 215.507, es decir, un 29,7% más que en el año 2019. La mayoría de las víctimas de ciberdelincuencia pertenecen al sexo masculino (51,8%), tienen mayoritariamente entre 26 y 40 años, y son objeto, principalmente, de los delitos de fraudes informáticos, amenazas y coacciones, así como falsificación informática. Sin embargo, si se analiza la distribución global de incidentes conocidos por ámbito y sexo, las mujeres exceden en porcentaje a las víctimas de sexo masculino cuando se trata de hechos relacionados con el acceso e interceptación ilícita, falsificación informática y los delitos sexuales. Además, se aprecia que, en 2020, el 30,7 % del conjunto de las víctimas recae sobre el grupo de edad de 26 a 40 años. Siendo este grupo de edad el mayoritario tanto para las víctimas de sexo masculino como femenino.

Por último, en dicho informe también se llama la atención sobre que las víctimas menores de edad son más vulnerables a otro tipo de hechos delictivos, en concreto a las amenazas y coacciones y delitos sexuales.

3. ALGUNOS CONCEPTOS PREVIOS: INTERNET, SURFACE WEB, DEEP WEB Y DARK WEB

Algunos de los principales conceptos introductorios que es necesario manejar son los de *surface web*, *deep web* y *dark web*[42]. Cada término se refiere a una parte del *World Wide Web*, o "la web" o "internet" en general.

La *surface web*, también llamada *Visible Web, Indexed Web, Indexable Web or Lightnet*, o internet superficial, es la parte de la *world wide web* (o de *internet*, en general) que se encuentra disponible al público en general y es *indexable* por los motores de búsqueda tradicionales, que pueden acceder fácilmente a dichas web. Se dice que la *surface web* representa tan sólo el diez por ciento de la información verdaderamente existente en internet.

La *deep web*, o internet profunda, por su parte, es aquella parte de la *world wide web* compuesta por sitios web que están disponibles para el público en general –es decir, no son necesarias claves especiales para acceder–, pero a los que solo se puede acceder si se conoce su dirección o URL, porque no se encuentran indexadas por los motores de búsqueda. Puede entenderse que los titulares de esta información no desean restringir el acceso a la misma, pero sí su difusión y trazabilidad. Aunque no lo parezca, hay muchas actividades legales que se desarrollan en Deep Web. Es un recurso útil para multitud de información. Por ejemplo, hay bases de datos con librerías académicas virtuales y con versiones antiguas de páginas web.

Por ello se ha dicho que, normalmente, en esta parte de internet se pueden encontrar cuestiones relacionadas con el contrabando, el cibertráfico de personas o el terrorismo y, en general, cualquier forma de cibercriminalidad. Deep Web se refiere a cualquier contenido de Internet que, por diversos motivos, no puede ser indexado por los buscadores. Incluye páginas web dinámicas, sitios bloqueados (como los que requieren responder un CAPTCHA para acceder), sitios no enlazados, contenidos que no son HTML, contextuales o con scripts, y redes de acceso limitado. Las redes de acceso limitado están formadas por nombres de dominio registrados en sistemas de nombres de dominio (DNS) no gestionados por ICANN (Internet Corporation for Assigned Names and Numbers) y por direcciones URL (Uniform Resource Locator) con dominios de primer nivel o TLD (Top-

[42] ECIJA BERNAL, Á., "Ciberespacio, Dark Web y Ciberpolicía", *Diario La Ley*, 8940, 2017, Wolters Kluwer, p. 2.

Level Domains) no estandarizados que generalmente requieren un servidor DNS específico para resolver correctamente. Un ejemplo de redes de acceso limitado son los sitios con dominios registrados en sistemas distintos del estándar DNS, como los .BIT. Bajo la categoría de redes de acceso limitado también se encuentran las Darknets o sitios alojados en infraestructuras que requieren el uso de software específico como Tor para acceder[43].

Ahora bien, es necesario tener presente la diferencia entre comportamiento ilícito y comportamiento ilegítimo, pues no son pocos los casos en los que, en otros Estados con menos garantías en materia de derechos y libertades, la sociedad civil acude a las herramientas de la *deep web* para poder expresarse, organizarse y actuar con menor probabilidad de sufrir la acción represiva del poder establecido. Puede decirse, en ese sentido, que la *deep web* es un instrumento para actuar de manera clandestina respecto del poder establecido, con independencia de cuál sea el contenido de dicha actuación clandestina.

Por último, la *darkweb* o *darknet* es aquella parte de la *world wide web* compuesta por sitios web que, no estando indexados en motores de búsqueda tradicionales, exigen además una acreditación específica para su acceso. Por tanto, los titulares de este tipo de información no sólo desean reducir su difusión y trazabilidad, sino también el acceso a ella. Como sucedía con la *deepweb*, supone un instrumento para actuar al margen del poder establecido cuyo contenido puede ser variable, incurriendo tanto en las conductas más execrables como en otras quizás amparadas desde el punto de vista del derecho natural. Dark Web se refiere a cualquier página web que se oculta a plena vista o que reside dentro de una capa pública pero separada de la Internet estándar. Por ejemplo, una página web que carece de enlaces de entrada, de manera que ni los usuarios ni los motores de búsqueda pueden localizarla. Las Darknets modernas necesitan software específico para usar la red distribuida. Hoy en día los ejemplos más notables son Tor, I2P (Invisible Internet Project) y Freenet. La arquitectura fluida de estas redes complica estimar su tamaño, pero parece que Tor es la más grande con I2P a bastante distancia[44].

Desde el punto de vista de la seguridad y la prevención de la delincuencia, la *Deep web* y la *dark web* suponen una fuente muy importante de ciberinteligencia, y en especial sobre amenazas, vulnerabilidades y riesgos. Las principales técnicas empleadas por la

---

[43] IBÁÑEZ, E. M., "Dark Web y Deep Web como fuentes de ciberinteligencia utilizando minería de datos", *Cuadernos de la Guardia Civil: Revista de seguridad pública*, 54, 2017, Dirección General de Estadística, p. 75.
[44] *Ibid.*, p. 76.

policía para obtener dicha inteligencia son las arañas (crawlers) para Deep Web, los sistemas de detección y prevención de intrusiones (IDPS) y la detección de comunidades virtuales[45].

4. LA RELEVANCIA Y COMPLEJIDAD DE LA INVESTIGACIÓN DE LA CIBERDELINCUENCIA

A. UN FENÓMENO EN CRECIENTE E IMPARABLE AUMENTO

Podemos definir el fenómeno de la cibercriminalidad como aquel conjunto de actividades ilícitas cometidas en el *ciberespacio* que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas.

La cibercriminalidad ha sido reconocida como un problema de seguridad ciudadana de primer orden, representando una de las amenazas más extendidas y generalizadas de nuestra actualidad, con apariciones constantes y afectando cada vez de manera más importante a miles de instituciones, empresas y ciudadanos. En particular, las nuevas modalidades de transacción financiera y económica, como las criptomonedas, suponen un novedoso riesgo para el tráfico y el comercio de bienes. Por otro lado, la prestación de servicios ilícitos o la extorsión, el fraude y la falsificación de medios de pago no monetarios, constituyen un serio desafío por su sofisticación y complejidad. Estos pueden ser utilizados en el blanqueo de capitales y la evasión de impuestos y representan una fuente de ingresos para el crimen organizado y por lo tanto son facilitadores de otras actividades como la financiación del terrorismo, que toma provecho de la dificultad de seguimiento que estas nuevas técnicas ofrecen.

En función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de los daños infligidos, se distingue entre ciberterrorismo, *ciberdelito*, y *hacktivismo*. Los ciberdelincuentes operan bajo esquemas de crimen organizado y continúan explorando técnicas sobre las que construir modelos de negocio lucrativo y de bajo riesgo, amparados por la difícil trazabilidad de sus acciones. Los grupos terroristas tratan de aprovechar las vulnerabilidades del *ciberespacio* para reclutar seguidores o realizar atentados, sean cibernéticos o puramente materiales. Por último, los grupos *hacktivistas* realizan ciberataques por razones ideológicas y, aprovechándose en ocasiones de productos,

[45] *Ibid.*, p. 89.

servicios y herramientas disponibles en el *ciberespacio*, buscan desarrollar ataques con un gran impacto mediático o social.[46]

Son múltiples los trabajos de investigación que identifican las características fundamentales de los *ciberdelito*s, de las pruebas tecnológicas y del dato digital. En nuestra investigación hemos considerado oportuno aportar una refundición de dichos caracteres –según han sido apreciados por los investigadores– desde la óptica de las diligencias de investigación que puede adoptar la Policía Judicial sin necesidad de autorización judicial previa. Esa intención lleva a atender, por un lado, al fenómeno de la ciberdelincuencia, en tanto realidad social objeto de la actividad policial de averiguación; y por otro, al dato digital, en tanto vestigio dejado por dicha actividad de ciberdelincuencia. El hecho de que ambos conceptos compartan un mismo medio –el *ciberespacio*– y que, al menos en lo que refiere a este trabajo, sean abordados desde una misma perspectiva –la de la investigación policial– obliga a estudiar sus caracteres desde un punto de vista unificado y homogéneo, de manera que eso es lo que hemos pretendido.

Tal similitud de naturaleza se pone de manifiesto cuando se comparan las características definitorias de la cibercriminalidad y del dato digital, según son identificadas por la doctrina. Así, por ejemplo, respecto de la cibercriminalidad se dice que se caracteriza por las siguientes notas[47]: 1) la magnitud de los daños que origina y su incidencia potencialmente global sobre la economía y el desarrollo tecnológico, 2) la facilidad comisiva, si se dispone de los suficientes conocimientos técnicos, 3) su elemento transnacional, 4) el alto grado de impunidad de que disfruta, fundamentalmente derivado de la problemática burocrática que plantea, y 5) la necesidad de que las entidades públicas y privadas de diferentes jurisdicciones colaboren entre sí.

Por otro lado, respecto del dato digital viene a afirmarse que es una fuente de prueba que se caracteriza por 1) su heterogeneidad, 2) su volatilidad o fácil manipulación, 3) la existencia de una huella digital, 4) su ubicuidad, 5) la posibilidad de generar "falsos positivos" y 6) su carácter eminentemente público, en la medida en que gran parte de ellos es de libre acceso en la red abierta.

---

[46] "Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.".

[47] CABEZUDO RODRÍGUEZ, N., "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal", cit., p. 11.

Nosotros, fusionando ambos elementos, proponemos los siguientes caracteres definitivos del ámbito *cibernético*, en lo que se refiere a las diligencias de investigación tecnológica, que exponemos en los siguientes puntos.

B. LA COMPLEJIDAD DE SU INVESTIGACIÓN

Una de las principales características de la cibercriminalidad es la elevada complejidad que alcanzan las diligencias de investigación tecnológicas, a la vista de la naturaleza del propio dato digital.

Uno de los elementos significativos de la prueba tecnológica es la gran variedad de hechos y métodos de investigación que pueden tener lugar, lo que se une también a la gran disparidad de tecnologías de información y comunicación que permiten su realización.

En ese sentido, pueden constituir fuentes de prueba tecnológica el contenido de una página web –alojado en la memoria de un servidor cuya ubicación física puede ser global–, mensajes enviados por aplicaciones de mensajería instantánea (texto, audio, fotografías o vídeos), actividad en una red social, fotografías digitales, la información extraída por drones, datos personales difundidos a través de internet, correos electrónicos, pero también otros datos menos tradicionales, como IP de dispositivos, metadatos, registros log, y otra serie de evidencias más sobre actividades respecto del propio medio virtual que sobre el medio físico al que se puedan referir.

En definitiva, la diversidad de pruebas tecnológicas existentes conlleva que el tratamiento de cada una de ellas pueda ser diferente, en tanto en cuanto su obtención puede afectar a derechos fundamentales distintos; pueden practicarse por medios diferentes y su valoración puede variar. Ello hace extraordinariamente difícil el establecimiento de unos criterios procesales homogéneos para su tratamiento y valoración cuando se aportan como prueba en un proceso, a fin de acreditar el contenido de una comunicación determinada.[48]

Otra característica fundamental de las pruebas tecnológicas es que son fácilmente manipulables. A este respecto, la doctrina concluye que "los datos pueden ser fácilmente modificados, sobrescritos o borrados, lo que determina un peligro evidente de

[48] FUENTES SORIANO, O.; DOMENECH FEDERIC, A., *El proceso penal: cuestiones fundamentales*, Tirant lo Blanch, Valencia, 2017, p. 277.

manipulación de las pruebas"[49]. Esta interpretación ha sido confirmada por multitud de pronunciamientos doctrinales al respecto[50], que defienden la necesidad de disponer de informes periciales para traer al proceso toda realidad contenida en un dato informático.

En todo caso, la STS 300/2015, de 19 de mayo, concluía que "la posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo". Esta sentencia, ampliamente comentada por la doctrina, reconoce la posibilidad de que cualquier persona con conocimientos tecnológicos suficientes elabore fuentes de prueba tecnológica falsas *ad hoc* para afectar al enjuiciamiento de un asunto determinado y, correlativamente, exige prudencia ante la valoración de una prueba tecnológica[51].

En este sentido, es desde luego perfectamente posible alterar mensajes de *Whatsapp* o de otras aplicaciones de mensajería instantánea, simular existencia de conversaciones o, incluso, las geolocalizaciones de terminales. No obstante, a nuestro juicio, la alegada facilidad de manipulación se debe más bien al desconocimiento del destinatario de la prueba que a la propia facilidad o carencia de rastro. En los soportes magnéticos queda, en efecto, rastro de las modificaciones efectuadas, dejando a salvo niveles profesionales de manipulación que, en todo caso, también se verifican en el medio físico tradicional respecto de otras pruebas.

Esta facilidad de manipulación ha provocado que de la prueba tecnológica se diga que es naturalmente volátil, pues, la información o datos relevantes son mudables y sometidos a constante cambio, especialmente en relación con los contenidos de Internet[52], como característica íntegramente vinculada a la facilidad de manipulación[53]. Precisamente esta inherente volatilidad es lo que hace surgir la necesidad de que las actuaciones

---

[49] DELGADO MARTÍN, J., "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015", *Diario La Ley*, 8693, 2016, Wolters Kluwer, p. 3.
[50] ORTIZ PRADILLO, J. C., *Problemas procesales de la ciberdelincuencia*, Colex, Majadahonda (Madrid), 2013.
[51] BUENO DE MATA, F., "La validez de los «screenhots» o «pantallazos» como prueba electrónica a tenor de la jurisprudencia del Tribunal Supremo", en *Los desafíos de la justicia en la era post crisis, 2016, pp. 141–152*, Atelier, 2016, p. 4.
[52] DELGADO MARTÍN, J., "La prueba digital. Concepto, clases, aportación al proceso y valoración", *Diario La Ley Ciberderecho*, 6, 2017, Wolters Kluwer, p. 1.
[53] PINTO PALACIOS, F., *La prueba en la era digital*, La Ley Wolters Kluwer, Madrid, 2017, p. 28.

deban dirigirse a conseguir la preservación de la fuente de prueba, evitando posibles alteraciones o contaminaciones[54].

La información generada por medio de dispositivos tecnológicos es compleja y volátil, en tanto en cuanto sus autores pueden destruir la información con la misma rapidez con la que la han creado[55], lo que lleva a que se aconseje asegurar la prueba por medio de su preconstitución o anticipación[56].

Brevemente, merece la pena señalar que la singularidad de la prueba anticipada reside en que la práctica de la misma se desarrolla en un momento anterior a la apertura de la fase probatoria del procedimiento, que en el proceso penal se encuadra en el juicio oral, mientras que la prueba preconstituida se caracteriza porque la práctica de la prueba no tiene lugar ante el órgano enjuiciador, sino ante el órgano instructor, con lo que la inmediación como tal desaparece y queda sustituida por el soporte en que se documente y refleje el resultado de dicha práctica anticipada de la prueba. En general, para que las pruebas de cargo practicadas fuera del juicio sean válidas, es necesario que concurran una serie de requisitos; que exista una causa legítima que impida esperar a su práctica en el acto de juicio, que se practique ante el Juez de Instrucción, que se garantice la contradicción de las partes, y que se introduzca su contenido en los autos a través del acta oportuna.[57]

No obstante, esta característica puede afirmarse también de las fuentes de prueba tradicionales, que pueden ser igual o aún más fácilmente manipuladas y destruidas por métodos más accesibles para el común de los ciudadanos, y que sin embargo son aportados al proceso sin mayor problema. En cualquier caso, siempre que exista un riesgo de destrucción de pruebas, las partes pueden solicitar su aseguramiento por los métodos legalmente previstos.

---

[54] MARTÍN RÍOS, P., "Problemas de admisibilidad de la prueba obtenida de dispositivos de almacenamiento digital", *Revista General de Derecho Procesal*, 51, 2020, Iustel, p. 3.
[55] CUADRADO SALINAS, C., "Registro informático y prueba digital. Estudio y análisis comparado de la ciberinvestigación criminal en Europa", 2014, La Ley, p. 1.
[56] CALAZA LÓPEZ, M. S., "Tres verdades (material, formal, virtual) y una sola realidad: la prueba electrónica", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, pp. 371–398*, Ediciones Jurídicas Castillo de Luna, 2020, p. 372.
[57] MUERZA ESPARZA, J. J., "Sobre la prueba testifical del menor–víctima en el proceso penal de mayores", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, pp. 1365–1378*, Ediciones Jurídicas Castillo de Luna, 2020, p. 1367.

En este sentido, si bien es cierto que la prueba tecnológica es alterable, no lo es menos que también puede modificarse cualquier documento impreso tradicional, o la declaración de un testigo. A esto se suma que, para manipular pruebas tecnológicas se requieren especiales conocimientos técnicos que no están al alcance de cualquier ciudadano.

En definitiva, admitiendo la alterabilidad de las pruebas tecnológicas como un elemento definitorio de las mismas, debe repararse en que no dista de lo que puede afirmarse de otros tipos de pruebas no tecnológicas. El proceso dispone, para estos supuestos en los que pueda dudarse de la originalidad de la prueba aportada, de herramientas necesarias para su impugnación, acreditación y valoración judicial, como se verá.

Hemos de examinar, igualmente, el riesgo de la generación de identidades ficticias derivado del anonimato, así como el peligro de usurpación de identidad, que –pese a su innegable relación– exigen de una individualización pormenorizada. En relación con el primero, las TICs sirven de resguardo para quienes las utilizan, porque se desconoce en la mayoría de las ocasiones el verdadero artífice, que se oculta tras técnicas informáticas. Con respecto a la segunda característica predicable de la prueba tecnológica, pero en relación con la anterior, el anonimato permite usurpar otras identidades. En este caso no se trataría de una identidad oculta, sino de que un sujeto actúe en nombre de un tercero sin su consentimiento y con *animus nocendi*. En ese sentido, el riesgo de la generación de identidades ficticias es un elemento distintivo de las pruebas tecnológicas que tienen su fundamento en el anonimato que proporcionan las nuevas tecnologías. Los usuarios elaboran un perfil que no siempre es posible asociar a una persona física determinada.

En una clara conexión con el anonimato que producen las nuevas tecnologías y el riesgo derivado de generación de identidades ficticias, existe el peligro de suplantación de la identidad de un tercero. La usurpación de una identidad ajena puede llevarse a cabo de dos maneras. La primera de las opciones es que quien se adueñe de otra identidad lo haga de una nueva ficticia, que no corresponda con ninguna persona física o jurídica. Esta posibilidad es la menos lesiva, pues no afecta al bien jurídico de una persona en concreto. La segunda de las posibilidades hace referencia al hecho de que la identidad suplantada corresponda a otro individuo diferente y que, por tanto, se obre en su nombre. En ese sentido, se recuerda también la asombrosa facilidad con la que las comunicaciones telemáticas pueden ser falseadas, inventadas o, incluso, efectivamente mantenidas, a través de suplantación de la personalidad de alguno de los comunicantes.

Por último, esta dificultad de investigación debe ponerse en contraposición con la facilidad de comisión de los ciberdelitos, sin duda derivada de: i) la facilidad de acceso al *hardware* necesario, siendo suficiente con disponer de un dispositivo con acceso a internet; ii) la facilidad de acceso al *software* necesario, incluyendo *malware*, troyanos, virus, etc., adaptados a cualquier acción de *hacking, cracking, phishing o pharming*; y iii) el desconocimiento de las potenciales víctimas de las amenazas que existen y las medidas de prevención que deberían adoptar.

C. LA INEVITABLE EXISTENCIA DE VESTIGIOS

Otra característica destacable de la prueba tecnológica es la que algunos autores han venido en denominar huella digital, identificando con esa expresión el rastro que toda actividad tecnológica produce (especialmente, en forma de metadatos). En este sentido, se afirma que "cuando una persona realiza una actividad utilizando tecnologías de la información y/o de la comunicación (TIC) hace surgir informaciones (huella o rastro digital) que pueden resultar útiles para la investigación por parte de los poderes públicos de actuaciones ilícitas"[58].

Estos vestigios que se generan en los dispositivos tecnológicos pueden quedar almacenados en archivos remotos ubicados en servidores de internet o en el mismo terminal[59]. Esta característica es relevante a efectos de la investigación de delitos propiamente informáticos o en aquellos que, aunque su naturaleza no es informática, tienen como base elementos probatorios informáticos (email, IP…). Por tanto, las pruebas digitales dejan unos "rastros" que pueden mantenerse *ad infinitum*[60].

Hay que tener en cuenta, no obstante, que dichos datos no siempre van a ser accesibles, utilizables o certeros, sino que, en ocasiones, las periciales informáticas sobre tales tienen un alcance limitado y no producen, en todos los casos, los resultados esperados[61].

Si bien el avance de la técnica permite acceder a muchos datos producidos por los mecanismos tecnológicos, en muchas ocasiones no es posible conocerlos e, incluso, pese a su conocimiento, es posible que un experto no pueda determinar si su contenido ha sido

---

[58] DELGADO MARTÍN, J., "Investigación del entorno virtual", cit., p. 1.
[59] BONACHERA VILLEGAS, R., "El registro de archivos informáticos: una cuestión necesitada de regulación", *Revista General de Derecho Procesal*, 27, 2012, Iustel, p. 2.
[60] DÍAZ CAPPA, J., "Confidencialidad, secreto de las comunicaciones e intimidad en el ámbito de los delitos informáticos", *Diario La Ley*, 7666, 2011, Wolters Kluwer, p. 2.
[61] ORTIZ PRADILLO, J. C., *Problemas procesales de la ciberdelincuencia*, cit.

o no manipulado. Esto lleva también a tener en cuenta que la existencia de vestigios exige la disponibilidad de personal con conocimientos técnicos suficientes

En relación con lo expuesto, se evidencia el carácter limitado de las periciales informáticas. Pese a que los peritos informáticos pueden aportar información útil en relación con determinadas pruebas tecnológicas, no siempre tendrán respuesta a las preguntas que puedan plantearse en un proceso judicial.

Adviértase, no obstante, que esta situación no difiere, sin embargo, de otros tipos de pruebas periciales. Por ejemplo, un perito forense puede no saber qué tipo de herramienta ha producido un determinado golpe, o un perito mecánico puede que no conozca qué elemento ha provocado unos daños en el vehículo que analiza, pero ello no le impedirá aportar los conocimientos de su ciencia para el esclarecimiento de los hechos sucedidos, en aquello que sea posible conocer.

En el análisis de este tipo de pruebas, a fin de desacreditarlas, es habitual la mención a su fácil manipulación. En este sentido, en la práctica ha quedado de manifiesto la posibilidad de modificar, sobrescribir o borrar datos de estas pruebas, lo que determina un peligro evidente de su manipulación.

Dentro del aspecto referido al rastro digital de la prueba tecnológica, tenemos que hacer referencia también a la publicidad de la misma, entendida en sentido estricto. Así, la prueba tecnológica puede consistir en información que los ciudadanos publican en la red voluntariamente y sin filtros para su acceso, de manera que cualquier tercero, también las Fuerzas y Cuerpos de Seguridad del Estado, pueden acceder e incluso recoger los datos que se encuentren en esa situación de disponibilidad de acceso –y que se ha venido en denominar como “fuentes abiertas”– y aportarlos posteriormente al proceso cuando tengan relación con la comisión o prueba de algún ilícito. Es, por ejemplo, el supuesto de la difusión de mensajes por medio de redes sociales, o la utilización de programas en redes P2P, como pone de manifiesto la STS 185/2019, de 2 de abril. Sobre esta cuestión nos volveremos a referir posteriormente.

La diferencia entre la prueba tecnológica y otras que no lo son radica, principalmente, en que las primeras —pese al riesgo descrito— en muchas ocasiones dejan un rastro digital (metadatos) que, de existir, aportarán más información sobre el propio delito.

D. EL ELEMENTO TRANSFRONTERIZO Y LA IMPORTANCIA DE LA COOPERACIÓN INTERNACIONAL

El elemento transfronterizo forma parte de la propia naturaleza de la cibercriminalidad y del dato digital. La transnacionalidad aparece en todos los fenómenos que se desarrollan en internet, sean prestaciones de servicios, operaciones de compra y venta o actividades delictivas, y también en el cibercrimen, por supuesto. Las acciones de phishing permiten engañar en un solo día a miles de personas en diferentes Estados, los virus infectan miles de servidores informáticos en segundos, el dinero pasa de un banco a otro en un paraíso fiscal mediante una operación electrónica que dura microsegundos, las *botnets* automatizan miles de ordenadores en tiempo real, etc[62].

Este carácter transfronterizo plantea una doble problemática, que resulta de especial interés para nuestro ámbito de investigación. Por un lado, el carácter transfronterizo de la ciberdelincuencia incidirá notablemente en la persecución de esta modalidad delictiva, porque va a ser fuente de conflictos competenciales entre los Estados. Por otro lado, también dificultará el acceso a los elementos probatorios y la propia captura del delincuente.

En ese sentido, se plantean cuestiones controvertidas acerca de los límites de la competencia jurisdiccional de los Estados, el ámbito de investigación de las diferentes fuerzas que realicen el *ciberpatrullaje* y el modo en que estas fuerzas van a comunicarse recíprocamente las noticias de delitos que recaben de la red.

En cuanto al primero de los aspectos mencionados, como es sabido, son cuatro los principios que tradicionalmente rigen la jurisdicción de los tribunales de un Estado: el principio de territorialidad, el de personalidad, el real y, finalmente, el de universalidad, recogidos en el artículo 23 LOPJ[63]. La aplicación del principio de territorialidad, determinado por el *forum delicti commissi*, es el criterio utilizado de ordinario para fijar la competencia jurisdiccional de los Estados. Sin embargo, no encuentra fácil acomodo en este ámbito, puesto que, en el cibercrimen, los resultados se manifiestan en lugares diversos (incluso las acciones se realizan en lugares distintos), por lo que la aplicación de esa regla competencial determina a menudo la convergencia de la jurisdicción de varios

---

[62] VELASCO NÚÑEZ, E., "Crimen organizado, internet y nuevas tecnologías", cit., p. 269.
[63] DÍAZ GÓMEZ, A., "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest", *Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR)*, 8, 2010, p. 8.

Estados en la persecución de un mismo delito. Esta cuestión, la de determinar el lugar de los hechos que ocurren en la red y la colaboración entre entidades de jurisdicciones diferentes e independientes ha generado un intenso debate doctrinal[64], en el que se plantean varias teorías, como son la teoría de la actividad (que entiende cometido el delito en el lugar en que se lleva a cabo la conducta delictiva), la del resultado (que mantiene que el delito se comete en el lugar en el que tiene lugar el resultado externo) o la teoría de la ubicuidad (para la cual el delito se entiende cometido en el lugar en que se lleva a cabo la actividad o se manifiesta el resultado)[65].

En cuanto al segundo aspecto referido, precisamente esa deslocalización de la actividad criminal puede determinar también que las pruebas, o los rastros de necesaria investigación, se encuentren dispersas entre varios Estados, lo que hace más complicada su búsqueda y aprehensión. El hecho de que la mayoría de las pruebas tecnológicas se originen, desarrollen y obtengan en la red, comporta una dificultad adicional en la ya exigente tarea de determinación de la competencia territorial, consecuencia directa de la deslocalización de internet. Por ejemplo, en relación con un correo electrónico que dé lugar a un procedimiento penal, el Tribunal puede que requiera la determinación del lugar desde el cual se ha enviado el mensaje o puede que necesite del auxilio del servidor de la empresa lo ha enviado y/o recibido, cuando se encuentre en un país extranjero. En particular, hay que considerar el carácter transnacional propio de múltiples actividades tecnológicas. Esto genera un problema de relevancia por dos motivos fundamentales: en primer lugar, porque los servidores que almacenan la información que se requiere pertenecen a empresas privadas que, en multitud de casos, se encuentran en otras jurisdicciones. Todo ello exige la colaboración de un nacional de un tercer Estado; en segundo término, por la problemática de la armonización entre las diferentes regulaciones[66]. Ambos elementos dificultan notablemente la aportación de pruebas tecnológicas a los procesos, y ello se acentúa con la ausencia de normativa internacional que armonice las diferentes legislaciones nacionales, lo que supone uno de los escollos fundamentales en la lucha contra el cibercrimen.

---

[64] ORTIZ PRADILLO, J. C., "Desafíos legales de las diligencias de investigación tecnológica", en *El proceso penal: Cuestiones fundamentales, 2017, pp. 279–291*, Tirant lo Blanch, 2017.
[65] RAYÓN BALLESTEROS, M. C.; GÓMEZ HERNÁNDEZ, J. A., "Cibercrimen: particularidades en su investigación y enjuiciamiento", *Anuario jurídico y económico escurialense*, 47, 2014, Real Centro Universitario Escorial–María Cristina.
[66] ORTIZ PRADILLO, J. C., *Problemas procesales de la ciberdelincuencia*, cit., p. 36.

De lo anterior resulta que, para una prevención y persecución efectivas de los *ciberdelito*s, es fundamental e irrenunciable el mantenimiento de una máxima cooperación entre los Estados y demás entidades, tanto públicas como privadas. Ello determina que sea necesario construir instrumentos internacionales destinados a ese fin, especialmente, a la resolución de controversias funcionales como la expuesta, haciendo especial énfasis en la agilidad de su aplicación, toda vez que, como señala CABEZUDO RODRÍGUEZ, "el éxito o fracaso de la lucha contra esta clase de criminalidad dependerá en gran medida de la rapidez de la respuesta procesal". En ese sentido, sería deseable que los convenios de cooperación internacional no se limitaran a contemplar actuaciones reactivas, como la obtención de elementos de convicción o que sirvan a la detención de los presuntos delincuentes, sino también formas de coordinación en sede preventiva que permitan evitar futuras amenazas[67].

En todo caso, un objetivo fundamental de estos instrumentos internacionales debe ser el de allanar la colaboración internacional, cuando menos, procurando que los Estados compartan un sustrato normativo común, cercano, armonizado o, al menos, compatible, que facilite tal cooperación. Una armonización que, aunque no implique una identidad absoluta en el contenido de las normas reguladoras, sí debería conformar un núcleo de principios generales compartido, un lenguaje unificado, etc.

En persecución de dicho objetivo, el 23 de octubre de 2001 se aprobó en Budapest el Convenio sobre Cibercrimen. Aunque nació bajo los auspicios del Consejo de Europa, su firma está abierta a cuantos Estados quieran sumarse a él. Dentro del contexto iberoamericano, se han alcanzado otros acuerdos, como el Convenio Iberoamericano de Cooperación sobre investigación, aseguramiento y obtención de pruebas en materia de cibercriminalidad de 2014, impulsado por la Conferencia de Ministros de Justicia Iberoamericanos (CMJIB). Aunque no dispone de la fuerza vinculante de un acuerdo internacional de estas características, la CMJIB ha evidenciado un notable esfuerzo de armonización legislativa en esta materia a través de la Recomendación relativa a la tipificación y sanción de la ciberdelincuencia, también abierta a la firma de los Estados parte[68].

---

[67] CABEZUDO RODRÍGUEZ, N., "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal", cit., p. 14.
[68] "SAIJ – Recomendación de la Conferencia de los Ministros de Justicia de los Países Iberoamericanos (COMJIB) relativa a la tipificación y sanción de la Ciberdelincuencia".

Otros instrumentos de cooperación internacional en materia de cibercriminalidad son los siguientes: el *Commonwealth of Independent States (CIS) Agreement on Cooperation in Combating Offences related to Computer Information (2001),* el *Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security (2009),* la *League of Arab States Convention on Combating Information Technology Offences (2010)* o la *African Union Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa (2012).*

En el ámbito europeo, cobra fuerza la asistencia interinstitucional, como se manifiesta con el Centro Europeo de Ciberdelincuencia (EC3), enmarcado dentro de Europol y operativo desde 11 de enero de 2013, con tareas de coordinación en la lucha extraterritorial contra el cibercrimen y apoyo tecnológico. También resultan especialmente útiles las redes policiales, como la Red de contacto 24/7 del artículo 35 del Convenio de Budapest, el Subgrupo de Delitos de Alta Tecnología del G–8 o la Red I–24/7 de Interpol. A ello hay que añadir medidas como las de conservación rápida de datos informáticos almacenados en un proveedor de servicios de internet cuando exista riesgo de pérdida o modificación, la conservación y revelación parcial rápida de datos sobre el tráfico, la obtención de datos sobre el tráfico y datos sobre el contenido en tiempo real[69], que permite que las autoridades encargadas de la investigación de un delito pueden acceder a la información que esté libremente accesible a través de la red, pero, para aquella restringida, deberán solicitar autorización a las autoridades competentes del lugar en el que la fuente de prueba se encuentre, siempre teniendo en consideración que las exigencias de admisibilidad del medio de prueba sean acordes a las reglas del proceso español.

El objetivo último en este proceso no puede ser otro sino la superación del principio de cooperación en favor del mutuo reconocimiento de las decisiones adoptadas en estas materias, a imagen de lo que sucede con la Orden europea de Detención y Entrega, así como alcanzar la máxima agilidad posible en las diligencias de investigación, sin comprometer su legitimidad. Conviene tener en cuenta que la obtención lícita de la información de que dispongan los ISP de terceros Estados deberá obtenerse mediante la

[69] ASENCIO GALLEGO, J. M., "Los delitos informáticos y las medidas de investigación y obtención de pruebas en el convenio de Budapest sobre la ciberdelincuencia", en *Justicia penal y nuevas formas de delincuencia, 2017, pp. 44–67,* Servei de Publicacions, 2017.

correspondiente comisión rogatoria internacional, dirigida al país guardador[70], o mediante la correspondiente Orden Europea de Investigación.

Por último, debe también tenerse presente que, si bien el elemento internacional puede comportar una dificultad investigadora adicional en el marco de la prueba tecnológica, también puede dar lugar a que resulten de aplicación diferentes ordenamientos jurídicos en lo que se refiere a las garantías procesales y potestades de investigación de la fuerza pública. En ese sentido, la configuración de los derechos fundamentales a la intimidad, al secreto de las comunicaciones, a la inviolabilidad del domicilio, a la autodeterminación informativa e, incluso, a la tutela judicial efectiva y a todas las garantías implícitas del proceso, puede ser manifiestamente diferente, o incluso inexistente, en los diferentes Estados.

E. EL ALTO ÍNDICE DE IMPUNIDAD

A las notas anteriores hay que añadir, como si de una consecuencia natural se tratase, el elevado índice de impunidad que acompaña a las diferentes formas de ciberdelincuencia.

Por un lado, nos encontramos con una falta de coordinación internacional entre las diferentes autoridades, lo que determina que la *notitia criminis* llegue tarde a la autoridad jurisdiccionalmente competente para investigar el delito o que, sencillamente, no llegue noticia alguna. Sucede así que, frecuentemente, el *ciberdelito* pasa de manera desapercibida ,y en no pocas ocasiones, ello sucede no sólo por la falta de coordinación pública, sino también porque la víctima prefiere no denunciarlo. Se han encontrado múltiples causas para esa conducta, entre las que se cuentan la falta de confianza en la capacidad de la policía en su persecución, la ignorancia de su propia condición de víctima, el desconocimiento de los mecanismos para formular esas denuncias, la vergüenza e, incluso, razones de carácter comercial, como puede ser la pérdida de prestigio si se hiciera pública la condición de perjudicado, etc.

Para intentar solucionar lo anterior, algunos Estados adoptan campañas de información sobre la ciberdelincuencia, crean sistemas *online* para la presentación de denuncias, construyen estrategias de cooperación con el sector privado o mejoran los sistemas

[70] VELASCO NÚÑEZ, E., "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica", *Diario La Ley*, 8183, 2013, Wolters Kluwer.

de intercambio de información policiales. Los efectos de estas medidas no consiguen, sin embargo, vencer la resistencia que se encuentra en el sector mercantil, especialmente cuando las víctimas son prestadoras de servicios de la sociedad de la información. Estas cuestiones, claro está, han tenido especial influencia en los protocolos de actuación de los cuerpos policiales en la investigación del delito, en los que, operativamente, reviste especial trascendencia la fase previa o de planificación de la diligencia de investigación en cuestión, que parte de la comprensión de la variedad de situaciones ante las que puede encontrarse el personal encargado materialmente de su realización. [71]

Por otro lado, también influye en la alta impunidad la dificultad que se observa en la obtención de pruebas, no necesariamente a causa de la volatilidad del dato informático. En efecto, también los intereses que otros Estados puedan tener cuando los elementos probatorios de un determinado delito se encuentran en el territorio de ese otro Estado (especialmente, en el caso de servicios alojado en la nube, y en los casos en los que las conductas se llevan a cabo desde Estados especialmente garantistas, que merecen la consideración de "paraísos de impunidad tecnológica"[72]) que puede dificultar tal obtención. Lo mismo sucede con la existencia de redes especialmente diseñadas para proteger el anonimato como *TOR*, canales *IRC*, *Red I2P*, *Freenet* o *GNUnet*. Del mismo modo, la complejidad creciente de las organizaciones de ciberdelincuencia, con acceso a mejores recursos, les permite el establecimiento de contramedidas, barreras y protecciones, que pueden retrasar o, incluso, frustrar la obtención de resultados. Asimismo, la exigencia de una elevada formación técnica, que comporta la necesidad de destinar recursos específicos no sólo a disponer de medios materiales, sino a formar en lo necesario a sus operadores.

Los elementos referidos han llevado a la doctrina a defender la imperiosa necesidad de construir una colaboración entre entidades públicas y privadas, nacionales e internacionales, en respuesta al fenómeno de la cibercriminalidad. Lo cierto es que en la obtención de elementos probatorios en orden a la efectiva persecución del delito se hace necesaria la colaboración de diversos sujetos ajenos al propio poder público. Especialmente, en lo relativo a sujetos que gestionan servicios o mantienen, en exclusiva, datos o informaciones esenciales a efectos de la represión del *ciberdelito*, cuya colaboración es

---

[71] CABEZUDO RODRÍGUEZ, N., "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal", cit., p. 18.
[72] *Ibid.*, p. 19.

esencial para dar respuesta inmediata a los supuestos de cibercriminalidad, sin perjuicio de las garantías que se reconozca a estos sujetos en orden a salvaguardar los derechos o intereses de trascendencia constitucional de que fueran titulares.

De igual modo, existen otros condicionantes que comportan la existencia de un alto índice de impunidad en relación con los ciberdelitos. Así, la posibilidad de automatización de las actuaciones informáticas necesarias para la comisión del delito permite que el mismo se cometa cuando su autor se encuentre ya lejos, o que las propias aplicaciones informáticas se reconfiguren de manera automática para encubrir todo lo posible el rastro. En el mismo sentido, la existencia de múltiples sistemas para ocultar la identidad del actuante, por ejemplo, mediante el empleo de servidores que ocultan la dirección final de la conexión.[73]

5. EL NECESARIO DESLINDE ENTRE LA ACTIVIDAD INVESTIGADORA Y LA ACTIVIDAD PROBATORIA

En nuestra sociedad de la información, con la llamada cuarta revolución industrial causada por los avances y descubrimientos en las tecnologías de computación y comunicaciones, la búsqueda tradicional del rastro físico o biológico de la actividad delictiva debe ser complementada con la búsqueda de rastros digitales[74].

A. CONCEPTO DE PRUEBA ELECTRÓNICA

La práctica de la prueba es la actividad procesal dirigida a acreditar la realidad de un hecho afirmado por las partes y que resulta relevante para el objeto del proceso[75]. Esta actividad persigue que el juez perciba mediante sus sentidos la información sobre la existencia de dicho hecho, a través de soportes de referencia que pueden ser personales o materiales.

En todo caso, hay que recordar que la admisión y práctica de las pruebas electrónicas se debe a un régimen jurídico establecido que requiere un esfuerzo de aproximación de los conceptos procesales a la realidad de la tecnología informática de nuestra sociedad actual.

---

[73] DAVARA RODRÍGUEZ, M. Á.; DAVARA FERNÁNDEZ DE MARCOS, E.; DAVARA FERNÁNDEZ DE MARCOS, L., *Delitos informáticos*, Editorial Aranzadi, Pamplona, 2017, p. 43, fecha de consulta 5 enero 2021, .
[74] 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*, 52, 2020, Iustel, p. 3.
[75] DELGADO MARTÍN, J., "Investigación del entorno virtual", cit., p. 38.

De igual modo, debemos señalar que el concepto de prueba digital como tal admite varias referencias, pues no existe una norma con rango legal a nivel nacional que establezca de manera expresa e indubitada un concepto de prueba electrónica, sino que lo que existen son varias referencias legislativas hacia figuras como el documento o la firma electrónicos[76].

La LO 16/1994, de 8 de noviembre, introdujo la posibilidad, si bien genérica, de utilizar medios técnicos, electrónicos e informáticos en los órganos judiciales, modificando para ello la Ley Orgánica 6/1985, de 1 de julio. Posteriormente, La Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, fue la que de modo expreso incorporó la regulación de las nuevas tecnologías en materia probatoria al proceso[77], con el tan citado artículo 300, además de los artículos 382 y 384, que regulan la incorporación de información y datos relevantes al proceso a través de la reproducción ante el tribunal de palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación y similares. Seguidamente, la Ley 18/2011, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, y la Ley 42/2015, de reforma de la LEC, terminaron por consolidar la aplicación de las TICs en la administración de justicia.

Posteriormente, en el año 2015, con la reforma operada por la Ley Orgánica 7/2015, de 21 de julio, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, quedó modificado el artículo 230 de la referida LOPJ para dar cabida expresa a las modalidades electrónicas de la prueba[78]. Con posterioridad, este artículo ha sido actualizado mediante la Ley Orgánica 4/2018, de 28 de diciembre, de reforma de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Del mismo modo, el artículo 26 del Código Penal no cierra la puerta a dichas modalidades, al disponer que "se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica", sin limitarse por tanto a la modalidad material de dichos documentos. En el mismo sentido, el artículo 24.2 de la Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico,

---

[76] BUENO DE MATA, F., "España", en *La prueba en el proceso: perspectivas nacionales, 2018, pp. 573–580*, Tirant lo Blanch, 2018, p. 573.
[77] BONET NAVARRO, J., "Apuntes sobre el concepto, obtención, introducción y fiabilidad de la prueba electrónica", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, pp. 279–298*, Ediciones Jurídicas Castillo de Luna, 2020, p. 279.
[78] DAVARA RODRÍGUEZ, M. Á. Y OTROS, *Delitos informáticos*, cit., p. 249.

prevé expresamente que, en todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental.

En síntesis, por prueba electrónica[79] cabe entender "toda la información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio"[80]. También puede definirse como "aquella información contenida en un dispositivo electrónico a través del cual se adquiere el conocimiento de un hecho controvertido, bien mediante el convencimiento psicológico, bien al fijar este hecho como cierto atendiendo a una norma legal"[81]. También podemos traer la definición contenida en una Decisión incluida en el Programa Marco AGIs de la Dirección General de Justicia de la Comisión Europea sobre cooperación judicial y policial en material penal, que la definía como "la información obtenida a partir de un dispositivo electrónico o medio digital el cual sirve para adquirir convencimiento de la certeza de un hecho". En el plano nacional, en los denominados "Foros de las Evidencias Electrónicas" se refieren a estas como "los documentos electrónicos o colecciones de datos procedentes de un sistema informático que pueden ser sometidos a los criterios de los peritos informáticos para determinar su autenticidad y ser aportados como prueba en juicio, de manera que su contenido es relevante para el caso"[82]

Otro concepto que también conviene tener en consideración es el de "dato informático", que se define en el Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2001 como "toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función", así como el de "medio electrónico", que se define en el anexo de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, como "mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como internet, telefonía fija y móvil u otras".

---

[79] También se utilizan las denominaciones prueba informática, prueba tecnológica y prueba digital.
[80] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, 2ª edición actualizada, La Ley, Madrid, 2018, p. 40.
[81] SANCHÍS CRESPO, C., "La prueba en soporte electrónico", en *Las tecnologías de la información y la comunicación en la administración de justicia: análisis sistemático de la Ley 18/2011, de 5 de julio, 2012, pp. 707–734*, Thomson Reuters Aranzadi, 2012, p. 713.
[82] BUENO DE MATA, F., "España", cit., p. 574.

En el desarrollo de nuestra actual sociedad de la información, es apreciable una tendencia al aumento del número de casos en los que el juez tiene que percibir una información sobre un hecho que, o bien es de naturaleza digital y ha quedado registrada en el correspondiente soporte digital, o bien, siendo material, ha quedado registrada de manera digital. Hay que tener en cuenta que, en materia de evidencia digital, no existe identidad entre la realidad conservada y la información exteriorizada, pues toda información contenida en un medio digital consiste en realidad en un conjunto de impulsos o estímulos eléctricos o fotosensibles –representado en lenguaje binario– que, dada su ininteligibilidad para el juez, debe ser transformada a signos directamente reconocibles[83]. Esta cuestión no es de escasa relevancia, toda vez que determina la inclusión de un nivel más de profundidad en la actividad probatoria, entendida como aquella consistente en traer un hecho de la realidad al proceso judicial, cuya evidencia debe ser interpretada en sí misma.

No está de más recordar que el uso del lenguaje binario en la prueba digital se debe a que es la base del funcionamiento de las computadoras –que es donde quedan generadas las pruebas digitales, entendidas en amplio sentido–, en la medida en que estas trabajan internamente con dos sistemas de voltaje, por lo que precisan de un modelo que, a partir de la representación de dos estados mutuamente excluyentes, permita generar toda la información necesaria, como es el lenguaje binario. En el lenguaje binario, que, por otro lado, data de fechas tan remotas como el siglo III a.C., la unidad mínima de información es el bit (acrónimo de *binary digit*), que puede tener solamente dos valores (0 y 1). La agrupación de bits, unida a su posición, permite representar la información. Es lo que determina, al ser un lenguaje de base 2, que en informática las medidas de información sean múltiplos de dicho número, en lugar de 10, como sucede en el sistema decimal.

La información estructurada en formato digital o electrónico, a diferencia de la insertada en un soporte material directo, solamente puede ser leída por una persona si esta utiliza un instrumento técnico electrónico que sea capaz de convertir la información cifrada –estructurada en dígitos binarios registrados como señales ópticas o magnéticas en el correspondiente soporte físico– en un texto en lenguaje natural alfabético que pueda visualizarse en la pantalla de ese dispositivo[84]. En todo caso, debería tenerse en cuenta

---

[83] GARCÍA TORRES, M. L., "La tramitación electrónica de los procedimientos judiciales", *La ley penal: revista de derecho penal, procesal y penitenciario*, 82, 2011, Wolters Kluwer.
[84] GONZÁLEZ–MENESES ROBLES, M., "La función notarial en el medio electrónico", *Anales de la Academia Matritense del Notariado*, 52, 2012, Editoriales de Derecho Reunidas. EDERSA, p. 47.

que el lenguaje natural no es sino otro método de cifrado de la realidad a la que se refiera la prueba practicada. La única diferencia respecto del lenguaje binario es la capacidad adquirida del juez para interpretar directamente la información codificada, mientras que en el caso de la prueba electrónica es necesaria un intérprete, del mismo modo que se precisa un traductor en aquellos supuestos en los que el lenguaje utilizado no es el habitual de la jurisdicción ante la que se sustancia la prueba.

Por último, no hay que perder de vista que la jurisprudencia considera las opiniones y manifestaciones *on line* como documentos privados, al igual que en el caso de la correspondencia postal. En el particular caso de las capturas de pantalla, los tribunales vienen exigiendo que se acredite el origen de la comunicación, la identidad de los interlocutores, y la integridad del contenido. Ello será posible, por ejemplo, mediante el acceso de un fedatario público a la cuenta perfil de la red social del que pretenda aportar la prueba, dejando constancia de lo que perciba mediante sus sentidos en el acta. No obstante, todo ello no consigue sino subrayar la importancia de obtener pruebas periciales suficientes sobre dichos extremos de hecho, que ayuden a desterrar cualquier sombra de duda que surja respecto del material aportado al proceso[85].

Al margen de lo anterior, es necesario realizar algunos apuntes en torno a la regulación de la prueba electrónica en España. Debemos mencionar, a este respecto, el artículo 24.2 de la Constitución Española, que recoge el derecho de toda parte procesal a utilizar los medios de prueba que sean pertinentes para su defensa, sin limitación respecto del medio en que dicho medio se verifique. Desde ahí, es necesario referirnos también a los artículos 299.2, 299.3, 382, 383 y 384 LEC, además de los artículos 300.1, 327, 333, 334, 352, 431 y 812 LEC, que se refieren a esta cuestión, también, de manera más indirecta.

B. FASES DE LA PRUEBA DIGITAL

En la doctrina[86] es frecuente realizar una distinción entre las diferentes fases que atraviesa la prueba electrónica o digital, distinguiéndose entre una fase de obtención de la información o datos electrónicos, esto es, de la fuente de prueba, y otra fase posterior, de incorporación de los datos al proceso, y su posterior valoración.

---

[85] DAVARA RODRÍGUEZ, M. Á. Y OTROS, *Delitos informáticos*, cit., p. 257.
[86] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 43.

La primera fase supone la actividad de obtención de la realidad material, esto es, de los datos informáticos producidos, ya se encuentren almacenados y en reposo o siendo objeto de transmisión, mediante el acceso a los diferentes soportes digitales. En todo caso, el acceso a esta fuente de prueba se producirá por las partes en conflicto o por la autoridad pública, en ejercicio de las funciones legalmente previstas y sin vulnerar los derechos fundamentales que puedan verse afectados.

La segunda fase radica en la incorporación al proceso de la información obtenida, siempre que sea relevante para el objeto del proceso y sirva para acreditar extremos relativos al mismo. Por tanto, dicha información debe ser pertinente, útil, lícita, y cumplidora de los requisitos procesales establecidos[87].

Finalmente, llega el momento de la valoración de la información aportada al proceso por parte del Juez o Tribunal, conforme a los principios que resulten de aplicación.

Partimos de que en la configuración de nuestro proceso penal existen dos fases diferenciadas con claridad: la de investigación del hecho delictivo, denominada de instrucción y dirigida por el órgano instructor (que, de momento, al menos en términos formales, sigue siendo el juez de instrucción), y la de enjuiciamiento del hecho delictivo averiguado, que se sustancia ante el órgano sentenciador que corresponda en función de las normas de competencia funcional. Además de esas dos, es de obligada mención, aunque sea por guardar la debida lógica, la de ejecución, que tendrá lugar tras la de enjuiciamiento, si la sentencia es condenatoria.

Desde esa perspectiva, las diligencias de investigación que se adopten y ejecuten en esa primera fase de instrucción no son sino los recursos o herramientas con los que el poder público puede contar para averiguar las circunstancias que permitan comprobar la realidad de unos hechos presuntamente delictivos y, en su caso, verificar su autoría. Es posible, incluso, que esta actividad indagatoria tenga lugar antes de la propia incoación del proceso de instrucción judicial.

Ahora bien, esta actividad instructora o indagatoria se encuentra regulada, del mismo modo que también lo está la actividad probatoria, con el objeto de delimitar los cauces por los que, en definitiva, puede perseguirse la verdad material. En ningún caso podría conllevar la renuncia o transgresión de unos principios que se entienden como

[87] *Ibid.*, p. 44.

irrenunciables y se plasman en los derechos fundamentales, tanto de contenido procesal (juez ordinario predeterminado por la ley, defensa, asistencia letrada, presunción de inocencia, y demás del artículo 24 CE.) como de contenido material (libertad ambulatoria, intimidad, inviolabilidad domiciliaria, secreto de las comunicaciones personales, y restantes derechos fundamentales).

Es necesario aclarar que el objeto principal de nuestra investigación es la fase de obtención de la prueba, referida al acceso a las fuentes de la prueba electrónica que, como hemos referido, está compuesta por los datos informáticos almacenados en un dispositivo electrónico o transmitidos electrónicamente mediante redes de comunicación abiertas o restringidas. Este acceso tendrá lugar porque lo efectúe la autoridad pública en sede de instrucción, sin perjuicio del acceso que pueda efectuar un tercero al dato informático, debiendo tenerse presente en ambos casos los mínimos imperativamente impuestos por la vigencia de los derechos fundamentales.

En cuanto al acceso a datos informáticos contenidos en dispositivos electrónicos, es posible que lo realice tanto la parte procesal como la autoridad competente en el marco de un proceso penal. En ambos casos, el acceso al dato informático contenido en un sistema o equipo informático puede efectuarse previa aprehensión del soporte físico, bien porque se encuentre legítimamente en poder del que pretende acceder a su contenido (que también puede que esté legitimado para dicho acceso), bien porque se encuentre en poder de un tercero que tenga el deber de colaborar con la autoridad pública, o, finalmente, porque la autoridad pública orqueste un sistema de acceso telemático, sin necesidad de detentar físicamente el soporte de los datos.

En los supuestos de acceso a datos por parte de particulares o terceros, puede suceder que los mismos se encuentren en un dispositivo titularidad de la propia parte interesada que los hará valer en el proceso. La licitud, en este supuesto, no supondría un problema fundamental; los principales escollos se encontrarían en la fase de incorporación al proceso y su valoración. En este sentido, hay que recordar que el artículo 11 b) de la Ley 4/2015, de 27 de abril, del Estatuto de la Víctima del delito, prevé que toda víctima tenga derecho a “comparecer ante las autoridades encargadas de la investigación para aportarles las fuentes de prueba y la información que estime relevante para el

esclarecimiento de los hechos"[88]. Sin embargo, puede suceder también que los datos se encuentren contenidos en un dispositivo ajeno y que el contenido del mismo deba ser aportado por una orden judicial o en cumplimiento de un deber de colaboración legamente previsto, en cuyo caso dicha aportación sería lícita. También es posible que dicho acceso se produzca sin elemento habilitador alguno, por lo que el acceso a los datos habría vulnerado los derechos fundamentales de su titular y la prueba habría devenido ilícita.

Por otro lado, en los supuestos de datos a los que accede la autoridad pública competente en el proceso penal, debe recordarse que existen varias posibilidades: la aprehensión del propio dispositivo encontrado fuera de lugar cerrado, la diligencia de entrada y registro en lugar cerrado con ocupación del dispositivo o de la información relevante, la posibilidad de acceder al contenido del sistema informático sin necesidad de proceder a la aprehensión física del equipo informático, el acceso a la información contenida en un servidor desde uno de los puestos de la red, y los registros transfronterizos.

En el caso de datos que sean accedidos mientras estaban siendo transmitidos por redes de comunicación, cabe distinguir entre aquellos que pueden considerarse incluidos en un proceso de comunicación de aquellos que simplemente estén siendo objeto de transmisión electrónica, pero no de una comunicación. En el primer caso, el dato puede ser obtenido por uno de los comunicantes, que es el supuesto en el que una de las personas participantes en el proceso de comunicación accede al dato y dispone de él para preparar su ulterior incorporación al proceso; o por un tercero no comunicante (que, principalmente, podrá ser el poder público, además de otros sujetos terceros obligados a colaborar con las autoridades. En el segundo supuesto, esto es, cuando el dato se transmite a través de una red de comunicación sin formar parte de un proceso comunicativo, nos referimos a contenidos de páginas web, historial de navegación, perfiles públicos y otras posibilidades que conforman las llamadas fuentes abiertas, a las que nos referiremos posteriormente.[89]

Es necesario, asimismo, realizar una distinción ente fuente y medio de prueba. Como es sabido, fuente de prueba es un concepto referido a la propia realidad material, que existe de forma previa e independientemente del proceso. En ese sentido, es el

---

[88] RODRÍGUEZ ÁLVAREZ, A., "Proceso penal y redes sociales: aportación por las partes de la información contenida en ellas", en *El proceso penal: Cuestiones fundamentales, 2016, pp. 339–348*, Tirant lo Blanch, 2016, p. 313, fecha de consulta 16 marzo 2020.
[89] RODRÍGUEZ ÁLVAREZ, A., "Proceso penal y redes sociales", cit.

elemento de la realidad material sobre el que posteriormente se pretenderá construir la convicción[90], los elementos que existen en la realidad al margen del proceso y convencen sobre datos de hecho.

El medio de prueba, por el contrario, es un concepto referido a la virtualidad del propio proceso judicial y, únicamente, tiene sentido dentro del propio proceso. En ese sentido, es el conducto mediante el que se verifica la actividad consistente en traer al proceso la realidad contenida en la fuente de prueba, disciplina la incorporación y práctica de la prueba. En este caso son limitados y están regulados.

En definitiva, y atendiendo al medio electrónico, la fuente de prueba es la realidad electrónica tal y como se haya producido, mientras que el medio de prueba es la forma en que dicha realidad electrónica se aporta al proceso. En esta cuestión hay que llamar la atención sobre el hecho de que la acelerada evolución tecnológica y la utilización masiva de herramientas informáticas en todos los aspectos de la vida actual, en continua expansión, genera constantemente nuevos instrumentos informáticos que no son sino nuevas fuentes de prueba (piénsese en la evolución de los medios de mensajería, de los formatos y soportes, e incluso de la localización de los datos).

Sin embargo, esa constantemente creciente variedad de fuentes probatorias no ha encontrado una tendencia paralela en cuanto a la figura de los medios de prueba legalmente previstos, que continúan siendo los del artículo 299.2 LEC.[91] Esta decisión del legislador solamente puede explicarse desde la idea de los diferentes medios informáticos no consiguen alterar la naturaleza de la fuente de prueba –el dato informático–, que –se entiende– se mantiene inalterable.

En añadidura, es probable que las diligencias de investigación, además de para comprobar la existencia del hecho delictivo y averiguar las personas que deban responder como autores (en sus diferentes gradaciones) de los mismos, sirvan para preparar y contener la prueba que habrá de practicarse en el juicio oral, pues a ellas corresponde la función el descubrimiento y aseguramiento de las fuentes probatorias. La fuente de prueba de la prueba electrónica, el dato informático, es naturalmente frágil, dúctil y de muy fácil

[90] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 41.
[91] *Ibid.*

variabilidad[92], esto es, es naturalmente volátil, especialmente cuando se trata de datos alojados en la red. Esta circunstancia comporta que las figuras de su preconstitución, o incluso la anticipación de su práctica, adquiera una especial relevancia. En concreto, el resultado de cualquier diligencia de investigación consiste en la obtención de datos, de información, que puedan constituir el punto de partida de nuevas diligencias, ser el soporte de la imputación formal o de los escritos de acusación, o incluso cuando proceda ser considerados como pruebas preconstituidas y fundamentar una futura sentencia de condena.[93]

En ese sentido, debe tenerse en cuenta que el conjunto normativo introducido con la LO 13/2015 se dirige de manera específica a la llamada "fase de obtención de prueba", y pretende abordar la problemática que surge durante la averiguación digital de los hechos que constituyen el delito investigado. Sobre este particular, hay que recordar que en la fase de instrucción pueden diferenciarse dos tipos de pruebas: las preconstituidas y las anticipadas. Ambas se diferencian desde un punto de vista subjetivo, en la medida en que la primera puede prepararse por el Ministerio Fiscal y la Policía Judicial –y accederá al procedimiento como prueba documental–, pero la segunda exige la intervención del Juez de Instrucción, en tanto que supone el adelantamiento de su práctica[94].

La prueba preconstituida, por su naturaleza y utilidad, se refiere a hechos irrepetibles que, por las circunstancias que le son inherentes, no pueden ser trasladados al momento del juicio oral. Para evitar que el enjuiciamiento se realice sin acceder a elementos de hecho fundamentales, es posible que dichas fuentes de prueba se analicen y queden plasmadas –con las debidas garantías– en una prueba documental, que sí lleva la realidad al proceso. En ese sentido, la prueba preconstituida tiene un carácter asegurador de los indicios y fuentes de prueba, en la medida en que permite su introducción en el juicio oral a través de la lectura de documentos, conforme a lo previsto en el artículo 730 LECrim.

Además de lo anterior, no puede olvidarse que también es posible que los propios sujetos pueden realizar las actuaciones necesarias para preconstituir la prueba antes del inicio del procedimiento, incorporando el dato informático (fuente de prueba) a

---

[92] MENDIZABAL, R. T.; GUILLÉN, J. F.; PÉREZ, J. C., "La obtención de la prueba electrónica, su acceso al proceso civil y la garantía de derechos en material penal", *Economist & Jurist*, vol. 20, 163, 2012, Global Economist & Jurist.
[93] NADAL GÓMEZ, I., "El Régimen de los hallazgos casuales en la Ley 13/2015, de modificación de la ley de Enjuiciamiento criminal", cit., p. 22.
[94] GIMENO SENDRA, J. V., *Derecho procesal penal*, 2ª ed., Civitas–Thomson Reuters, Madrid, 2015.

cualquiera de los medios de prueba previstos en derecho (documento físico, documento electrónico, e incluso mediante dictamen pericial), en los que podrá asumirse la intervención de una empresa que preste servicios de certificación, según el Reglamento (UE) 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. En todos estos casos sería recomendable la intervención de un fedatario público que levante acta en la que recoja el contenido de la fuente de prueba que pretenda llevarse posteriormente al procedimiento[95].

C. MODALIDADES DE FUENTE DE PRUEBA ELECTRÓNICA

La doctrina[96] distingue dos modalidades fundamentales de fuente de prueba electrónica en función del estado en que se encuentren los datos intervenidos: los datos o informaciones almacenados en un dispositivo electrónico y los datos transmitidos por cualesquiera redes de comunicación, abiertas o restringidas, como Internet, redes de telefonía fija y móvil, u otras. Esta distinción es importante, porque afecta a las diferentes diligencias de investigación tecnológica que realizará la policía judicial en el ejercicio de sus funciones de averiguación del delito.

De esa manera, por un lado, se distinguen los supuestos de acceso e incorporación al proceso de información contenida y en reposo en dispositivos electrónicos, sean sistemas informáticos, aparatos informáticos o medios de almacenamiento masivo de memoria. En ese sentido, el artículo 19 del Convenio de Budapest[97] se refiere al registro y confiscación de datos informáticos contenidos "en un medio de almacenamiento de datos en el que puedan almacenarse datos informáticos" y "en un sistema informático o una parte del mismo así como los datos informáticos almacenados en él" y, según el artículo 1 del mismo, por sistema informático se entiende "todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa".

Por otro lado, se distinguen los supuestos de acceso e incorporación al proceso de información que se encuentre en tránsito por ser objeto de una transmisión electrónica mediante redes de comunicación. A su vez, en estos supuestos puede distinguirse entre aquellos casos en los que la información se transmite en un proceso de comunicación,

---

[95] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 75.
[96] *Ibid.*, p. 42.
[97] "Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 (BOE–A–2010–14221)".

esto es, en un proceso de transmisión de información entre un transmisor y un receptor a través de redes de comunicación abiertas o restringidas, y aquellos en los que la información se transmite, también a través de redes de comunicación abiertas o restringidas, pero sin existir un proceso de comunicación entre personas determinadas o determinables, sino exclusivamente entre dispositivos. En estos últimos supuestos las garantías del artículo 18 CE operan con menor intensidad y la Policía Judicial, como veremos en múltiples ocasiones a lo largo de este trabajo, podrá adoptar medidas de investigación sin necesidad de autorización judicial al respecto.

En otro orden de cosas, es necesario señalar también que, en materia de prueba electrónica, la doctrina coincide en afirmar que no hay un catálogo estricto de las mismas, sino que debe aplicarse un criterio de *numerus apertus*[98]. En tal sentido, se ha distinguido entre pruebas electrónicas creadas directamente a través de la informática (*cookies*, *tags*, *logs*, y demás información que no dispone de formato físico por naturaleza); pruebas electrónicas que proceden de medios de reproducción o archivos electrónicos, pero que representan una parte sensible de la realidad (fotografías, vídeos, grabaciones de audio); pruebas electrónicas que se presentan mediante un *hardware* informático en sí mismo (componentes informáticos); y pruebas electrónicas mixtas (una prueba pericial electrónica, por ejemplo).

D. DATOS DE TRÁFICO Y DATOS DE ABONADO

Es necesario poner también en correlación estas distinciones con la oportuna diferenciación entre datos de tráfico y datos de abonado. Los primeros pueden definirse como "todos aquellos relativos a la comunicación por medio de sistema informático, generados por el sistema informático que forma parte de la cadena de comunicación, indicando origen, destino, ruta, hora, fecha, tamaño, duración o tipo de servicio subyacente"[99], mientras que los segundos quedan definidos en el artículo 18.3 del Convenio de Budapest, que indica que por datos de abonado "se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar: a) El tipo de servicio de comunicaciones

[98] BUENO DE MATA, F., "España", cit., p. 578.
[99] CALVO LÓPEZ, D., "Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (apartados K) a M) del art. 588 ter de la LECrim)", cit., p. 7.

utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio; b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios; c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios".

La distinción es fundamental porque la ley y la jurisprudencia vienen considerando a los datos de tráfico como parte del proceso comunicativo, quedando por tanto incluidos en la protección dispensada por el artículo 18.3 CE, que establece el monopolio jurisdiccional sobre su limitación. Por el contrario, los datos de abonado, en tanto que no se consideran como parte de un proceso de comunicación, quedan protegidos únicamente por el artículo 18.4 CE, que permite su afección sin necesidad de previa autorización judicial[100].

A tal efecto, se ha entendido que son datos de tráfico aquella información de identificación de los medios de comunicación emisores y receptores generados en el marco de la conducción de una comunicación[101].

En el mismo sentido, la STS 247/2010, de 18 de marzo, distingue entre "datos personales externos o de tráfico que hacen referencia a una comunicación concreta y contribuyen a desvelar todo o parte del secreto que protege el artículo 18.3 CE; y b) datos o circunstancias personales referentes a la intimidad de una persona (artículo 18.1 CE), pero autónomos o desconectados de cualquier comunicación, que caerán dentro del derecho a la protección de datos informáticos o *habeas data* del artículo 18.4 CE que no pueden comprometer un proceso de comunicación".

En todo caso, debe tenerse en cuenta que, conforme a lo expuesto, no todos los datos de tráfico generados y externos al contenido de la comunicación merecen el amparo del artículo 18.3 CE, pues dicho tratamiento solamente corresponderá a aquellos que contienen información íntimamente ligada al secreto de lo comunicado, por revelar el origen y destino de la misma, su momento y duración, el volumen de información transmitida y

[100] *Ibid.*, p. 8.
[101] GIMENO SENDRA, J. V., "La Prova preconstituïda de la policia judicial", *Revista catalana de seguretat pública*, 22, 2010, Institut de Seguretat Pública de Catalunya.

el tipo de comunicación entablada[102]. Por el contrario, al resto de datos de tráfico (IMSI, IMEI y demás etiquetas identificativas y datos de conexión) corresponderá el tratamiento correspondiente al artículo 18.4 CE.

En ese sentido, la misma STS 247/2010, de 18 de marzo, continuaba indicando que "la absoluta equiparación de todo tipo de datos de tráfico o externos o la inclusión de todos ellos dentro del derecho al secreto de las comunicaciones comportaría un auténtico desenfoque del problema, pues incorporaría en el ámbito de la protección constitucional del artículo 18.3, circunstancias cuyo tratamiento jurídico no debería separarse del que se dispensa a la protección de datos o al derecho a la autodeterminación informática del artículo 18–4 C.E. (véase por todas S.T.S. 249 de 20–5–2008)". Este es también el parecer de la Fiscalía General del Estado en su Circular 1/2013, de 11 de enero[103].

También se ha distinguido entre los datos de naturaleza dinámica y los datos estáticos. A dicha distinción se refiere la Fiscalía General del Estado cuando afirma que "los primeros son los que se generan durante un proceso de comunicación, mientras que los segundos aparecen almacenados en las bases de datos de los prestadores de servicios de comunicación para posibilitar esas comunicaciones, pero no se generan como consecuencia de una comunicación concreta". La STS 740/2017, de 16 de noviembre, también identifica a los datos estáticos como aquellos en los que el proceso comunicativo ha finalizado, así como los de identificación.

Tampoco puede desatenderse la definición que, a estos efectos, contiene el Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, cuando indica en su artículo 64, que por dato de tráfico debe entenderse "cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de su facturación".

La distinción entre datos de tráfico y datos de abonado ha trascendido a nuestro ordenamiento jurídico mediante el artículo 588 *ter* b) LECrim, al referirse al contenido

---

[102] CALVO LÓPEZ, D., "Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (apartados K) a M) del art. 588 ter de la LECrim)", cit., p. 8.

[103] "Circular 1/2013, de 11 de enero, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas.", fecha de consulta 29 abril 2020, en https://www.boe.es/buscar/doc.php?coleccion=fiscalia&id=FIS–C–2013–00001&tn=2.

de las comunicaciones, a los datos electrónicos de tráfico o asociados al proceso de comunicación y a los que se generen con independencia del establecimiento o no de una concreta comunicación. Sin embargo, la distinción entre datos de tráfico dinámicos y datos de tráfico estáticos no queda prevista de manera expresa en nuestro ordenamiento, a pesar de que puede deducirse que "la solicitud de datos dinámicos (vinculados a una comunicación) exige autorización judicial, mientras que la solicitud de datos de tráfico estáticos (no vinculados a ninguna comunicación) puede realizarse de manera independiente a una autorización judicial."[104] En ese sentido, el artículo 588 *ter* j) LECrim regula la incorporación al proceso de datos de tráfico o asociados que se encuentren vinculados a procesos de comunicación, que requerirán siempre autorización judicial, y los artículos 588 *ter* k) al 588 *ter* m) LECrim prevén el acceso a determinados datos de identificación de usuarios o dispositivos, que no requieren autorización judicial[105].

Tampoco puede desatenderse la pertinencia de obtener un acta notarial de presencia que dé fe de lo que el notario perciba por sus sentidos[106].

E. REFERENCIA A LA SITUACIÓN ACTUAL DE LA PRUEBA ILÍCITA

No podemos finalizar este capítulo sin hacer una referencia, siquiera breve, a la situación en la que actualmente se encuentra el instituto de la prueba ilícita y la consiguiente regla de exclusión, de acuerdo con la doctrina de nuestro Tribunal Constitucional.

Desde una aproximación conceptual, el instituto de la prueba ilícita y la regla de exclusión plantea el interrogante de si el ejercicio del *ius puniendi* del Estado puede ejercitarse de cualquier modo y sin limitación alguna o si, por el contrario, existen límites irrenunciables a la hora de ejercer la función jurisdiccional. Como se ha indicado, no puede olvidarse que, aunque la averiguación de hechos delictivos constituye una actividad que encierra un interés especialmente merecedor de protección en el Estado de derecho,

---

[104] ARRABAL PLATERO, P., *La prueba tecnológica: aportación, práctica y valoración*, Tirant lo Blanch, Valencia, 2019, p. 162.
[105] "Circular 2/2019, de 6 de marzo, de la Fiscal General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas.", fecha de consulta 25 abril 2020, en https://www.boe.es/diario_boe/txt.php?id=BOE–A–2019–4241.
[106] DAVARA RODRÍGUEZ, M. Á. Y OTROS, *Delitos informáticos*, cit., p. 254.

es también función del Estado la de garantizar los derechos de los ciudadanos, especialmente, los elevados a categoría de fundamentales[107].

Como es sabido, la figura de la prueba ilícita ha atravesado diferentes teorías desde su nacimiento, que son las que pasamos a señalar a continuación.[108]

a) Teoría directa

La teoría directa aparece con el caso *Weeks v. United States*, de 1904, en el que, con ocasión de una documentación hallada en un registro ilícito, viene a afirmarse que el castigo de los culpables no debe llevarse a cabo sacrificando los derechos fundamentales garantizados constitucionalmente. Posteriormente, esta postura se confirmaría en la sentencia del caso *Mapp vs. Ohio.*

En España, el TC se pronunció a favor de dicha teoría en su STC 114/1984, de 29 de noviembre, que mantiene la inadmisibilidad en el proceso de las pruebas obtenidas con violación de derechos fundamentales.

A pesar de que la sentencia se refería a una grabación de una conversación obtenida por uno de sus interlocutores, concluyendo que dicha práctica no vulnera el secreto de las comunicaciones, también afirma que no pueden ser recibidas en sede jurisdiccional, por impertinentes desde el punto de vista constitucional, aquellas pruebas obtenidas de manera antijurídica, dado el valor preferente del sistema de derechos fundamentales[109]. No obstante, la anterior postura devino al poco tiempo inútil por ineficiente, pues no ofrecía protección frente a aquellas pruebas que se obtuvieran sin conculcar derechos fundamentales, pero derivando de otras pruebas o indicios obtenidos de manera ilícita.

b) Teoría indirecta o refleja

La insuficiente protección que dispensaba la teoría directa, junto con la entrada en vigor del artículo 11.1 LOPJ, que extendía la prohibición de valoración a los resultados indirectos de las pruebas obtenidas con vulneración de derechos fundamentales, provocó

---

[107] ARMENTA DEU, T., "Prueba ilícita y regla de exclusión: perspectiva subjetiva", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, pp. 117–140*, Ediciones Jurídicas Castillo de Luna, 2020, p. 118.

[108] A este respecto, son también reiterados los pronunciamientos que recuerdan que la indeterminación del artículo 11.1 LOPJ ha provocado que exista cierta indeterminación en cuanto a la aplicación de la regla de la exclusión de la prueba ilícitamente obtenida en nuestro país

[109] ASENCIO MELLADO, J. M., "Prueba ilícita: declaración y efectos", *Revista General de Derecho Procesal*, 26, 2012, Iustel.

que por nuestros tribunales se adoptara la teoría indirecta, o refleja, o teoría de los frutos del árbol envenenado, aparecida por vez primera en la sentencia *Co. Inc v. United States*, en 1920.

Nuestro Tribunal Supremo adopta esta doctrina con ocasión de las SSTS 210/1992, de 7 de febrero, y 814/1992, de 7 de abril, pudiendo citarse también, entre otras, las 22783/1993, de 13 de diciembre, 311/1994, de 19 de noviembre, 1284/1994, de 17 de junio, 2054/1994, de 26 de noviembre, 799/1996 14 de octubre, y 985/1996, de 27 de noviembre.

El Tribunal Constitucional, por su parte, se pronuncia en el mismo sentido en la STC 85/1994, de 14 de marzo, en la que concluye que "todo elemento probatorio que pretendiera deducirse del contenido de las conversaciones intervenidas no debió ser objeto de valoración probatoria, ya que la imposibilidad de admitir en el proceso una prueba obtenida violentando un derecho fundamental no sólo deriva directamente de la nulidad de todo acto violatorio de los derechos reconocidos en el Capítulo Segundo del Título I de la Constitución, y de la necesidad de confirmar, reconociéndolas efectivas, las contravenciones de los mismos (…), sino ahora también en el plano de la legalidad en virtud de lo dispuesto en el art. 11.1 de la Ley Orgánica del Poder Judicial". Otras importantes son las SSTC 114/1984, de 29 de noviembre; 107/1985, de 7 de octubre; 64/1986, de 21 de mayo; 80/1991, de 15 de abril; 85/1994, de 14 de marzo; 86/1995, de 6 de junio; 181/1995, de 11 de diciembre; 49/1996, de 26 de marzo; 54/1996, de 26 de marzo; 81/1998, de 2 de abril; 69/2001, de 26 de marzo[110].

De acuerdo con esta teoría, resulta fundamental distinguir entre la denominada prueba diferente, que es la prueba distinta pero derivada de aquella obtenida con vulneración de derechos fundamentales, y la prueba independiente, que es la que, además de ser diferente, no guarda conexión alguna con la referida transgresión del derecho fundamental. La primera es ilícita y no puede conformar juicio probatorio; la segunda, sí. Esta distinción, como podrá apreciarse, no resulta en absoluto fácil, siendo necesario no sólo estar a las circunstancias del caso concreto, sino construir reglas generales que permitan establecer con la suficiente seguridad jurídica cuándo una prueba es independiente.

[110] ARRABAL PLATERO, P., *La prueba tecnológica*, cit., p. 79.

En esa labor, han aparecido los conceptos de independencia material, conexión de antijuridicidad y descubrimiento inevitable.

El primero de dichos conceptos hace referencia a una independencia *per se* entre la prueba obtenida ilícitamente y aquella que se obtiene sin tener nada que ver con la primera. Así, se ha entendido como pruebas independientes la confesión del acusado o la declaración de un testigo (SSTC 86/1995, de 6 de junio y 54/1996, de 26 de marzo, entre otras muchas).

El segundo parte de la regla del "nexo causal atenuado", como ponderación de intereses para acreditar la desconexión de antijuridicidad. La STC 320/2011, de 22 de abril, expone el funcionamiento del criterio cuando indica que a tal fin se ha establecido una doble perspectiva: una perspectiva interna, que atiende a la índole y características de la vulneración del derecho constitucional afectado (qué garantías de la injerencia en el derecho se han visto menoscabadas y en qué forma), así como al resultado de la infracción (el conocimiento adquirido) y una perspectiva externa, que atiende a las necesidades esenciales de tutela que la realidad y efectividad del derecho conculcado exige. Ambos criterios son de igual importancia, pues sólo si la prueba refleja resulta jurídicamente ajena a la vulneración del derecho y la prohibición de valorarla no viene exigida por las necesidades esenciales de tutela del mismo cabrá entender que su efectiva apreciación es constitucionalmente legítima, al no incidir negativamente sobre ninguno de los dos aspectos que configuran el contenido del derecho fundamental sustantivo.

Ese doble rasero también ha sido referido en la STC 81/1998, que venía a identificarlas con una perspectiva natural y otra jurídica. Conforme a ello, la perspectiva natural supondría que la prueba refleja derive materialmente de la inicialmente declarada nula; la perspectiva jurídica, referida a la secuencia de derechos afectados y a si, en fin, desde un punto de vista interno, su inconstitucionalidad se trasmite o no a la prueba obtenida por derivación de aquella

Desafortunadamente, y como se puede deducir, el criterio de la conexión de antijuridicidad implica que los tribunales deban realizar una valoración de cada caso concreto

con base en "juicios de experiencia", lo que afecta gravemente a la seguridad jurídica de los ciudadanos[111], además de carecer de escaso respaldo legal.[112]

Por último, el descubrimiento inevitable pretende atender a la circunstancia de que la prueba derivada hubiera sido igualmente conocida por otras vías independientes, respetuosas con los derechos fundamentales, según las reglas de la experiencia.[113] Supone, en definitiva, "la admisión de validez de la prueba derivada de forma natural de otra inconstitucional en todos aquellos casos en que se considere que, si no se hubiera producido la violación del derecho fundamental, la prueba contaminada habría terminado por ser inevitablemente adquirida de forma independiente durante el normal curso de la investigación"[114]. Tanto el Tribunal Supremo como el Tribunal Constitucional se refieren a este criterio en multitud de pronunciamientos, pero la doctrina lo ha criticado sobre la base de que parte de reconstrucciones de casos hipotéticos que no tienen por qué tener anclaje en la realidad[115].

c) Situación actual de la prueba ilícita

Si las SSTC 114/1984, de 29 de noviembre, y 85/1994, de 14 de marzo, supusieron hitos fundamentales en el régimen de la prueba ilícita en nuestro país, la STC 97/2019, de 16 de julio, ha supuesto una modificación radical de dicho instituto.

La referida sentencia desestima un recurso de amparo formulado contra la archiconocida STS 471/2017, de 23 de febrero[116], en la que el Tribunal Supremo, abandonando su postura mayoritaria de excluir el valor probatorio de las fuentes probatorias obtenidas ilícitamente por un particular[117], afirma "la posibilidad de valorar una fuente de prueba

---

[111] ASENCIO MELLADO, J. M., "La exclusión de la prueba ilícita en la fase de instrucción como expresión de garantía de los derechos fundamentales", *Diario La Ley*, 8009, 2013, Wolters Kluwer.
[112] ASENCIO MELLADO, J. M., "La STC 97/2019, de 16 de julio. Descanse en paz la prueba ilícita", cit., p. 3.
[113] ARRABAL PLATERO, P., *La prueba tecnológica*, cit., p. 92.
[114] GÁLVEZ MUÑOZ, L. A., *La ineficacia de la prueba obtenida con violación de derechos fundamentales: normas y jurisprudencia (TEDH, TC, TS, TSJ y AP) en los ámbitos penal, civil, contencioso–administrativo y social*, Thomson Reuters Aranzadi, 2003.
[115] FERNÁNDEZ ENTRALGO, J., "Prueba ilegítimamente obtenida", *Jueces para la democracia*, 7, 1989, Jueces para la Democracia.
[116] Caso *Falciani*, referido al reconocido robo de la lista Belarmino Falciani, que incluía cantidad ingente de información bancaria sobre titulares de fondos gestionados por la entidad suiza HSBC, sustraída por un empleado de la entidad y a través de la cual se iniciaron varios procesos por delito fiscal, procesos en los que, en lo que nos interesa ahora, se denunció la procedencia ilícita de la información y, en consecuencia, la imposibilidad de considerarla como elemento de cargo para enervar la presunción de inocencia..
[117] SSTS 239/2014, de 1 de abril, 596/2013, de 26 de junio y 1066/2009, de 4 de noviembre, entre otras muchas.

obtenida por un particular con absoluta desconexión de toda actividad estatal ajena en su origen a la voluntad de prefabricar pruebas, […] ya que la prohibición de valorar pruebas obtenidas con vulneración de derechos fundamentales cobra su genuino sentido como mecanismo de contención de los excesos policiales en la búsqueda de la verdad oculta en la comisión de cualquier delito". En definitiva, el Tribunal Supremo declara que no constituye un supuesto de prueba ilícita aquella obtenida por un particular con desconexión total y absoluta de actividad estatal, ajena a la voluntad de prefabricar pruebas.

Como decimos, la STC 97/2019 vino a confirmar la referida STS 471/2017, declarando que la garantía de ilicitud de las pruebas obtenidas con vulneración de derechos fundamentales no está contenida por sí misma, y de forma autónoma, en el resto de las garantías del artículo 24.2 CE como debería suceder a consecuencia de la supremacía de los derechos fundamentales en el ordenamiento jurídico sino que, en realidad, está integrada dentro del concepto de un proceso justo y equitativo. De este modo, la obtención de pruebas con vulneración de derechos fundamentales ha pasado a ser meramente instrumental y únicamente atendible si, además, se entiende vulnerada dicha idea de un proceso justo y equitativo[118]. Es palpable, por tanto, que se retoma el criterio del efecto disuasorio frente al de la protección incondicional de los derechos fundamentales. La consecuencia natural de este giro no puede ser otra que como venimos apreciando la relajación de la regla de exclusión de la prueba ilícita, al concluir que, en la actualidad, no resulta necesario mantener un estímulo disuasorio de tal magnitud[119].

La decisión del Tribunal Constitucional ha sido entendida como un complemento de la teoría de la conexión de antijuridicidad para limitar aún más el efecto de la ilicitud de la prueba, y viene a concluir que "la admisión de la ineficacia de tal prueba deriva siempre de un "juicio de experiencia", de un análisis de cada caso, de los intereses en juego"[120].

En definitiva, el TC decide en dicha sentencia que la exclusión de la prueba ilícita debe ser abordada desde las garantías del proceso justo, de manera que deja de ser una garantía procesal en sí misma, para pasar a estar supeditada a un análisis en el caso de

---

[118] ASENCIO MELLADO, J. M., "La prueba ilícita y su triste destino", en *La Administración de Justicia en España y en América, Vol. I*, Editorial Astigi, Sevilla, 2021, p. 192.
[119] ARMENTA DEU, T., "Prueba ilícita y regla de exclusión", cit., p. 128.
[120] ASENCIO MELLADO, J. M., "La STC 97/2019, de 16 de julio. Descanse en paz la prueba ilícita", cit., p. 17.

que la prueba así alcanzada rompa el equilibrio y la igualdad entre las partes. De esta manera, la prueba ilícita queda degradada a una mera irregularidad procesal, supeditada a la valoración de generalidades abiertas y no definidas objetivamente, generando inseguridad jurídica. Y así, definitivamente, la ilicitud probatoria queda reconducida a una simple vulneración infraconstitucional, supeditada a objetivos de justicia siempre atendibles por encima del valor de los derechos fundamentales[121].

En esta tendencia apreciable desde el punto de vista histórico de sacrificar garantías liberales con la justificación de obtener una mayor seguridad, es perfectamente posible que nuestros tribunales flexibilicen, en algunos supuestos, incluso la exigencia de autorización judicial.

Sin ir más lejos, y aplicando esta cuestión general a nuestro prioritario objeto de estudio en una reciente sentencia, nuestro Tribunal Supremo ha alterado de manera sustancial el régimen de garantías aplicable al listado de llamadas –no a la agenda de contactos, sino a la relación de comunicaciones entrantes y salientes, de llamadas, recibidas, realizadas y perdidas– de un teléfono móvil, afirmando que para dicha actuación por parte de la Policía Judicial, no es necesaria autorización judicial cuando la medida resulte proporcional.

En particular, dicha sentencia (STS 87/2020, de 3 de marzo), para justificar su postura, expuso tan solo que "la injerencia se encuentra justificada dada la gravedad de los hechos, la urgencia y necesidad de investigación de los participantes en la operación, por lo que, ponderando los intereses en juego, puesto en relación con la motivación del auto autorizante de la medida que se remite al atestado policial, la injerencia en la intimidad se encontraba justificada y era proporcional a las circunstancias del caso concreto". Precisamente esta es la raíz de la cuestión problemática, pues debe entenderse, a nuestro juicio, que ello afecta al derecho al secreto de las comunicaciones, no al de la intimidad.

Interesa reseñar que la STS 444/2014, de 9 de junio, llegaba a afirmar lo contrario cuando, al recordar la admisión de los accesos policiales a la agenda de contactos telefónicos sin autorización judicial, afirmaba también que "distinto sería el caso si se hubiese producido el acceso policial a cualquier otra función del teléfono móvil que pudiera desvelar procesos comunicativos, como por ejemplo el acceso al registro de llamadas

[121] ASENCIO MELLADO, J. M., "La STC 97/2019, de 16 de julio. Descanse en paz la prueba ilícita", cit.

entrantes y salientes". Parece, pues, que en la referida STS 444/2014 el propio Tribunal Supremo reconoce que tal actuación supondría una inmisión en el derecho fundamental al secreto de las comunicaciones, en cuanto que "pudiera desvelar procesos comunicativos". Automáticamente, ello nos sitúa en el terreno del monopolio jurisdiccional en materia de inmisiones en el referido derecho y, además, nos ubica en los artículos 588 *ter* a) y siguientes LECrim, relativos a la interceptación de comunicaciones telemáticas, cuya única posibilidad de adopción urgente queda prevista en el apartado 3 del artículo 588 *ter* d) LECrim, exclusivamente para supuestos de actuación de bandas armadas o elementos terroristas, previa autorización del Ministro del Interior o, en su defecto, del Secretario de Estado de Seguridad[122].

De igual modo, aunque se entendiera que la referida actuación supondría tan sólo un registro de dispositivo de almacenamiento masivo de la información, previsto en los artículos 588 *sexies* y siguientes LECrim, tampoco se habría cumplido con lo previsto en el artículo 588 *sexies* c) LECrim para los supuestos de urgencia.

La postura del Tribunal Supremo en el caso analizado, validando una actuación policial que no ha seguido el cauce legalmente previsto –588 *ter* d).3 o 588 *sexies* c) LECrim– por entender que constituyó una medida proporcional y justificada conforme a las circunstancias del caso, supone una manifestación más en nuestro sistema judicial del asentamiento de la idea de que es necesario un cierto sacrificio de derechos fundamentales para garantizar la seguridad de nuestra sociedad.[123]

En realidad, la postura del Tribunal Supremo casa con una óptica que únicamente funcione bajo los parámetros de eficiencia y eficacia, que desde luego se ha convertido en uno de los objetivos primordiales de las políticas públicas desde los últimos años[124].

En ese sentido, se aprecia cómo el argumento de la sentencia convierte el requisito de la proporcionalidad de la medida en una vía de escape para que aquellas diligencias que, debiendo haber sido autorizadas previamente, no lo fueron. En realidad, la postura mantenida por el tribunal equivale a afirmar que lo determinante es que la medida sea

---

[122] Exigiendo en todo caso comunicación inmediata al juez competente en el plazo máximo de 24 horas, que deberá confirmar la medida.
[123] ASENCIO MELLADO, J. M., "La prueba ilícita y su triste destino", cit.
[124] LUACES GUTIÉRREZ, A. I., "La conformidad en el Anteproyecto de Ley de Medidas de Eficiencia Procesal del Servicio Público de Justicia", en *El impacto de la oportunidad sobre los principios procesales clásicos: Estudios y diálogos, 2021, pp. 289–308*, Iustel, 2021, p. 289.

proporcionada, con independencia de que no haya sido sometida a autorización previa, cuando debió serlo, y que dicha proporcionalidad sanará cualquier deficiencia procedimental. Bajo ese punto de vista, resulta que la función del órgano judicial pasa de ser autorizante a revisora. Esto, a su vez, implica que esta revisión debe efectuarse sin atender a los resultados de la medida. Pero ¿actúa así realmente? A nuestro juicio, tanto la STC 97/2019 como la doctrina del TEDH en materia de delitos graves pueden llevar a que los órganos judiciales comprueben la proporcionalidad de la medida transgresora atendiendo a cuáles sean los delitos descubiertos, lo que abriría un peligroso horizonte en lo que se refiere a la protección de derechos fundamentales.

Estas posturas coinciden en cierta medida con la evolución actual de la teoría de la prueba ilícita en Estados Unidos, en donde han provocado el declive de la aplicación de esta figura en las últimas décadas, considerando que su principal finalidad, la de disuadir al poder público de investigar los delitos sin vulnerar los derechos y libertades fundamentales de los ciudadanos, ya se encuentra satisfecha mediante la profesionalización de las fuerzas de policía y el incremento de la disciplina policial. A nuestro juicio, constituye una manifestación importante de la, a nuestro parecer, discutible tendencia a limitar derechos y libertades en aras de la seguridad.

El cúmulo de cambios operados en la teoría de la prueba ilícita ha provocado que se eleven voces desde la doctrina reclamando una regulación específica[125] y con rango de ley en la materia que indique sin dubitaciones el fundamento de la regla de exclusión probatoria y las excepciones de dicha regla de exclusión[126], así como los criterios que podrán servir para ponderar los intereses en conflicto, a fin de dotar de una mínima seguridad jurídica al proceso valorativo que deberá realizar, en cada caso, el tribunal[127].

---

[125] DÍEZ–PICAZO GIMÉNEZ, I., "Algunas ideas sobre la prueba ilícitamente obtenida", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, pp. 575–590*, Ediciones Jurídicas Castillo de Luna, 2020, p. 577.

[126] ÁLVAREZ SÁNCHEZ DE MOVELLÁN, P., "Ponderaciones» judiciales en materia de prueba prohibida y garantías para la nueva investigación en el proceso penal", en *Exclusiones probatorias en el entorno de la investigación y prueba electrónica, 2020, pp. 105–140*, Reus, 2020, p. 116.

[127] FUENTES SORIANO, O., "La prueba prohibida aportada por particulares: a la luz de las nuevas tecnologías", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, pp. 715–744*, Ediciones Jurídicas Castillo de Luna, 2020, p. 741, fecha de consulta 17 agosto 2021, en https://dialnet.unirioja.es/servlet/articulo?codigo=7870311.

6. MARCO NORMATIVO: LA TRASCENDENCIA DE LA REFORMA OPERADA POR LA LEY ORGÁNICA 13/2015

A. NOTAS GENERALES

La Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales, ha introducido unas sustanciales reformas en materia de diligencias de investigación que, aunque no pueden ser el objeto principal de nuestro estudio, son de obligada mención.

Con esta reforma, además, se han asumido las obligaciones derivadas de la ratificación del Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2011, que prevé la aplicación de dichas exigencias no solo a los delitos informáticos en cuanto tales, sino a toda obtención de pruebas electrónicas, con independencia de la naturaleza del delito investigado, de conformidad con lo dispuesto en el artículo 14.2 c) del referido convenio[128].

B. SITUACIÓN ANTERIOR A LA REFORMA

En lo que se refiere a los propios medios de investigación, hasta la reforma operada por la LO 13/2015, nuestra LECrim contenía únicamente la regulación de los medios de investigación "tradicionales"[129].

Sin embargo, estos medios de investigación, aunque pudieran resultar de utilidad en la persecución del cibercrimen, no eran ni mucho menos suficientes, pues no se ajustan específicamente al medio en el que la propia conducta se verifica (esto es, el *ciberespacio*).

En el momento de la aprobación de la LECrim, las circunstancias tecnológicas de la época provocaron que solamente pudiera contemplar las intervenciones de las comunicaciones postales y telegráficas (artículos 579 y siguientes). Tras la aprobación de la Constitución Española de 1978, esta regulación quedó modernizada con la Ley Orgánica 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal, que incorporó las intervenciones o escuchas telefónicas en los apartados 2º a 4º del artículo 579, y con

---

[128] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 388.
[129] Como el examen del imputado (artículos 385 a 409), el interrogatorio de los testigos (artículos 410 a 455), los informes periciales (artículos 456 a 484), la entrada y registro de lugar cerrado (artículos 545 a 572), el secuestro de libros y papeles (artículos 573 a 578), la intervención de las comunicaciones postales, telegráficas y telefónicas (artículos 579 a 588) o la toma de muestras biológicas del sospechoso (artículo 326.II)

la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, que incorporó la regulación relativa a la intervención de los datos electrónicos de tráfico[130].

Posteriormente, y en lo que interesa a nuestra investigación, la LECrim fue reformada mediante la LO 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. La regulación en nuestro sistema procesal penal en lo relativo a la intervención de las comunicaciones telemáticas, así como el acceso a los llamados datos de tráfico y, en general, cualquier medida de investigación tecnológica, ha sido extremadamente pobre hasta la reciente reforma introducida por LO 13/2015, que es una más de las continuas reformas parciales de las que viene siendo objeto nuestra Ley de Enjuiciamiento Criminal, ante la dificultad de ejecutar una reforma global[131].

Hasta la aprobación de dicha reforma, el evidente vacío legal se ha venido cubriendo gracias a normas ajenas al ámbito penal y a una abundante jurisprudencia que trataba de aplicar extensivamente las escasas normas sobre intervenciones telefónicas[132], postales y telegráficas (contenidas en los artículos 579 y siguientes LECrim) al resto de modalidades comunicativas que iban surgiendo con la revolución tecnológica. Esto, aunque fuera suficiente para dar cobertura a las actuaciones de investigación ante la jurisdicción nacional, ha merecido conocidos reproches internacionales.

En efecto, hasta la subsanación de dicha insuficiencia normativa esta situación de anomia fue colmada mediante la jurisprudencia de los tribunales, de los que hay que destacar las posiciones del TEDH y de nuestros tribunales internos.

El TEDH ha exigido tradicionalmente que exista previsión legal de las medidas limitativas de los derechos reconocidos en el CEDH[133]. Así, ha interpretado el concepto de vida privada previsto en el artículo 8 CEDH en un sentido muy amplio, que incluye elementos tan dispares como la integridad física y psicológica de una persona, la identificación de su género, el nombre y la orientación sexual, los datos sobre su salud y

---

[130] GIMENO SENDRA, J. V., *Derecho procesal penal*, cit.
[131] NADAL GÓMEZ, I., "El Régimen de los hallazgos casuales en la Ley 13/2015, de modificación de la ley de Enjuiciamiento criminal", cit., p. 2.
[132] CUADRADO SALINAS, C., "Registro informático y prueba digital. Estudio y análisis comparado de la ciberinvestigación criminal en Europa", cit., p. 2.
[133] GIMENO SENDRA, J. V., *Derecho procesal penal*, cit., p. 402.

pertenencia étnica, y el desarrollo personal, incluyendo el derecho a establecer y desarrollar relaciones con otros seres humanos y la sociedad en su conjunta. En materia de aplicación de la tecnológica a las funciones de investigación de las conductas delictivas, el TEDH se ha pronunciado sobre la proporcionalidad de la interceptación de las telecomunicaciones (SSTEDH *Valenzuela Contreras c. España*, de 30 de abril de 1998 y Bugallo c. España, de 18 de febrero de 2003; así como el auto de inadmisión en el caso *Abdulkadir Coban c. España*, de 25 de septiembre de 2006), el rastreo e identificación de una dirección IP (STEDH *K.U. c. Finlandia*, de 2 de diciembre de 2008), la recopilación sistemática y el archivo de datos a través de instrumentos tecnológicos por parte de las autoridades policiales y de seguridad (STEDH *Leander c. Suecia*, de 26 de marzo de 198), incluyendo los supuestos de datos recopilados de lugares públicos (SSTED *Rotaru c. Rumania*, de 4 de mayo de 2000; *PG y JH c. Reino* Unido ,de 25 de septiembre de 2001; *Peck c. Reino Unido*, de 28 de enero de 2003, y o *Shomovolos c. Rusia*, de 21 de junio de 2011), la utilización de micrófonos en residencias privadas (STED *Vetter c. Franc*ia, de 31 de mayo de 2005), el uso del GPS por la policía (STED *Uzun c. Alemania*, de 2 de septiembre de 2010)[134].

En particular, en su sentencia de 30 de abril de 1998, *Valenzuela Contreras c. España*, el TEDH declaró que, aunque en el artículo 18.3 de la Constitución Española se reconoce una base legal en materia de limitación del derecho al secreto de las comunicaciones (al garantizar el secreto de las mismas excepto resolución judicial), dicho precepto no podía satisfacer, por sí solo, las condiciones exigidas por el CEDH para que pudiera entenderse que dichas injerencias estaban previstas en la ley y garantizaban el respeto al derecho a la vida privada y de la correspondencia, superando el juicio de proporcionalidad, pues ni en el artículo 18.3 CE ni en ninguna parte del ordenamiento jurídico español se establecía la definición de las categorías de personas susceptibles de ser sometidas a vigilancia telefónica judicial, la naturaleza de las infracciones a que puedan dar lugar, la fijación de un límite de la duración de la ejecución de la medida, las condiciones de establecimiento de los atestados que consignen las conversaciones interceptadas y la utilización y borrado de las grabaciones[135].

---

[134] ORTIZ PRADILLO, J. C., "El impacto de la tecnología en la investigación penal y en los derechos fundamentales", cit., p. 321.
[135] ORTIZ PRADILLO, J. C., *Problemas procesales de la ciberdelincuencia*, cit., p. 229.

Posteriormente, tras la entrada en vigor del artículo 579 LECrim, el TEDH volvió a condenar a España en su sentencia de 18 de febrero de 2003, *Prado Bugallo c. España*, declarando la vulneración del artículo 8 CEDH por entender que la redacción del citado artículo 579 LECrim no colmaba el requisito de la previsión legal de la injerencia al no ofrecer una reglamentación exhaustiva de la materia, así como que la jurisprudencia creada para colmar el vacío legislativo no era suficiente para evitar la arbitrariedad de los poderes públicos. En concreto, afirmaba que "las garantías introducidas por la Ley de 1988 no responden a todas las condiciones exigidas por la jurisprudencia del Tribunal, especialmente en las sentencias *Kruslin c. Francia* y *Huvig c. Francia*, para evitar los abusos. Se trata de la naturaleza de las infracciones susceptibles de dar lugar a las escuchas, de la fijación de un límite a la duración de la ejecución de la medida, y de las condiciones de establecimiento del procedimiento de trascripción de las conversaciones interceptadas. Estas insuficiencias afectan igualmente a las precauciones a observar, para comunicar intactas y completas las grabaciones realizadas, a los fines del eventual control por el juez y la defensa. La Ley no contiene ninguna disposición en relación con ello".

En España, los tribunales han centrado sus esfuerzos en materia de licitud y admisibilidad probatoria sobre las evidencias obtenidas mediante la aplicación de tecnología a la investigación criminal, a la vista de la obsoleta legislación procesal que debía darles cobertura –con la consiguiente ventaja, todo hay que decirlo– para la investigación policial, cuyas técnicas gozaban del más absoluto secreto. Puede decirse que, desde el primer momento, nuestros tribunales han considerado legítima la injerencia efectuada por los poderes públicos cuando se respetaban las pautas establecidas jurisprudencialmente, sin que la ausencia de regulación expresa en la ley pudiera determinar, por sí sola, la vulneración del derecho fundamental en cuestión[136].

Así, la doctrina del TC se caracteriza por realizar cambios paulatinos, pasando, en materia de ilicitud de la prueba por vulneración de derechos fundamentales, de la teoría directa a la refleja y de ahí a la teoría de la conexión de antijuridicidad. Aunque el TC considera necesario establecer una serie de garantías frente a los riesgos existentes para los derechos y libertades públicas a causa del uso indebido de la informática en las diligencias de investigación (STC 173/2011, de 7 de noviembre), su doctrina ha venido evolucionando hasta el punto de aceptar, como sucede en la STC 97/2019, de 16 de julio, la

[136] ATS de 18 de junio de 1992 y STC 49/1999, de 15 de abril, y 184/2003, de 23 de octubre.

eventual validez de pruebas obtenidas con vulneración de derechos fundamentales cuando no se vulnera el derecho a un proceso justo y equitativo, atendidas las circunstancias concurrentes.

Por su parte, el Tribunal Supremo ha dictado múltiples resoluciones en materia de utilización de la tecnología por la policía en sus funciones de investigación delictiva. La doctrina[137] distingue tres grupos de resoluciones: aquellas que se refieren al empleo de diversos instrumentos tecnológicos y la necesidad, o no, de la previa autorización judicial (SSTS de 20 de mayo de 2008, de 18 de noviembre de 2008, y de 28 de enero de 2009, entre otras muchas); aquellas que se refieren al funcionamiento y utilización del sistema informático SITEL (SSTS de 5 de febrero de 2008, de 20 de mayo de 2008, y de 13 de marzo, 29 de junio, 6 de julio y 5 de noviembre de 2009); y otras relativas a métodos especialmente novedosos de investigación, como las grabaciones de conversaciones entre presos penitenciarios (SSTS de 10 de febrero de 1998 y 2 de junio de 2010)[138].

Los esfuerzos de los órganos judiciales españoles parece que no cayeron en balde pues, con el auto de inadmisión de 25 de septiembre de 2006 (Abdulkadir Coban c. España), el TEDH acepta que las insuficiencias del ordenamiento jurídico español fueron paliadas por la jurisprudencia, que contiene reglas claras y detalladas para la práctica de las injerencias y precisa con suficiente claridad y extensión las modalidades de ejercicio del poder público aspecto, aunque mantiene la deseabilidad de que se produjera una modificación legislativa que incorporase dichos principios jurisprudenciales al ordenamiento jurídico[139].

Partiendo de la situación jurisprudencial y doctrinal descrita y atendiendo, especialmente, a los constantes pronunciamientos del TEDH que, invariablemente, destacaban la falta de cumplimiento del ordenamiento jurídico español del requisito de la previsión legal suficiente para la adopción de cualquier medida de investigación que supusiera

---

[137] ORTIZ PRADILLO, J. C., "El impacto de la tecnología en la investigación penal y en los derechos fundamentales", cit., p. 331.

[138] Interesa traer a colación, igualmente, distintas sentencias del Tribunal Constitucional alemán en este asunto: la sentencia de 15 de diciembre de 1983, que aludía por primera vez al derecho a la autodeterminación informativa, la sentencia de 30 de marzo de 2004, sobre los límites aplicables a la vigilancia acústica del domicilio, la sentencia de 12 de abril de 2005, sobre aplicación de balizas GPS por parte de la policía en un vehículo de un acusado, y la sentencia de 27 de febrero de 2008, que con ocasión de los registros *online* reconoció la existencia de un derecho fundamental a la garantía de confidencialidad e integridad de los equipos informáticos, como señala Ortiz Pradillo, J.C., en J. C. ORTIZ PRADILLO, "El impacto de la tecnología en la investigación penal y en los derechos fundamentales", cit., p. 327

[139] ORTIZ PRADILLO, J. C., *Problemas procesales de la ciberdelincuencia*, cit., p. 229.

una injerencia en cualquiera de los derechos reconocidos en el CEDH, la LO 13/2015 ha procurado atender la necesidad del legislador español de cumplir con la doctrina del TEDH en la materia y de colmar la laguna legal existente en materia de diligencias de investigación tecnológicas.

No en vano, en el apartado IV de la exposición de motivos de dicha LO 13/2015, el legislador ha expuesto las motivaciones que justifican la adopción de la normativa que contiene, indicando que el paso del tiempo y el surgimiento de una nueva realidad social no es algo que el ordenamiento jurídico, y menos la parte del mismo que regula el proceso penal –presupuesto para el ejercicio del *ius puniendi*– de una sociedad, pueda desoír. En ese sentido, y reconociendo esta obligación de todo el ordenamiento y, especialmente, de las ramas del mismo que afectan directamente a la vigencia de los derechos y libertades fundamentales, el legislador llama la atención sobre las ya no tan nuevas tecnologías y formas de interacción con comportan y, especialmente, sobre el flujo de información que genera el propio uso de estas tecnologías –basadas en la comunicación–, que ofrece posibilidades sin parangón tanto para la comisión de comportamientos que merezcan un reproche penal como para la investigación y retribución de los mismos por el poder público[140]. La doctrina ha referido que es inevitable entender que, más bien, supone una toma de conocimiento del carácter inevitablemente tardío de la reforma[141].

Es evidente que la regulación de la nueva realidad tecnológica ha planteado también la necesidad de diferenciar el ámbito físico del ámbito virtual en el plano procesal penal. Este es el motivo de que el artículo 579 LECrim acote específicamente su ámbito material, limitándolo a la detención y apertura de la correspondencia escrita y telegráfica.

La LO 13/2015, en todo caso, responde a una situación que ya había sido tachada de inaplazable desde cualquier perspectiva, constitucional, nacional o internacional[142], pudiendo citar, por todas, la STC 253/2006, que concluía indicando que "la regulación de las intromisiones en la privacidad del investigado en un proceso penal no puede subsanarse acudiendo a un voluntarista expediente de integración analógica que desborda los límites de lo constitucionalmente aceptable."

---

[140] GIMENO SENDRA, J. V., *Derecho procesal penal*, cit., p. 404.
[141] *Ibid.*, p. 405.
[142] *Ibid.*, p. 407.

A este respecto, se ha venido afirmando que la regulación de las medidas de investigación tecnológica permanecía sumida en "la más absoluta indigencia jurídica", con el consiguiente perjuicio para la investigación y represión de la cibercriminalidad[143].

C. CONTENIDO DE LA REFORMA EN MATERIA DE DILIGENCIAS DE INVESTIGACIÓN

La reforma operada por la LO 13/2015 que venimos analizando ha incluido en la LECrim una regulación expresa de las llamadas medidas de investigación tecnológica: i) la interceptación de las comunicaciones telefónicas y telemáticas; ii) la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, iii) la utilización de dispositivos técnicos de seguimiento, iv) localización y captación de la imagen, v) el registro de dispositivos de almacenamiento masivo de la información y vi) los registros remotos sobre equipos informáticos.

La regulación de esas medidas de investigación tecnológica se halla contenida en los artículos 588 *bis* y siguientes LECrim que, a su vez, se encuentran distribuidos en los capítulos IV a X del título VIII (denominado "De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución Española"), contenido en el Libro II.

El contenido de los referidos capítulos, en términos sintéticos y meramente enunciativos, es el que exponemos a continuación.

El capítulo IV contiene la regulación de las disposiciones comunes que serán de aplicación a todas las modalidades de limitación digital de los derechos reconocidos en el artículo 18 CE. En concreto, regula los principios rectores generales (artículo 588 *bis* a), la solicitud de autorización judicial (artículo 588 *bis* b), la resolución judicial que acuerde la medida (artículo 588 *bis* c), el carácter secreto de las actuaciones (artículo 588 *bis* d), la duración de la medida (artículo 588 *bis* e), la solicitud de prórroga de la medida (artículo 588 *bis* f), las formas de control de la medida (artículo 588 *bis* g), la afectación a terceras personas (artículo 588 *bis* h), la posibilidad de utilizar la información obtenida en la ejecución de la medida en un procedimiento distinto, así como el tratamiento que deba darse a los descubrimientos casuales (artículo 588 *bis* i), el cese de la medida

[143] JIMÉNEZ SEGADO, C.; PUCHOL AIGUABELLA, M., "Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección datos", *Diario La Ley*, 8676, 2016, Wolters Kluwer.

(artículo 588 *bis* j), y la destrucción de registros originales que se hubieran originado (artículo 588 *bis* k).

El capítulo V contiene la regulación de las interceptaciones de las comunicaciones telefónicas y telemáticas, y se organiza en tres secciones diferenciadas. La sección 1ª contiene las disposiciones generales que regularán toda medida de interceptación de comunicaciones telefónicas y telemáticas, y regula los presupuestos necesarios para su adopción (artículo 588 *ter* a), el ámbito de aplicación (artículo 588 *ter* b), la afectación a tercero (artículo 588 *ter* c), la solicitud de autorización judicial (artículo 588 *ter* d), el deber de colaboración (artículo 588 *ter* e), el control de la medida (artículo 588 *ter* f), su duración (artículo 588 *ter* g), la solicitud de prórroga (artículo 588 *ter* h), y el acceso de las partes a las grabaciones (artículo 588 *ter* i). La sección 2ª regula la incorporación al proceso de datos electrónicos de tráfico o asociados (artículo 588 *ter* j). La sección 3ª, finalmente, regula el acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad; en concreto, se refiere a la identificación mediante el número IP (artículo 588 *ter* k), mediante captación de códigos de identificación del aparato o de sus componentes (artículo 588 *ter* l) y a la identificación de titulares, terminales o dispositivos de conectividad (artículo 588 *ter* m).

El capítulo VI regula las actividades de captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos. En concreto, regula la grabación de las comunicaciones orales directas (artículo 588 *quater* a), los presupuestos necesarios (artículo 588 *quater* b), el contenido de la resolución judicial que acuerde dicha medida (artículo 588 *quater* c), las formas de control de la medida (artículo 588 *quater* d) y su cese (artículo 588 *quater* e).

El capítulo VII aborda la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización. En concreto, regula la captación de imágenes en lugares o espacios públicos (artículo 588 *quinquies* a), a la utilización de dispositivos o medios técnicos de seguimiento y localización (artículo 588 *quinquies* b), y a la duración de la medida (artículo 588 *quinquies* c).

El capítulo VIII se consagra al registro de dispositivos de almacenamiento masivo de información. En concreto, regula la necesidad de que la resolución que lo acuerde sea motivada de manera individualizada (artículo 588 *sexies* a), al acceso a la información de

dispositivos electrónicos incautados fuera del domicilio del investigado (artículo 588 *sexies* b), y a la autorización judicial que lo acuerde (artículo 588 *septies* c).

El capítulo IX por su parte, se refiere a los registros remotos sobre equipos informáticos. En concreto, se refiere a los presupuestos (artículo 588 *septies* a), deber de colaboración (artículo 588 *septies* b) y duración máxima (artículo 588 *septies* c).

El capítulo X, finalmente, contiene la regulación de las medidas de aseguramiento. En concreto, regula la orden de conservación de datos (artículo 588 *octies*).

En cuanto a la regulación legal de estas medidas de investigación, es necesario destacar que las diligencias de investigación consistentes en la intervención de los actos de comunicación efectuados mediante vía telefónica o electrónica habilitada judicialmente están previstas en el artículo 18.3 de la Constitución, cuando dispone que "se garantiza el secreto de las comunicaciones y, en especial, de las postales telegráficas y telefónicas, salvo resolución judicial". Como apunta la doctrina[144], en virtud del contenido integrador de las normas destinadas a tutelar los derechos fundamentales que ostentan los Pactos Internacionales de derechos Humanos, conforme al artículo 10.2º de la Constitución, dicho precepto debe interpretarse de acuerdo a con lo dispuesto en el artículo 8 del CEUDH, a la luz de la doctrina del TEDH, que es el órgano jurisdiccional encargado de garantizar su aplicación.

Por otro lado, y a nivel de la regulación nacional, este tipo de diligencias de investigación se instauró mediante la Ley Orgánica 7/1984, que incorporó al Código Penal entonces vigente los artículos 192 *bis* y 497 bis, reguladores del delito de escuchas telefónicas clandestinas (posteriormente tipificado en los artículos 536, 197 y 198 del Código Penal), y mediante la Ley Orgánica 4/1988, que modificó el artículo 579 de la LECrim para que incluyera expresamente, como acto de investigación, las intervenciones telefónicas. Antes de estas disposiciones, en nuestro ordenamiento jurídico podemos encontrar el artículo 17 de la ya derogada LO 9/1984 la LO 4/1981, sobre estados de alarma, excepción y sitio. En la actualidad, además de la regulación específica del artículo 588 LECrim, hay que citar los supuestos especiales del artículo 51 lo 1/1989 y en el artículo único de la LO 2/2002 de 6 de mayo.

---

[144] GIMENO SENDRA, J. V., *Derecho procesal penal*, cit., p. 409.

D. CONTENIDO DE LA REFORMA EN MATERIA DE CIBERPATRULLAJE

En cuanto al objeto de nuestra investigación, que no es sino la actividad de prevención y vigilancia de las Fuerzas y Cuerpos de Seguridad del Estado y su incidencia en el proceso penal, la reforma apenas incide en él. Únicamente pueden mencionarse como aplicables los artículos 579 bis, en la medida en que delimita el ámbito de los hallazgos casuales –que exigen, como veremos, la existencia de una diligencia de investigación válidamente ejecutada– y los artículos 588 *ter* k), l) y m), relativos a diligencias de investigación que pueden ser realizadas por la Policía Judicial sin necesidad de autorización judicial, y de los que posteriormente nos ocuparemos.

En ese sentido, el marco jurídico de la actividad de *ciberpatrullaje* por la Policía Judicial no ha variado con ocasión de la reformo,

a operada por la LO 13/2015, debiendo estarse a lo dispuesto en el artículo 282 LECrim[145], el artículo 547 LOPJ[146], y el artículo 11 LFFCCSS[147].

A lo anterior hay que añadir, también, los artículos 588 *bis* y siguientes LECrim, que al contener las disposiciones generales aplicables a las diligencias de investigación tecnológica afectan también a las previstas en los artículos 588 *ter* k), l) y m) LECrim, toda vez que estas han resultado objeto de dicha consideración en la ley de reforma.

---

[145] "La Policía Judicial tiene por objeto y será obligación de todos los que la componen, averiguar los delitos públicos que se cometieren en su territorio o demarcación; practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la autoridad judicial. Cuando las víctimas entren en contacto con la Policía Judicial, cumplirá con los deberes de información que prevé la legislación vigente. Asimismo, llevarán a cabo una valoración de las circunstancias particulares de las víctimas para determinar provisionalmente qué medidas de protección deben ser adoptadas para garantizarles una protección adecuada, sin perjuicio de la decisión final que corresponderá adoptar al Juez o Tribunal".

[146] "La función de la Policía Judicial comprende el auxilio a los juzgados y tribunales y al Ministerio Fiscal en la averiguación de los delitos y en el descubrimiento y aseguramiento de los delincuentes. Esta función competerá, cuando fueren requeridos para prestarla, a todos los miembros de las Fuerzas y Cuerpos de Seguridad, tanto si dependen del Gobierno central como de las comunidades autónomas o de los entes locales, dentro del ámbito de sus respectivas competencias".

[147] "Las Fuerzas y Cuerpos de Seguridad del Estado tienen como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana mediante el desempeño de las siguientes funciones: g) Investigar los delitos para descubrir y detener a los presuntos culpables, asegurar los instrumentos, efectos y pruebas del delito, poniéndolos a disposición del Juez o Tribunal competente y elaborar los informes técnicos y periciales procedentes".

7. DERECHOS FUNDAMENTALES AFECTADOS POR LA ACTIVIDAD INVESTIGADORA EN MATERIA DE CIBERDELITOS

La obtención de la prueba digital afecta a los derechos fundamentales declarados en el artículo 18 CE, esto es, la intimidad personal, el secreto de las comunicaciones, la inviolabilidad domiciliaria (en los supuestos en que el dispositivo electrónico sea hallado en el marco de una entrada y registro en domicilio), y el derecho a la autodeterminación informativa en el ámbito de la protección de datos personales.

A pesar de que las referencias que traemos a continuación apuntan fundamentalmente al desarrollo de dichos derechos fundamentales en el marco de sus relaciones con los poderes públicos, es necesario recordar que los derechos fundamentales despliegan su vigencia tanto en las relaciones del ciudadano afectado con los poderes públicos (efecto directo o vertical) como en las relaciones entre los ciudadanos entre sí (efecto indirecto u horizontal)[148]. En tal sentido, la STC 18/1984, de 7 de febrero, recordaba que no podía interpretarse la Constitución de tal manera que los derechos fundamentales y libertades públicas únicamente tuvieran eficacia en relación con los poderes públicos.

A. DERECHO FUNDAMENTAL A LA INTIMIDAD

El derecho fundamental a la intimidad personal y familiar está reconocido en el artículo 18.1 CE, junto con los derechos fundamentales al honor y a la propia imagen, y también en el artículo 8 CEDH. Su régimen se desarrolla en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Es un derecho personalísimo, exclusivo de las personas físicas, irrenunciable y que se extingue con el fallecimiento, y tiene una doble dimensión, la personal y la familiar, reconociéndose ambas intimidades como merecedoras de protección, como destacan las SSTC 124/1985, de 17 de octubre y 69/1999, de 26 de abril, y la STS 592/2011, de 12 de septiembre. En según qué circunstancias, sus fronteras respecto de otros derechos fundamentales, como los de no declarar sobre la ideología, religión o creencias propias del artículo 16.2 CE, la inviolabilidad del domicilio del artículo 18.2 CE o el secreto de las comunicaciones del artículo 18.3 CE, pueden quedar difuminadas, como de hecho parece

[148] ÁLVAREZ CONDE, E., "El sistema constitucional español de derechos fundamentales", *Corts: Anuario de derecho parlamentario*, 15, 2004, Cortes Valencianas.

advertir la doctrina.[149] En definitiva, protege el ámbito personal y familiar de dignidad de los ciudadanos frente a la acción, al conocimiento y a la divulgación de terceros[150]

En cuanto a la determinación del contenido del derecho, conviene destacar las teorías que distinguen la existencia de tres niveles concéntricos de intimidad con protección creciente conforme más se aproximan al núcleo de la personalidad del individuo. Así, se distingue entre un nivel exterior o esfera pública, compuesto por todos aquellos conocimientos que el individuo libremente expone ante la sociedad; un nivel intermedio, en el que se incluirían los datos que el individuo compartiera con algunos individuos o grupos pequeños, pero excluyendo a grupos amplios y a la propia sociedad; y un nivel nuclear, en el que quedarían protegidos los datos a las relaciones afectivas, orientación sexual, creencias religiosas, posicionamiento ideológico y demás circunstancias sociales, físicas y profesionales, y que coincidiría con el ámbito protegido por el artículo 18.1 CE[151].

Decimos que esta cuestión merece ser destacada porque, quizás, sería necesario revisar la estructura en la que se ha construido ese derecho, habida cuenta de las posibilidades actuales de construcción de perfiles y predicción de comportamiento que ponen a nuestra disposición las altas capacidades de computación y el volumen masivo de los repositorios de datos de los usuarios de la red. En ese sentido, no podemos dejar de llamar la atención sobre cómo circunstancias de hecho que podrían entenderse comprendidas en el primer nivel de intimidad –el público o menos protegido–, disponiendo de una muestra lo suficientemente amplia, podrían permitir predecir suficientemente el contenido del nivel nuclear. También es necesario abordar, en ese sentido, el establecimiento de las delimitaciones suficientes que permitan determinar qué contenido se encuentra en qué nivel. Es conocido el concepto de expectativa de intimidad y cómo los propios actos de un sujeto determinan qué partes de su vida pueden o no quedar protegidas por el derecho a la

---

[149] ETXEBERRIA GURIDI, J. F., "La sentencia del TEDH «S. y Marper c. Reino Unido», de 4 de diciembre de 2008, sobre ficheros de ADN, y su repercusión en la normativa española", en *Derecho y nuevas tecnologías, Vol. 1, 2011 (Primera parte. Nuevas tecnologías, sociedad y derechos fundamentales), pp. 393–406*, Universidad de Deusto = Deustuko Unibertsitatea, 2011, fecha de consulta 23 abril 2020, en https://dialnet.unirioja.es/servlet/articulo?codigo=3461170.

[150] Como se extrae de las SSTC 231/1988, de 2 de diciembre; 197/1991, de 17 de octubre, 142/1993, de 22 de abril, 57/1994, de 28 de febrero, 98/2000, de 10 de abril, 186/2000, de 10 de julio, 70/2002, de 3 de abril, 218/2002, de 25 de noviembre, 127/2003, de 30 de junio, 23/2007, de 30 de junio o STS 882/2011, de 7 de diciembre

[151] GIMENO SENDRA, J. V., "Las intervenciones electrónicas y la policía judicial", *Diario La Ley*, 7298, 2009, Wolters Kluwer.

intimidad, pero consideramos que tal vez sería necesario plantearse si esa publicidad que a veces se nos refiere como aceptada no ha sido en realidad más bien impuesta por las plataformas correspondientes, incluso desconociendo el propio sujeto el tratamiento que dicha plataforma efectúe de sus datos.

En relación con esta cuestión, sí se ha reconocido por la doctrina que en el nivel intermedio pueden encontrarse datos que, aun no siendo propios de la esfera más nuclear de la intimidad, sí pueden ofrecer una visión importante del sujeto. Estos datos quedan protegidos dentro del derecho fundamental a la protección de datos personales[152].

Sobre los límites del derecho fundamental a la intimidad, la STC 11/1984, de 26 de noviembre, recordaba que todo derecho encuentra sus límites en la necesidad de proteger o preservar otros derechos constitucionales u otros bienes constitucionalmente protegidos, ya estuvieran previstos en la propia Constitución o en una norma derivada de ella. En ese sentido, el derecho a la intimidad encuentra sus límites en el consentimiento del titular y en los actos de injerencia que superen el requisito de la proporcionalidad, en sentido amplio, conforme a lo que se comentará en el apartado relativo a los principios que deben seguir las diligencias de investigación tecnológica.

En cuanto al consentimiento de la persona afectada, lo cierto es que este puede manifestarse tanto de forma expresa como tácita, pues los actos concluyentes pueden suponer autorización suficiente, según las SSTC 22/1984, de 17 de febrero, 196/2004, de 15 de noviembre, 209/2007, de 24 de septiembre, STS 97/2015, de 24 de febrero y STS 786/2015, de 4 de diciembre. En este punto, no podemos dejar de llamar la atención sobre que se admita la figura de un consentimiento tácito respecto de un derecho fundamental irrenunciable, por más que se haya concluido que "tampoco tendrán este carácter las [injerencias] consentidas por el propio interesado, posibilidad esta que no se opone a la irrenunciabilidad abstracta de dichos derechos, pues ese consentimiento no implica la absoluta abdicación de los mismos, sino tan sólo el parcial desprendimiento de alguna de las facultades que los integran"[153]. A juicio del TC, la notoriedad reduce el ámbito de intimidad constitucionalmente asegurado, pero los únicos motivos que legitiman una

[152] REVENGA SÁNCHEZ, M., "El derecho a la intimidad: un derecho en demolición (y necesitado de reconstrucción)", en *El derecho a la privacidad en un nuevo entorno tecnológico: XX Jornadas de la Asociación de Letrados del Tribunal Constitucional, 2016, pp. 71–98*, 2016.
[153] COTINO HUESO, L., *Derecho constitucional II: Derechos fundamentales*, Universitat de València, 2011, p. 237.

supremacía de las libertades de información son el interés general y la formación de opinión pública en una sociedad democrática. La aplicación de estos razonamientos ha llevado al concepto de "expectativa de intimidad", como criterio para determinar los límites de las intromisiones en la intimidad a los que una determinada persona ha prestado consentimiento, al que nos dedicaremos posteriormente, especialmente atendiendo a una sociedad en la que, como la nuestra, las compañías obligan a ceder ciertos aspectos de la privacidad para acceder a sus servicios.

Tampoco puede olvidarse que, como indicaba la STC 115/2013, "de conformidad con el artículo 18.3 CE, la intervención de las comunicaciones (telefónicas, telegráficas, postales o de cualquier otro tipo) requiere siempre de autorización judicial (a menos que medie el consentimiento previo del afectado), pero el artículo 18.1 CE no prevé esa misma garantía respecto del derecho a la intimidad, de modo que se ha admitido la legitimidad constitucional de que en algunos casos y con la suficiente y precisa habilitación legal, la policía realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas sin previa autorización judicial (y sin consentimiento del afectado), siempre que se hayan respetado las exigencias dimanantes del principio de proporcionalidad (por todas, SSTC 70/2002, de 3 de abril, FJ 10; 123/2002, de 20 de mayo, FJ 4; 56/2003, de 24 de marzo, FJ 2; 281/2006, de 9 de octubre, FJ 4; y 142/2012, de 2 de julio, FJ 2)".

B. DERECHO FUNDAMENTAL A LA INVIOLABILIDAD DEL DOMICILIO

El derecho a la inviolabilidad del domicilio queda reconocido en el artículo 18.2 CE, en el artículo 8 CEDH, y en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.

En cuanto a su relación con el derecho fundamental a la intimidad, en la STC 94/1999, de 31 de mayo, se ha afirmado que el derecho fundamental a la inviolabilidad domiciliaria protege de forma instrumental la vida privada de una persona[154].

Por lo que se refiere a su contenido, constituye el poder de su titular de impedir la agresión, entrada o permanencia de un tercero en su domicilio, por ser un ámbito reservado a su libertad más íntima. En ese sentido, se ha afirmado que "el domicilio constituye el espacio físico cerrado en el que el individuo puede ejercer su libertad más amplia e íntima, quedando formalmente protegido o inmune frente a toda clase de injerencia

[154] ARRABAL PLATERO, P., *La prueba tecnológica*, cit., p. 130.

externa"[155], que, interpretado funcionalmente, ha llevado a reconocer, en multitud de pronunciamientos judiciales, la condición de domicilio a espacios físicos diferentes, como habitaciones de hotel, tiendas de campaña, camarotes, caravanas, etc. Por el contrario, quedaría fuera de dicha concepción todos aquellos espacios en los que la persona titular no invocase privacidad alguna, como casas deshabitadas o con uso diferente al de su propia habitación, bares, restaurantes, tiendas de comestibles, gimnasios, almacenes, sótanos o cocinas de establecimientos abiertos al público, etc.

En cuanto a las limitaciones de este derecho fundamental, también hemos de analizar aquí el consentimiento del titular del derecho, la autorización judicial y la flagrancia delictiva. Por lo que se refiere al consentimiento, este debe ser otorgado por una persona con capacidad de obrar, informado, libre y expreso, claro e inequívoco, siendo inaceptable la denominada "intimidación ambiental"[156]. Así, lo declaran, entre otras, las SSTS 113/2013, de 15 de marzo, 1171/2011, de 9 de noviembre, 892/2008, de 26 de diciembre, y 2026/2004, de 14 de octubre, que también concluye recordando que "no se refieren solo a las declaraciones autoinculpatorias, se refieren también a la inexistencia de obligación alguna de proporcionar ninguna clase de elementos a la acusación que pudieran servir para los fines de esta".

En cuanto a la autorización judicial, esta debe revestir la forma de auto motivado, acordado por el Juez competente del territorio en el que se encuentra el domicilio. Partiendo del respeto debido al principio de proporcionalidad, deberá también hacer referencia expresa a las circunstancias personales, temporales y espaciales. Por último, la flagrancia puede suplir la ausencia de autorización judicial siempre que exista evidencia directa de la comisión de un delito que necesite de una actuación policial urgente e inmediata para evitar su consumación o la desaparición de sus huellas, debiendo interpretarse de manera restrictiva para garantizar el mayor respeto al derecho fundamental[157].

---

[155] RIVES SEVA, A. P., *La prueba en el proceso penal. Doctrina de la Sala Segunda del Tribunal Supremo*, Navarra, Aranzadi, 2022, p. 55.

[156] MARTÍN RÍOS, P., "La colaboración del investigado/encausado en el registro de dispositivos de almacenamiento masivo de información: ¿un supuesto de autoincriminación?", en *FODERTICS 6.0: los nuevos retos del derecho ante la era digital, 2017, pp. 161–171*, Comares, 2017, fecha de consulta 6 octubre 2020, en https://dialnet.unirioja.es/servlet/articulo?codigo=6200844.

[157] MATIA PORTILLA, F. J., "Delito flagrante e inviolabilidad del domicilio (Comentario a la STC 341/1993)", *Revista española de derecho constitucional*, vol. 14, 42, 1994, Centro de Estudios Políticos y Constitucionales (España).

Con ocasión del desarrollo de las nuevas tecnologías, el alcance de las injerencias en el derecho fundamental a la inviolabilidad domiciliaria también ha debido ser delimitado por nuestros tribunales.

En ese sentido, el Tribunal Supremo, en su STS 342/2013, de 17 de abril, ya advirtió que el acceso y registro legítimo de un domicilio no incluye el acceso al contenido de un ordenador o dispositivo de almacenamiento masivo de información. En todo caso, debe tenerse en consideración que hoy en día es perfectamente posible llevar a cabo una intromisión virtual en el propio domicilio utilizando instrumentos a distancia y sin mantener contacto directo, especialmente en los casos, cada vez más extendidos, de hogares automatizados. En este sentido, conviene recordar que la jurisprudencia viene permitiendo la observación policial desde el exterior cuando no existen elementos que protejan el espacio íntimo, como cortinas, ventanas, toldos o vallas (SSTS de 15 de abril de 1997 y de 18 de febrero de 1999), pero no así cuando el observador recurre a medios técnicos específicos (STS 329/2016, de 20 de abril[158], entre otras muchas)[159].

De esa manera, no se admiten tampoco, sin autorización judicial previa, medios técnicos de escucha que permitan una vigilancia acústica del domicilio, o de visión térmica, por ejemplo[160]. Del mismo modo, la STS 329/2016, de 20 de abril, declaró la nulidad de las pruebas obtenidas por los agentes de policía mediante el uso de prismáticos para observar dentro de un domicilio. Partiendo de ese argumento, se ha concluido que no contar con contraseña en un teléfono móvil o en un ordenador no puede entenderse como una renuncia a la intimidad o una invitación para que cualquiera pueda inspeccionarlo sin consentimiento del titular afectado[161].

---

[158] En la célebre "sentencia de los prismáticos", en la que el Tribunal Supremo concluyó que el alcance del derecho fundamental a la intimidad no depende de las medidas que se utilicen para protegerla, anulando la condena impuesta en la sentencia recurrida porque la principal prueba de cargo, al haberse obtenido mediante la vigilancia policial mediante prismáticos del interior de una vivienda, debía considerarse ilícita.

[159] "Nulidad de la prueba por la intromisión virtual en domicilio. Una breve reflexión sobre la observación policial ilícita de la intimidad personal y familiar", fecha de consulta 24 abril 2020, en https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAkNDIwsLI7Wy1KLizPw8WyMDQzMDM0MLkEBmWqVLfnJIZUGqbVpiTnEqANGdvcM1AAAAWKE.

[160] ORTIZ PRADILLO, J. C., *Problemas procesales de la ciberdelincuencia*, cit., p. 172.

[161] MARTÍN RÍOS, P., "El alcance del derecho al propio entorno virtual en la valoración de la evidencia digital", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, pp. 1259–1270*, Ediciones Jurídicas Castillo de Luna, 2020, p. 1268.

C. DERECHO FUNDAMENTAL AL SECRETO DE LAS COMUNICACIONES

El derecho al secreto de las comunicaciones se encuentra reconocido en el artículo 18.3 CE.

Este derecho protege el proceso de comunicación que se encuentre en marcha entre dos titulares del mismo, que pueden ser personas físicas o jurídicas, nacionales o extranjeras, tanto en cuanto a su existencia como en cuanto a su contenido, respecto de injerencias de terceros. Sin embargo, una vez que se finaliza la comunicación, la protección constitucional se tiene que realizar a través de otros derechos fundamentales, como el derecho a la intimidad. Según reiterada doctrina del Tribunal Constitucional, "la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos"[162]. Pese a ello la jurisprudencia entiende también comprometido este derecho cuando se accede a una comunicación a través de fuentes obtenidas mediante interceptación de la comunicación en curso, aunque el acceso a dichas fuentes se produzca después de terminada la comunicación[163]. El criterio para determinar si el secreto de las comunicaciones resulta o no afectado parece ser, por tanto, si los datos de la comunicación a que se accede han sido obtenidos con interferencia o sin interferencia del proceso de comunicación[164].

Llama la atención que este derecho protege los procesos comunicativos entre los titulares sin importar la trascendencia de su contenido, en contraposición a la protección material de que es merecedor el derecho a la intimidad, de modo que toda comunicación es secreta, pero no toda es íntima[165].

En cuanto al concepto de comunicación, puede definirse como aquel proceso comprendido entre dos personas para transmitir algún significado. En tal sentido, la STC 281/2006, de 9 de octubre, refiere que "los mensajes pueden expresarse no solo mediante

---

[162] STC 70/2002, de 3 de abril; STC 123/2002, de 20 de mayo; STC 56/2003, de 24 de marzo.
[163] STS de 28 de junio de 2007 y de 30 de noviembre de 2005, entre otras.
[164] VEGAS TORRES, J., "Sobre el alcance del secreto de las comunicaciones", en *Una filosofía del derecho en acción: homenaje al profesor Andrés Ollero, 2015, pp. 1609–1626*, Dirección de Estudios, Análisis y Publicaciones. Departamento de Publicaciones, 2015, p. 6, fecha de consulta 17 agosto 2021, en https://dialnet.unirioja.es/servlet/articulo?codigo=6323650.
[165] GARCÍA GONZÁLEZ, A., "Desdentado Bonete, Aurelio y Muñoz Ruiz Ana Belén, Control informático, videovigilancia y protección de datos en el trabajo.", *Revista Latinoamericana de Derecho Social*, 19, 2014, Instituto de Investigaciones Jurídicas.

palabras, sino a través de otro conjunto de signos o señales que componen otras clases de lenguajes", llegando incluso a admitirse tal condición en procesos en los que se han utilizado únicamente emoticonos, como se hace en la SAP Madrid 247/2017, de 31 de marzo.

En todo caso, merece la pena destacar que la protección que dispensa el derecho no afecta a aquellos que hayan formado parte del proceso comunicativo, aunque estos sí estarán vinculados por el debido respeto a la intimidad de su interlocutor. En ese sentido, la STC 114/1984, de 19 de noviembre, concluyó que cuando se graba una conversación entre terceros se vulnera el derecho reconocido en el artículo 18.3 de la Constitución, pero que cuando quien graba la conversación interviene en la misma dicho derecho no puede entenderse vulnerado por dicha sola causa, pues si se impusiera un deber de secreto genérico a cada uno de los interlocutores o de los corresponsables, se estaría vaciando de sentido a la protección de la esfera íntima personal establecida en el artículo 18.1, llevando a resultados prácticos "del todo irrazonables y contradictorios, en definitiva, con la misma posibilidad de los procesos de libre comunicación humana."

A lo anterior añadía el razonamiento de que el artículo 18.1 CE, al no universalizar el deber de secreto, reconoce, precisamente, la imposibilidad de imponerlo a todo interviniente en la conversación.

En cuanto al ámbito de aplicación, el efecto del derecho fundamental se produce sobre aquellas comunicaciones efectuadas entre sujetos determinados con independencia del medio (postal, telegráfico, telefónico, electrónico, etc.) empleado, pero no se extiende a aquellos que constituyan discursos a un colectivo[166].

Al contrario de lo que sucede respecto del resto de apartados del artículo 18 CE, el secreto de las comunicaciones sí está sometido expresamente al monopolio jurisdiccional para su limitación, por lo que solo el juez podrá autorizar que se realicen válidamente injerencias en tal derecho. Ello no impide, sin embargo, que en los casos relacionados con la actuación de bandas armadas o elementos terroristas y en los que concurra urgencia, de conformidad con el artículo 579 LECrim, dicha autorización judicial pase a ser, de hecho, una mera ratificación (sin olvidar también la posibilidad de abrir paquetes postales por parte de las autoridades administrativas y aduaneras, conforme a la Ley 43/2010, de 30

[166] ROMERO PAREJA, A., "Intervención de las comunicaciones", *Diario La Ley*, 7816, 2012, Wolters Kluwer.

de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal).

En cuanto a las medidas tecnológicas que puedan lesionar el derecho, la ley prevé, respecto a la interceptación de las comunicaciones telefónicas o telemáticas, que la autorización solo se conceda para delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión, delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación, delitos cometidos en el seno de un grupo u organización criminal y delitos de terrorismo[167]. En todo caso, hay que recordar que este derecho puede verse afectado no sólo con ocasión de las diligencias de interceptación de comunicaciones sino, también, en relación con las que consisten en registros de dispositivos de almacenamiento masivo de información digital, cuando entre los datos accedidos se encuentran soportes de procesos comunicativos efectuados.

Merece la pena recordar aquí que el acceso a la agenda de contactos de un investigado no supone una inmisión en el derecho fundamental al secreto de las comunicaciones, sino en el derecho a la intimidad. Así lo entendió, entre otras[168], la STS 493/2010, de 25 de abril, al indicar que la agenda de un teléfono móvil –entendiendo como tal el archivo de dicho aparato en el que consta un listado de números identificados normalmente por un nombre– es equiparable a una agenda en soporte de papel o electrónica, y que su registro u observación no supone la inmisión o injerencia en el derecho al secreto de las comunicaciones sino en el derecho a la intimidad. A su vez, ello comporta que dicho registro esté permitido a la policía siempre que resulte justificado con arreglo a los criterios de urgencia y necesidad y que se cumpla el requisito de proporcionalidad al ponderar los intereses en juego en el caso concreto (al contrario de lo que sucedería si se entendiera protegida por el derecho al secreto de las comunicaciones, en cuyo caso sería requisito indispensable la previa autorización judicial).

De igual modo, en la STS 444/2014, de 9 de junio, concluía el tribunal, con cita de la STC 115/2013, de 9 de mayo, que el acceso por parte de los agentes de policía, sin

---

[167] Si bien podrá llevarse a cabo con la orden del Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad en la investigación de delitos relacionados con la actuación de bandas armadas o elementos terroristas en los que concurra urgencia y existan razones fundadas, de conformidad con el artículo 588 ter d) LECrim.

[168] SSTS 316/2000, de 3–3; 1235/2002, de 27–6; 1086/2003, de 25–7; 1231/2003, de 25–9; 449/2006, de 17–4; y 1315/2009, de 18–12

consentimiento del afectado y sin autorización judicial, a la relación de números telefónicos contenidos en la agenda de contactos telefónicos de un teléfono móvil, no afecta al derecho al secreto de las comunicaciones del usuario de dicho aparato de telefonía sino, exclusivamente, al derecho a la intimidad. E, igualmente, concluía que así como la intervención de las comunicaciones requiere siempre de autorización judicial, el derecho a la intimidad no prevé esa misma garantía, por lo que se admite la legitimidad constitucional de que la policía realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas sin previa autorización judicial (y sin consentimiento del afectado), siempre que exista la suficiente y precisa habilitación legal y se hayan respetado las exigencias dimanantes del principio de proporcionalidad.

Ahora bien, también debe llamarse la atención sobre que, si se hubiese producido el acceso policial a cualquier otra función del teléfono móvil que pudiera desvelar procesos comunicativos, como por ejemplo el acceso al registro de llamadas entrantes y salientes, sí sería necesaria la previa autorización judicial. En nuestra opinión, entender que el acceso a la agenda de un teléfono, o a su registro de llamadas, únicamente vulnera el derecho a la intimidad de su titular obvia la especial naturaleza del soporte y la potencialidad lesiva que el acceso al soporte puede tener para la esfera individual. Es sencillamente imposible acceder al registro de llamadas de un teléfono móvil sin advertir, siquiera por equivocación o por casualidad, otros datos más íntimos de la persona (piénsese, por ejemplo, en una mera fotografía que se encuentre de fondo de pantalla del terminal) y, en todo caso, la potencialidad lesiva es tal y tan carente de control, que quizás sería conveniente que, en todo caso, se entendiera afectado algo más que el derecho a la intimidad de la persona. Se trata de terminales en los que está toda la vida del individuo, y no solamente en archivos que se encuentren "en local", esto es, en la memoria interna del dispositivo, sino que, normalmente, el dispositivo se encuentra autorizado para acceder a los diferentes servicios online (servidores de almacenamiento, redes sociales, cuentas bancarias, correo electrónico, aplicaciones de mensajería, etc.) cuyos servicios tenga contratados el titular del terminal.

D. DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

El derecho fundamental a la protección de datos, también conocido como derecho a la autodeterminación informativa, queda previsto en el artículo 18.4 CE –lo que, habida cuenta del momento histórico en que fue aprobada, es calificado como un hito por la

doctrina[169]–, y desarrollado por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Se ha definido como "la facultad de toda persona para ejercer control sobre la información personal almacenada en medios informáticos tanto por las administraciones públicas como entidades u organizaciones privadas"[170].

El derecho fundamental en cuestión ya fue abordado por las SSTC 290/2000 y 292/2000, de 30 de noviembre, que concluían que "el objeto de protección del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos sean o no fundamentales, porque su objeto no es solo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal" y que "persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado". Se configura inicialmente, por tanto, como "un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática"[171].

En la ya citada STC 292/2000, el Tribunal Constitucional concluía que "La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4). Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del

[169] ORTEGA GIMÉNEZ, A.; GONZÁLEZ MARTÍNEZ, J. A., "Protección de datos, secreto de las comunicaciones, utilización del correo electrónico por los trabajadores y control empresarial", *Diario La Ley*, 7188, 2009, Wolters Kluwer.
[170] LUCENA CID, I. V., "La protección de la intimidad en la era teconlógica: hacia una reconceptualización", *Revista internacional de pensamiento político*, 7, 2012, Laboratorio de Ideas y Prácticas Políticas.
[171] ARRABAL PLATERO, P., *La prueba tecnológica*, cit., p. 165.

art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran".

Adicionalmente, el contenido del derecho fundamental ha sido vinculado al del acceso de los ciudadanos a los archivos y registros de la Administración Pública, tal y como se prevé en el artículo 105 CE[172].

El referido control que tienen las personas físicas sobre la recogida, tratamiento y destino sus datos personales se articula, además, desde una doble perspectiva: por un lado, es necesaria la información previa, expresa, precisa e inequívoca sobre dichos extremos, dando a conocer al titular qué datos personales se tratan, la finalidad del tratamiento, y la posibilidad de ejercitar los denominados derechos ARCO (acceso, rectificación, cancelación y oposición), por otro lado, el titular de dichos datos debe prestar su consentimiento, de manera libre e informada, aunque no necesariamente de forma expresa. La relevancia de este derecho fundamental se ha descubierto conforme han ido avanzado las técnicas de recolección y tratamiento de los datos personales, situación que ha dado lugar incluso, con la STJUE C-131/12, al reconocimiento de un derecho no ya al borrado de dicha información, sino a que los motores de búsqueda de internet eviten que determinada información forme parte de sus resultados, lo que se ha conocido como derecho de supresión, o "derecho al olvido"[173].

[172] Atendiendo al desarrollo efectuado, entre otras, en las STEDH Társaság a Szabadságjogo–kért v. Hungary, de 14 abril 2009, Kenedi v. Hungary, de 26 mayo 2009 o Youth Initiative for Human Rights v. Serbia, de 25 de junio de 2013

[173] "Derecho de supresión («al olvido»): buscadores de internet", *AEPD,* fecha de consulta 25 abril 2020, en https://www.aepd.es/es/areas–de–actuacion/internet–y–redes–sociales/derecho–al–olvido.

E. DERECHO FUNDAMENTAL AL PROPIO ENTORNO VIRTUAL

Debemos comenzar recordando que, como es conocido, en nuestro ordenamiento jurídico no existe previsión de un derecho fundamental a la privacidad informática que se considere de manera autónoma y diferenciada de la manifestación genérica del derecho a la intimidad. Esta circunstancia destaca por sí misma, pues el secreto de las comunicaciones y la inviolabilidad del domicilio, que no dejan de ser sino manifestaciones de la intimidad igual de singulares y diferenciadas que la privacidad informática, sí tienen previsión específica al respecto. A pesar de ello, y como se ha indicado, con ocasión de la reforma operada por la LO 13/2015 se ha establecido, con rango de ley, la exigencia de autorización judicial cuando se trate de acceder al contenido de dispositivos de almacenamiento masivo[174].

En consecuencia, el derecho al propio entorno virtual es un derecho fundamental de creación jurisprudencial y recientísimo origen, concebido para amparar al conjunto de información cibernética que configura el perfil de un ciudadano en particular[175]. No está previsto explícitamente en nuestro ordenamiento jurídico, sino que ha sido la práctica de nuestros tribunales la que lo ha descubierto, sin perjuicio de la silueta que marcan los artículos 588 y siguientes LECrim. En general, este derecho interviene cuando se accede al conjunto de información digital que acumula una persona en su dispositivo personal[176].

Generalmente, viene a señalarse como primer reconocimiento del mismo la sentencia del Tribunal Constitucional alemán dictada el 27 de febrero de 2008, en la que, tras comprobar la insuficiencia de la protección que dispensaban frente a investigaciones tecnológicas los derechos fundamentales al libre desarrollo de la personalidad, al secreto de las comunicaciones y a la inviolabilidad del domicilio, reconoció la existencia de un nuevo derecho, que entendió como "el derecho fundamental a la garantía de confidencialidad e integridad de los grupos informáticos", cuyo objeto era "proteger la vida privada y personal de los sujetos de los derechos fundamentales contra el acceso por parte del Estado en el ámbito de las tecnologías de la información, en la medida en que el Estado posea acceso al sistema de tecnologías de la información en su conjunto y no sólo a los

[174] MARTÍN RÍOS, P., "El alcance del derecho al propio entorno virtual en la valoración de la evidencia digital", cit., p. 1260.
[175] *Ibid.*
[176] FUENTES SORIANO, O., "La prueba prohibida aportada por particulares", cit., p. 725.

acontecimientos de comunicación individuales o a los datos almacenados"[177]. Como antecedente de dicha sentencia, debe mencionarse la sentencia de 15 de diciembre de 1983, que aludía por primera vez al derecho a la autodeterminación informativa.

El contenido de este derecho fundamental está compuesto de las protecciones que los diferentes derechos fundamentales del artículo 18 CE dispensarían a los datos informáticos, cuyo alcance ha sido comprobado que es insuficiente para proteger la información en formato electrónico que genera un usuario al utilizar las TICs, sea consciente o inconscientemente, hasta el punto de generar un rastro susceptible de seguimiento. A ello se han referido las SSTS 342/2013, de 17 de abril; 97/2015, de 24 de febrero; 204/2016, de 10 de marzo; 426/2016, de 19 de mayo. La Fiscalía General del Estado, por su parte, lo ha calificado como un "derecho omnicomprensivo que abarca la protección de la gran diversidad de datos que pueden guardarse en un dispositivo o sistema informático, como puede ser un ordenador"[178]. Se trata, en definitiva, de un "derecho mosaico", siguiendo la teoría elaborada al respecto.[179]

Por su parte, nuestro Tribunal Constitucional, en su STC 173/2011, de 7 de diciembre, ya reconoció la necesidad de establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática, así como de las nuevas tecnologías de la información. En su sentencia, concluía que así como los datos personales relativos a una persona individualmente considerados están dentro del ámbito de la intimidad constitucionalmente protegido, de igual modo sucede con el cúmulo de la información que se almacena por su titular en un ordenador personal con ocasión de su uso ordinario, y que hacen posible llegar a descubrir aspectos de la esfera más íntima de su titular.

El TC reconoció especialmente que, cuando una persona navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo

---

[177] CABEZUDO RODRÍGUEZ, N., "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal", cit., p. 42.
[178] "Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre registro de dispositivos y equipos informáticos.", fecha de consulta 25 abril 2020, en https://www.boe.es/diario_boe/txt.php?id=BOE–A–2019–4244.
[179] GIMENO SENDRA, J. V., "Libertad de expresion, honor e intimidad personal", *Economist & Jurist*, vol. 17, 136, 2010, Global Economist & Jurist.

más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Todos estos datos, aun cuando individual o aisladamente podrían parecer irrelevantes o livianos, configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A ello se añadía la circunstancia, claro está, de que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones sino también el derecho a la intimidad personal, en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado.

De igual modo, la STC 115/2013 recordaba la necesidad de tener en cuenta que la versatilidad tecnológica que han alcanzado los teléfonos móviles, convirtiéndose en herramientas indispensables en la vida cotidiana con múltiples funciones, tanto de recopilación y almacenamiento de datos como de comunicación con terceros (llamadas de voz, grabación de voz, mensajes de texto, acceso a internet y comunicación con terceros a través de internet, archivos con fotos, videos, etc.), susceptibles, según los diferentes supuestos a considerar en cada caso, de afectar no sólo al derecho al secreto de las comunicaciones, sino también a los derechos al honor, a la intimidad personal y a la propia imagen e incluso al derecho a la protección de datos personales. Todo ello implicaba la necesidad de que el parámetro de control a proyectar sobre la conducta de acceso a dicho instrumento debiera ser especialmente riguroso, tanto desde la perspectiva de la existencia de norma legal habilitante, incluyendo la necesaria calidad de la habilitación legislativa, como desde la perspectiva de exigir un respeto escrupuloso al principio de proporcionalidad.

En esencia, una de las principales utilidades del referido derecho fundamental es que, a pesar de ausencia de criterios legales expresos, los órganos judiciales han establecido el principio de reserva jurisdiccional para su limitación. Es destacable que, mediante este mecanismo, consiguen salvar el hecho de que en el artículo 18 CE no se establece dicho monopolio jurisdiccional para los apartados distintos del 18.3, de manera que, en último término, permite afirmar que los derechos fundamentales de los artículos 18.1, 18.2 y 18.4 CE sí están protegidos por la necesidad de autorización judicial previa cuando la injerencia va a tener lugar respecto de datos informáticos generados por el titular de

esos derechos. La justificación de esta postura no puede ser otra que la información adicional sobre la personalidad individual que arroja el tratamiento automatizado y entrecruzado de dichos datos. En tal sentido, la STS 426/2019, concluía que, a la vista de las diferentes injerencias que el acceso policial a cualquier ordenador podría causar en los derechos fundamentales de su titular, resulta fundamental contar con el presupuesto habilitante de una autorización judicial, de manera que la garantía prevista en el ordenamiento jurídico se haga efectiva siempre y en todo caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal. En similares términos, la STS 786/2015, de 4 de diciembre, subraya la circunstancia de que el cúmulo de información que se almacena por el titular en un ordenador personal puede descubrir aspectos de la esfera más íntima de su personalidad.

En todo caso, habrá que entender que no existe necesidad de dicha autorización judicial previa en los supuestos expresamente previstos en los artículos 588 k y siguientes LECrim –que trataremos después–, faltando por concretar si ello se debe a que dichos supuestos no afectarían al derecho fundamental al propio entorno virtual o a que, aun afectándolo, la injerencia sería de mínima trascendencia. Adelantamos ya que, a nuestro juicio, muchas de las medidas que no precisan autorización tienen una potencialidad lesiva idéntica a la de otras medidas que sí exigen, por el contrario, la referida autorización.

Por otro lado, la jurisprudencia concluye este derecho fundamental al propio entorno virtual también es susceptible de ser ampliado o reducido por los actos propios de su titular, siendo posible también apreciar aquí la existencia de un consentimiento tácito que dé lugar a una expectativa de privacidad reducida, como de hecho refería la STS 287/2017, de 19 de abril[180]. Esta postura jurisprudencial, sin embargo, no encuentra refrendo unánime en la doctrina, que expresa sus reservas a este respecto, y ello por dos razones fundamentalmente: por entender que el derecho al propio entorno virtual no es susceptible de disminución o renuncia como tal y por entender que los extremos a los que se atiende para apreciar una eventual renuncia tácita no son los acertados.

[180] Sentencia en la que el Tribunal Supremo resolvía un supuesto de aportación de información proveniente de un dispositivo de uso compartido. En particular, la esposa del condenado había aportado datos extraídos del ordenador familiar, y el Tribunal Supremo mantuvo que el propio titular del derecho al entorno virtual puede ampliar o reducir el espacio de exclusión que el mismo implica. En palabras del propio tribunal: "Quien incorpora fotografías o documentos digitales a un dispositivo de almacenamiento masivo compartido por varios es consciente de que la frontera que define los límites entre lo íntimo y lo susceptible de conocimiento por terceros, se difumina de forma inevitable".

En cuanto al primer motivo, relativo a la improcedencia de apreciar la posibilidad de disminuir o renunciar, tácita o expresamente, a la protección dispensada por el derecho fundamental al propio entorno virtual, la doctrina, estableciendo un paralelismo con el derecho a la inviolabilidad del domicilio[181], respecto del que se ha llegado a mantener su completa vigencia –negando cualquier atisbo de "renuncia tácita"– incluso en supuestos en los que el titular no había corrido las cortinas[182], si el derecho al propio entorno virtual tiene tanta trascendencia[183], no puede resultar justificado que la inmisión en dispositivos de almacenamiento digital cuente con menores garantías que el acceso por parte del poder público a un domicilio físico[184]. Además, recuerdan que en este caso no puede resultar de aplicación esa doctrina jurisprudencial que, respecto de la intimidad "genéricamente considerada", admite la posibilidad de que la policía realice actividades que la limiten, siempre que sea de forma leve y desproporcionada. Esta imposibilidad se deriva de la circunstancia de que cualquier inmisión en un dispositivo de almacenamiento masivo –o en las carpetas almacenadas en la nube– no puede considerarse como una injerencia leve, a la vista de la especial capacidad reveladora que tienen dichos repositorios de datos, por contener elementos de la vida más íntima de la persona.

En cuanto al segundo motivo, relativo a los extremos de hecho a que atienden los tribunales para apreciar la existencia de esa eventual renuncia tácita, la doctrina parece entender que dichos criterios desatienden la realidad social del tiempo en el que debe ser aplicada. Así, por ejemplo, se considera negativamente el empleo de equipos compartidos[185] (ordenadores familiares, por ejemplo), considerando en estos supuestos que los usuarios están renunciando a buena parte de su privacidad. Como se ha destacado[186], el hecho de que una familia comparta un ordenador –o una red WiFi– no puede significar

---

[181] Paralelismo que tiene su origen en el ordenamiento jurídico italiano, pues la Ley italiana 547/93 reconoce desde el año 1993 el derecho a desarrollar cualquier actividad lícita en un "lugar informático", entendido como aquella parcela digital que supone la extensión de la misma personalidad en el medio virtual y respecto de la que queda excluido el acceso por parte de terceros.
[182] STS 329/2016, de 20 de abril.
[183] Como de hecho tiene, y así lo declararon la STC 173/2011, de 7 de noviembre, y STS 786/2015, de 4 de diciembre, que destacaron que el conjunto de datos e información almacenado por el titular en su ordenador personal puede revelar aspectos de su esfera personal más íntima.
[184] MARTÍN RÍOS, P., "El alcance del derecho al propio entorno virtual en la valoración de la evidencia digital", cit., p. 168.
[185] Debe diferenciarse esta concepción de los equipos de público acceso, como los ordenadores de bibliotecas y cibercafés, a los que no nos referimos. En el argumento nos referimos a equipos compartidos por un grupo reducido de personas que, además, se diferencia por razones de confianza, convivencia, etc., de la generalidad de los individuos.
[186] MARTÍN RÍOS, P., "El alcance del derecho al propio entorno virtual en la valoración de la evidencia digital", cit., p. 1269.

que estén renunciando a su privacidad informática, y ello no sólo porque sea esperable y exigible a los demás miembros del grupo no acceder a los archivos particulares de cada familiar, sino porque, en todo caso, dichos usuarios esperan conservar su privacidad respecto de terceros ajenos a dicho grupo.

Apreciamos en relación con este último aspecto el mismo fenómeno al que haremos referencia en relación con las direcciones IP y demás datos que se publican libremente en la red, como suele entender la jurisprudencia, fenómeno consistente en una suerte de atribución de responsabilidad al propio interesado cuando es posible que este no sea verdaderamente consciente de las implicaciones que sus actos puedan tener en materia de seguridad y privacidad informática[187]. Por ejemplo, en una red WiFi abierta permite que cualquier usuario conectado revise el tráfico del resto de usuarios, siempre que no esté encriptado. Esto incluye contraseñas, nombres de usuarios, identificación de medios de pago, etc.[188] ¿Puede entenderse el hecho de navegar por una red WiFi abierta como una cesión del espacio de intimidad por el usuario? ¿Acaso el usuario tiene forma ordinaria de conocer qué tipo de red está utilizando? ¿Debería conocerla? ¿Acaso debe exigirse la encriptación –tanto de los datos en tráfico como de los datos en reposo– como manifestación definitiva del deseo de los individuos de que sus datos sean vigilados? El nivel de conocimientos técnicos necesarios para adoptar dichas medidas obliga, a nuestro juicio, a responder negativamente a tales interrogantes, y de ahí que consideremos los criterios empleados para apreciar renuncias tácitas en materia de privacidad informática se encuentran desanclados de la realidad.

8. EL RECIENTE ANTEPROYECTO DE LECRIM DE 2020

El pasado 24 de noviembre de 2020 fue aprobado por el Consejo de Ministros el Anteproyecto de Ley de Enjuiciamiento Criminal, con el que se pretende responder a la cada vez más innegable "necesidad de aprobar una nueva Ley de Enjuiciamiento Criminal que permita la construcción de un sistema de justicia penal moderno y garantista"[189], actuación que ha venido postponiéndose de manera continuada y reiterada.

---

[187] ARRABAL PLATERO, P., "El derecho fundamental al propio entorno virtual y su incidencia en el proceso", en *Era Digital, Sociedad y Derecho*, Tirant lo Blanch, Valencia, 2020, p. 436.
[188] "Consejos de un cazador de hackers para que tu smartphone esté protegido", fecha de consulta 2 mayo 2020, en https://www.youtube.com/watch?v=eVJCOsvFXg0.
[189] Consulta pública sobre el Anteproyecto, disponible en Consulta_publica_previa_APL_Enjuiciamiento_Criminal_REV.pdf (mjusticia.gob.es).

La propuesta nace con vocación de responder al mandato constitucional de proporcionar a los ciudadanos un sistema normativo que asegure la protección penal de sus bienes y derechos y que sujete, al tiempo, la capacidad de injerencia del Estado a límites racionales y efectivos.

Debe recordarse que, pese a las setenta y nueve modificaciones de la LECrim, más de cincuenta de ellas posteriores a la entrada en vigor de la Constitución en 1978, ha sido ampliamente desbordada por la realidad social, jurídica y procesal. Con 138 años de historia, la norma, que permitió superar el modelo inquisitivo de enjuiciamiento, recoge disposiciones redactadas durante tres siglos distintos, circunstancia esta que obliga a su reinterpretación constante por parte de la nuestros juzgados y tribunales.

Precisamente, hace ya más de veinte años que en el "Pacto de Estado para la Reforma de la Justicia" se estableció como objetivo básico la elaboración de una nueva Ley de Enjuiciamiento Criminal, expresándose claramente que se trataba de una actuación imprescindible para culminar el proceso de modernización de nuestras leyes procesales. Como consecuencia, tanto el gobierno socialista en 2011, como posteriormente el popular en 2013, elaboraron propuestas normativas encaminadas a sustituir totalmente el texto de 1882. Decenas de reformas parciales han convertido la Ley de Enjuiciamiento Criminal en un cuerpo normativo irreconocible que se ha visto, *de facto*, sustituido por una maraña de normas fragmentarias, encajadas unas con otras por razones coyunturales.

Aunque algunas de dichas reformas supusieron importantes avances en el proceso penal, en conjunto, dicha sucesión de modificaciones no ha resuelto los problemas estructurales que el paso del tiempo ha producido en el modelo de enjuiciamiento penal decimonónico aún vigente en España. El aplazamiento de tan necesaria tarea reformadora ha derivado en la progresiva acumulación de deficiencias estructurales en el sistema judicial penal que son producto de la inadecuación del modelo procesal al tiempo presente.

De esa manera, y entendiendo el legislador que nuestra justicia penal demanda, en el momento presente, un proceso ágil y exento de dilaciones indebidas, pero que al mismo tiempo permita dar una respuesta efectiva a modalidades delictivas cada vez más sofisticadas y complejas, surge este nuevo Anteproyecto[190]. Además, se aprovecha también para

[190] Expuestos por MORENO CATENA, V. M., "El mito de la instrucción dirigida por el juez", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, pp. 1339–1364*, Ediciones Jurídicas Castillo de Luna, 2020.

armonizar el nuevo paradigma procesal con la pertenencia de España al espacio normativo de libertad y justicia de la Unión Europea, en el que la investigación penal es una competencia que se ha extraído del ámbito del Poder Judicial y se ha atribuido al Ministerio Fiscal, modelo asumido por el Reglamento (UE) 2017/1939 del Consejo, de 12 de octubre de 2017, por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea en las materias propias de su competencia.

Entre los objetivos de la norma, pueden mencionarse los siguientes:

En primer lugar, dar respuesta a la demanda histórica de superar el modelo procesal penal decimonónico e implantar en España un moderno y avanzado proceso penal.

En segundo lugar, armonizar nuestro modelo procesal con el paradigma contemporáneo que hoy rige, con muy escasas excepciones, entre los países de nuestro entorno. Esta opción también implica la superación de las últimas notas inquisitivas del proceso penal español, que ya eran contempladas como meramente transitorias por el propio legislador decimonónico.

En tercer lugar, actualizar nuestro ordenamiento jurídico penal. Ahora se da regulación a las más avanzadas técnicas de investigación contra el crimen que aún no tenían acomodo en nuestro ordenamiento y, en algunos casos, todavía no se encuentran reguladas por ningún otro país del mundo.

El texto del anteproyecto, de nueva creación, se encuentra estructurado en nueve libros precedidos de un título preliminar, compuestos por un total de 789 artículos, a los que siguen una disposición adicional, una disposición derogatoria, seis disposiciones transitorias y tres disposiciones finales, previéndose una *vacatio legis* de 6 años.

No obstante, el anteproyecto también constituye una unión de los aspectos relevantes de sus predecesores.

El Anteproyecto dibuja profundas modificaciones de nuestro sistema judicial penal. Ahora bien, precisamente por su carácter profundo y rompedor con la realidad actual han surgido dudas sobre su viabilidad, en relación con la crónica situación de insuficiencia de recursos y sobrecarga de trabajo que padece la administración de justicia[191].

[191] RODRÍGUEZ PADRÓN, C., "El anteproyecto de Ley de Enjuiciamiento Criminal: implicaciones orgánicas", *Diario La Ley*, 9826, 2021, Wolters Kluwer, p. 2.

A continuación, queremos hacer referencia a las novedades más importantes que prevé el citado texto, novedades que plantean una transformación radical de nuestro procesal penal y que provocan, además, que sea necesario modificar otras normas cuyo contenido podría chocar frontalmente con el contenido del anteproyecto, como la Ley Orgánica del Poder Judicial, el Estatuto Orgánico del Ministerio Fiscal y la Ley de Planta y Demarcación Judicial, entre otras.

A. MINISTERIO FISCAL COMO INSTRUCTOR DE LAS CAUSAS

El Anteproyecto añade a las funciones ordinarias del Ministerio Fiscal la de dirigir la investigación oficial de un proceso penal. Según refiere el propio legislador en la exposición de motivos, era una perspectiva ya explorada por el legislador de 1882. En la actualidad, la atribución al Ministerio Fiscal de esta función directiva persigue una clara dimensión garantista en relación con la necesidad de preservar la imparcialidad objetiva del juez y de restar valor a los meros actos de investigación.

En el plano procesal, se parte, en principio, de la propuesta realizada en el Anteproyecto de 2011 para: i) suprimir la exigencia de que el Ministerio Fiscal continúe con la acción civil de resarcimiento de daños, cuando la víctima pueda reclamarla por sí misma y, por tanto, se haya personado como parte; ii) utilizar las reglas competenciales, de fueros personales y territoriales que determinaban al juez competente para la instrucción, ahora para determinar la fiscalía que se encargue de la misma; iii) para constituir equipos de fiscales, si bien con diferente finalidad, pues se pasa de pretender que se constituyeran para instruir asuntos complejos a definirlos como estructuras colegiadas permanentes, capaces de actuar con autonomía plena y máxima eficiencia en relación con toda clase de delitos; y iv) acentuar la dependencia que ya caracterizaba la actuación de la Policía Judicial respecto de lo ordenado por el Ministerio Fiscal.

En ese sentido, se opta por favorecer una organización interna basada en el funcionamiento de equipos autónomos de fiscales, dotados, si es preciso, de unidades policiales adscritas y de peritos y expertos adecuados a las exigencias derivadas de su específico ámbito de competencia. Se configuran, por tanto, auténticas oficinas de investigación. La idea no consiste, por tanto, únicamente en facilitar la creación de unidades específicas, sino la de establecer dentro del Ministerio Fiscal estructuras permanentes que actúen de manera autónoma y eficiente en ejercicio de la función de investigación penal.

Asimismo, se aplican las mismas reglas de competencia del Juez de Garantías para determinar qué oficina del Ministerio Fiscal es la competente para dirigir la instrucción del procedimiento. Son, de este modo, los distintos fueros personales y territoriales fijados para el juez los que han de designar, por regla general, la fiscalía competente.

Tras determinar la competencia dentro de la estructura del Ministerio Fiscal, el Anteproyecto potencia una organización interna basada en el funcionamiento de equipos autónomos de fiscales. Estos equipos podrán, incluso, contar con unidades policiales adscritas, peritos y otros expertos que sean necesarios, de manera que la oficina del fiscal cuente con todos los medios necesarios para atender las exigencias que plantee una determinada fase de instrucción.

Algo que es necesario destacar es que, como indica el propio legislador, este nuevo Anteproyecto persigue un objetivo más ambicioso que los anteriores, que se concreta en la intención de establecer dentro del Ministerio Fiscal estructuras colegiadas permanentes, capaces de actuar con autonomía plena y máxima eficiencia en relación con toda clase de delitos. Se prevé que en estas estructuras existan fiscales responsables de cada administración concreta, que han de contar con el oportuno apoyo y auxilio procesal y administrativo, así como un fiscal coordinador que realice la función de gestionar los recursos comunes, mantener los estándares de calidad del trabajo y dar coherencia y unidad al conjunto de las investigaciones emprendidas, entendemos que con sujeción a las instrucciones y circulares que se emitan desde la Fiscalía General del Estado.

En primer lugar, la fase de instrucción será iniciada con el comienzo de la investigación. Según lo establecido en los artículos 550 y ss. del anteproyecto (Título IV, Cap. I), el Ministerio Fiscal acordará mediante Decreto el inicio de las investigaciones, ya sea de oficio o según atestado o denuncia, exceptuando los supuestos en los que sea preceptiva querella privada, donde se establecerá “a) la identidad de la persona investigada, de resultar conocida, b) la de las personas ofendidas y perjudicadas, c) los hechos objeto de investigación y d) la calificación jurídica que provisionalmente pueda atribuirse a dichos hechos” (artículo 550.2). No obstante, el Fiscal también podrá decretar el archivo de la denuncia (que podrá recurrir la parte) ante el Juez de Garantías.

Por otro lado, según el art. 553 del mismo texto, el Fiscal podrá optar por otras alternativas al inicio de la fase de investigación. Destaca la previsión de un procedimiento de justicia restaurativa.

Una vez practicadas las diligencias suficientes, el Fiscal convocará a la persona investigada a una primera comparecencia, donde se le informará de este hecho, así como de los derechos que le asisten. Su acta se remitirá al Juez de Garantías. En toda esta labor hay que tener presente que el Ministerio Fiscal deberá cumplir con los plazos, lo cual es remarcado en el art. 560 LECrim.

Otra de las funciones destacables del Fiscal –que constituye, asimismo, una novedad– es la posibilidad que se le otorga, como director de la instrucción, de iniciar el procedimiento de investigación en los casos de detención el investigado, dando instrucciones a la policía; así como de acordar la libertad del investigado cuando haya sido detenido por la policía.

B. RÉGIMEN DE LA POLICÍA JUDICIAL

En el anteproyecto de LECrim de 2020, el legislador español es coherente con la decisión de otorgar al Ministerio Fiscal la dirección de la fase de investigación del proceso penal y, en tal sentido, establece la dependencia funcional de la Policía Judicial respecto del mismo.

Hay que destacar que el propio texto normativo reconoce la imposibilidad de realizar una división absoluta de las actividades policiales de seguridad pública y de investigación criminal, pues las fuerzas policiales han de dar una respuesta coordinada a la delincuencia, como perturbación de la seguridad ciudadana, tanto desde el punto de vista preventivo como represivo. En consecuencia, la noción de policía judicial contenida en el Anteproyecto es meramente funcional, y comprende todos aquellos cuerpos administrativos con carácter de agentes de la autoridad que realicen funciones de policía criminal bajo la dependencia del Ministerio Fiscal. Se abre así la posibilidad a que agentes de autoridad que no pertenezcan a las Fuerzas y Cuerpos de Seguridad también realicen funciones de policía judicial, siempre que exista disposición con rango de ley al respecto (Servicio de Vigilancia Aduanera, Oficina de Recuperación y Gestión de Activos, etc.).

Partiendo de dicha concepción funcional, generalista, y dependiente de las órdenes del Ministerio Fiscal, se reconoce expresamente la existencia de dos fases en las actuaciones investigadoras de la policía judicial. Una primera, compuestas por unas primeras diligencias que persiguen dar respuesta inmediata a la comisión del delito, y una segunda, compuesta por las diligencias que se realizan con posterioridad. Aunque tal paralelismo podría dar lugar a pensar que esta segunda fase estaría bajo la dirección funcional

directa del Ministerio Fiscal, lo cierto es que el legislador asume la idea de que la investigación policial ha de tener un espacio específico, un marco propio de desarrollo inicial, que debe deslindarse de todas aquellas actividades que requieren de una orden del fiscal o de una autorización judicial, por más que se mantenga dicha dependencia funcional, que se manifestará en forma de directrices o instrucciones generales.

Se prevé, por tanto, una fase preliminar en la que la policía judicial realizará actuaciones, posterior a las diligencias de respuesta rápida al delito, pero anteriores todavía a la incoación de un procedimiento penal. Se hace, por tanto, fundamental determinar cuáles son aquellas diligencias que la policía judicial podrá llevar a cabo de manera autónoma.

En todo caso, la investigación policial cesa con la identificación del sujeto al que se considera responsable, circunstancia que ha de llevar a la incoación de un procedimiento directamente a cargo del Ministerio Fiscal, bajo el control de un Juez de Garantías. En cualquier caso, el Ministerio Fiscal tendrá capacidad de decidir en todo momento la finalización de la investigación policial preliminar procediendo a asumir la inmediata dirección de las actuaciones.

C. NUEVA REGULACIÓN DE LOS ACTOS DE INVESTIGACIÓN

En su Libro III, el Anteproyecto se dedica a los actos de investigación, y lo hace con ánimo renovador. Como reconoce el legislador en la propia exposición de motivos, la mayor parte de las diligencias de investigación sigue anclada en una regulación legal obsoleta y deficitaria, con las salvedades de aquellos concretos actos de injerencia en la esfera de la persona investigada que, por carecer de cobertura legal suficiente, fueron regulados de manera específica con la Ley Orgánica 13/2015 (reguladora, entre otras cosas, de las diligencias de investigación tecnológica).

La finalidad de esta nueva regulación no es otra que dotar a nuestro proceso penal de un régimen normativo más preciso y útil, circunstancias estas que se verifican en la exigencia de un elevado estándar de garantías objetivas para la realización de los diferentes actos de investigación.

En claro cumplimiento de dicha finalidad tuitiva, el Anteproyecto prescinde del criterio de la autoridad habilitada para realizar el acto de investigación como criterio

organizativo y, en su lugar, clasifica los actos de investigación en función de la afectación que sufren los derechos de la persona sometida a cada uno de ellos.

Se parte, así, de los actos que afectan a la persona misma investigada –como las diversas formas de identificación y las inspecciones e intervenciones corporales–, continuando por las que suponen una intromisión en los derechos de la personalidad (fundamentalmente, en su intimidad e imagen), y las que injieren en el ámbito de desarrollo de su vida privada (con la consiguiente protección del domicilio). Finalmente, se regulan otros medios de investigación más complejos, como las investigaciones encubiertas y la obtención de datos protegidos.

D. NUEVA REGULACIÓN DE LAS OBSERVACIONES Y VIGILANCIAS POLICIALES

Si el Anteproyecto prosperase, por primera vez existiría en nuestro ordenamiento procesal una referencia expresa a las observaciones y vigilancias que pueden desarrollarse en la vía pública y en otros espacios abiertos respecto de personas, lugares y objetos relacionados con el delito. Esto es, por primera vez se incluye en la norma procesal una previsión relativa a la actividad de patrullaje de la policía (artículos 394 y siguientes ALECRIM).

El texto opta por distinguir las vigilancias ordinarias, que la policía puede realizar por su propia autoridad, de las de carácter sistemático.

Se consideran sistemáticas las que duran más de treinta y seis horas ininterrumpidas o más de cinco días, consecutivos o no, dentro del plazo de un mes. Esta modalidad, y la que se materializa a través de medios técnicos de localización y seguimiento o incluye la obtención de imágenes de personas, solo pueden llevarse a cabo respecto de la persona investigada (salvo que, excepcionalmente, se refieran a un tercero que va a contactar con ella). Requieren, además, la previa autorización judicial, salvo en los casos de urgencia, en los que pueden ser acordadas por el fiscal, con trámite de ratificación judicial en las veinticuatro horas siguientes. Todos estos seguimientos tendrán una duración máxima de tres meses a contar desde la fecha de la autorización, pudiendo acordarse prórrogas sucesivas hasta un máximo de dieciocho meses.

También se somete a autorización judicial la captación de imágenes en domicilios o en lugares cerrados destinados a la realización de actos de carácter íntimo, aunque puedan ser divisados desde el exterior.

Se regula, finalmente, con igual sujeción a garantía judicial, la posibilidad de recabar de las compañías u operadores telefónicos la entrega de toda la información que posean sobre la situación geográfica o punto de terminación de red del origen y destino de las llamadas telefónicas realizadas o recibidas por la persona investigada.

E. ACTUACIONES PRELIMINARES DE LA POLICÍA

Como hemos comentado, el texto del Anteproyecto también prevé que la policía pueda realizar por sí misma actuaciones preliminares, que se caracterizan porque solo pueden abarcar actos de injerencia nula o mínima, que deben cesar con la identificación del sujeto que se considera responsable.

En cuanto a la primera nota característica, las actividades investigadoras que realmente pueden suponer una intromisión relevante en la esfera de derechos de un ciudadano exigen en todo caso la intervención del fiscal. Y en los supuestos previstos en el artículo 18 de la Constitución, será imprescindible la autorización del propio juez, que siempre se recabará por conducto del fiscal, como único interlocutor directo de la autoridad judicial en la estructura del Estado investigador.

En cuanto al segundo rasgo antes aludido, las indagaciones preliminares de la policía solo estarán justificadas cuando no exista una persona claramente identificada como posible responsable de la infracción criminal. Hecha esta averiguación, la amenaza potencial que la investigación supone para la libertad y los derechos de la persona investigada obligará a formalizar las actuaciones en un procedimiento bajo la dirección inmediata del Ministerio Fiscal y con la vigilancia de un Juez de Garantías.

De ahí que, por regla general[192], las investigaciones sin autor conocido hayan de quedar archivadas en sede policial –sin perjuicio de su necesaria comunicación por relación al Ministerio Fiscal, que podrá incoar el procedimiento de investigación en todos aquellos supuestos en los que lo considere preciso–. Una vez que se produzca la

[192] El artículo 544 del Anteproyecto establece, en su apartado primero" el Fiscal General del Estado y los Fiscales Jefes de los distintos órganos del Ministerio Fiscal, en el ámbito de sus respectivas competencias, podrán disponer que la investigación de determinadas clases de delitos sea siempre comunicada mediante atestado, aunque no exista autor conocido."

identificación del posible autor se pondrá la investigación a disposición del fiscal por medio del correspondiente atestado.

En definitiva, las actuaciones policiales previas deberán terminar con la identificación del sujeto al que se atribuye la comisión del delito. Se entiende así que la determinación del sospechoso exige el inicio del verdadero procedimiento de investigación, que lleva consigo garantías formales de gran importancia en beneficio de la persona que se convierte en sujeto pasivo de esa actividad estatal.

En nuestra opinión, se trata de una posibilidad que, aunque no es nueva –en la actualidad, son múltiples los supuestos en los que la policía, antes de trasladar el atestado al Juzgado, realiza las diligencias que entiende necesarias para determinar el posible autor de los hechos– puede plantear graves problemáticas, pues, por un lado, no existe un control directo de la actuación policial para determinar el momento en el que la persona sospechoso se encuentra determinada y, por otro lado, y como ya hemos comentado, asistimos a una progresiva relajación de la figura de la prueba ilícita, con la posibilidad de que pruebas de cargo que hayan sido obtenidas de manera, cuanto menos, discutible, accedan al proceso.

F. TRIBUNALES DE INSTANCIA

El texto del anteproyecto prevé la creación de órganos colegiados, denominados tribunales de instancia, con capacidad de ejercer sus competencias en forma unipersonal o colegiada en función de las necesidades del caso concreto. De esta manera, se supera la estructura dual basada en Juzgados como órganos unipersonales de instancia, y se dividen las funciones judiciales de garantía, juicio acusación y enjuiciamiento en diferentes componentes de un mismo órgano.

Al concebir esta nueva organización de la justicia, el prelegislador recupera el objetivo frustrado de la Ley provisional de 22 de diciembre de 1872 y de la Ley de Bases de 7 de febrero de 1881, recupera el concepto de los tribunales de instancia, que suponen la colegiación de la organización judicial en todos los niveles del orden jurisdiccional penal, y que comporta la desaparición de los actuales Juzgados.

Los tribunales de instancia aglutinarían las funciones judiciales previstas en el anteproyecto –garantías, juicio de acusación y enjuiciamiento– que serán ejercitadas por diferentes secciones y magistrados del mismo tribunal. Se procede a unificar todo el

enjuiciamiento de las causas criminales en este nuevo órgano que, en función de la naturaleza del asunto concreto, puede actuar jurisdiccionalmente de forma unipersonal o colegiada. El legislador ha decidido combinar el criterio de gravedad de la pena –que determina actualmente la competencia de la Audiencia Provincial– con un listado de delitos que, por su especial complejidad o naturaleza, exigen una decisión colegiada.

Asimismo, los magistrados de los tribunales de instancia estarán exclusivamente dedicados al enjuiciamiento, unipersonal o colegiado, de los delitos mientras que las diversas Salas de Apelación de los Tribunales Superiores de Justicia estarán especializadas en la tramitación de los recursos de apelación frente a sentencias.

G. JUEZ DE GARANTÍAS

La atribución al Ministerio Fiscal de la dirección de la fase de instrucción comporta la necesidad de prever una figura que garantice el respeto a los derechos fundamentales.

El que se atribuye al juez en la fase de instrucción desde el Anteproyecto de 2011 (continuado en el de 2013 y, ahora, en el de 2020), es propio de un Juez de Garantías. Ello supone que el Ministerio Fiscal tendrá un cierto control por parte de dicho órgano, ya que será este el que velará porque las garantías y derechos constitucionales se garanticen en dicha fase.

Ya en el Anteproyecto de 2011 se establecía la serie de funciones que habría de tener dicho Juez de Garantías. Así pues, será el que apruebe o deniegue la práctica de ciertas diligencias que afecten a derechos del investigado, como la integridad física e intimidad, la inviolabilidad del domicilio o las comunicaciones del investigado. Controlará, asimismo, la adopción de medidas cautelares que afecten a dichos ámbitos de la vida del investigado.

En el Anteproyecto LECrim 2020 se regula todo ello en su artículo 19, bajo la rúbrica “imparcialidad objetiva”.

H. JUEZ DE LA AUDIENCIA PRELIMINAR

Hasta este momento, en los procedimientos abreviados, la fase de instrucción y la fase intermedia de un proceso penal la ha dirigido el juez instructor encargado.

A esta situación se pone fin con el nuevo Anteproyecto. Esto es así puesto que, como se entiende y se explica en el Anteproyecto, el órgano jurisdiccional que ya ha investigado se encuentra "contaminado", lo que no garantiza la imparcialidad que se pretende del mismo al diferenciar sus funciones de la del Ministerio Fiscal.

Con la finalidad de distinguir las competencias judiciales ejercitadas en la fase procesal de un procedimiento penal, y persiguiendo con ello asegurar un mayor grado de imparcialidad en el enjuiciamiento de la causa, el Anteproyecto prevé la figura del "Juez de la Audiencia Preliminar", siguiendo en ello la estela del Anteproyecto de Ley de Enjuiciamiento Criminal de 2011.

De esta manera, se crea un tercer sujeto: el Juez de la Audiencia Preliminar, el cual, realizará las funciones que viene desempeñando el juez de instrucción dentro de la fase de instrucción, es decir, será quien decida si se abre o no el juicio oral en la celebración de la audiencia previa, es decir, declarará motivadamente si son suficientes los indicios de criminalidad.

A este respecto, la exposición de motivos del anteproyecto de LECrim 2020 viene a precisar que "esta denominación no debe identificarse con un trámite procedimental de carácter necesariamente oral sino con una función de admisión y saneamiento similar a la que el procedimiento civil ordinario cumple la llamada "audiencia previa" al juicio. De ahí que se haya optado por la denominación aludida, acorde, por otra parte, con el nombre que recibe el trámite semejante que existe en la Ley del Jurado".

Lo que se consigue, además, con esto, es que todas las diligencias de investigación y todas las pruebas recogidas gracias a dichas diligencias lleguen de la forma más depurada posible ante el Juez de Audiencia Preliminar.

En otro orden de cosas, la idea de armonización de la normativa procesal penal con respecto a los países europeos cobra realidad en el establecimiento de un procedimiento de cooperación del Ministerio Fiscal con la Fiscalía Europea.

Este procedimiento, recogido en los arts. 818 a 835, pretende garantizar una mejor fluidez de la cooperación internacional con respecto a procesos penales internacionales, cuya competencia (ya sea su remisión, inicio o transferencia del mismo) será la de la Audiencia Nacional.

De esta manera, según el art. 818.4, las comunicaciones entre el Fiscal nacional y la Fiscalía Europea se regirán por lo establecido en el Estatuto Orgánico del Ministerio Fiscal y la normativa de la Fiscalía Europea.

Según la exposición de motivos del Anteproyecto que nos ocupa, la finalidad de esta audiencia preliminar es la de permitir que se realice un control de admisión y saneamiento similar al que cumple la audiencia previa en los procesos civiles. Así, el órgano judicial determinará si la acción penal interpuesta está suficientemente fundada, decidiendo sobre la apertura de la fase de juicio oral o el sobreseimiento, examinando también, por tanto, la licitud de la prueba que las partes pretendan llevar al juicio oral.

Este Juez de la Audiencia Preliminar no intervendrá posteriormente en el enjuiciamiento de la causa, que tendrá lugar ante los magistrados que resulten competentes. De esta manera, como se puede comprobar, se pretende garantizar que la decisión sobre la continuación de un proceso penal la tome un tercero completamente imparcial que no haya intervenido en la fase investigadora y, por tanto, pueda encontrarse afectado por cierto ánimo persecutorio, y que tampoco vaya a intervenir en la fase enjuiciadora.

I. MODIFICACIÓN DE OTRAS LEYES

Al modificarse las funciones del Ministerio Fiscal dentro del proceso penal como hemos visto, es lógico que su Estatuto Orgánico tenga que ser adaptado a la nueva situación.

Así lo dispone el Anteproyecto en su Disposición Adicional segunda, en la que se establece que el Gobierno deberá modificar dicho Estatuto, elevando al Parlamento en el plazo de un año, un proyecto de reforma de la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal.

Además, el desdoblamiento de funciones entre el Juez de Garantías y el establecimiento de un nuevo órgano, el Juez de Audiencia Preliminar, hacen necesario que la Disposición Adicional Primera del Anteproyecto 2020 disponga que sea modificada la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y de la Ley 38/1988, de 28 de diciembre, de Demarcación y Planta Judicial.

En esta Disposición, se establece que la implantación de la nueva LECrim se realizará de manera coordinada con las Comunidades Autónomas y el Consejo General del Poder Judicial, señalando que, hasta que los órganos no se encuentren totalmente

adaptados a la nueva regulación, se mantendrá vigente la aplicación de las reglas y normas competenciales establecidas en la Ley Orgánica del Poder Judicial.

El proceso de adaptación deberá realizarse en un periodo de tres años y se llevará a cabo en dos distintas fases, en la que la primera se centrará en la integración dentro del Tribunal de Instancia de los órganos jurisdiccionales unipersonales; en la segunda, se tendrá en cuenta la modificación competencial de los órganos colegiados.

En las siguientes Disposiciones también se continúa estableciendo la necesidad de reformar otras disposiciones de nuestro ordenamiento jurídico, como la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, otras leyes especiales penales y, en general, cuantas leyes sean contrarias a dicho Anteproyecto. Para todo ello se prevé el plazo de un año.

CAPÍTULO III
ACTIVIDAD PREPROCESAL DE LA POLICÍA JUDICIAL: EL CIBERPATRULLAJE COMO ACTIVIDAD PREVENTIVA

1. DISTINCIÓN CONCEPTUAL

En este apartado, es nuestra intención analizar esa actividad de prevención de la criminalidad que, mediante el rastreo de la red y, en general, el uso de la informática, puede acometer la Policía Judicial sin necesidad de autorización judicial, sin que exista un destinatario específico de las averiguaciones y, en consecuencia, sin que exista un procedimiento penal incoado. Nos referimos aquí, por tanto, a la actividad de "mantenerse a la escucha" por parte de la policía, en una conducta paralela a la de que aquellos agentes que patrullan físicamente un terreno o territorio, como las calles de una ciudad, lugares con mayor densidad de personas, etc.

Como hemos referido, en nuestro ordenamiento jurídico se distinguen, desde una perspectiva general, dos funciones policiales realizadas por los Cuerpos y Fuerzas de Seguridad del Estado: la prevención de la delincuencia, mediante el mantenimiento de la seguridad ciudadana y el orden público, y la investigación de delitos, que es la actividad dirigida a la búsqueda de evidencias que permitan esclarecer los hechos delictivos ya cometidos y que están siendo objeto de investigación.[193] Pues bien, dentro de la primera categoría se encuentra el denominado *ciberpatrullaje*, entendido como el conjunto de actuaciones de vigilancia, prevención y evitación de ilícitos penales llevadas a cabo por la policía en el ámbito del *ciberespacio*.

Dos grandes factores intervienen en la aparición del *ciberpatrullaje* como uno de los principales interrogantes de nuestro tiempo. Por un lado, la denominada *war on terror*[194], término que se emplea para designar a la política desarrollada desde los atentados del 11S por Estados Unidos y el bloque occidental y que, en plena evolución de la

[193] VELASCO NÚÑEZ, E., "La investigación de delitos cometidos a través de Internet y otras nuevas tecnologías: cuestiones procesales", 2010, Universidade da Coruña, p. 161.
[194] MARTÍNEZ SANTOS, A., "Terrorismo, proceso penal y derechos fundamentales", *Cuestiones constitucionales*, 29, 2013, Instituto de Investigaciones Jurídicas, UNAM.

"sociedad del riesgo"[195] y con la inestimable ayuda de la corriente que defiende el "Derecho penal del enemigo" ha provocado que, paulatinamente, se vayan relajando las garantías del Estado de derecho por entender que, en determinados supuestos, el fin justifica los medios. Por otro lado, el hecho de que las herramientas que se utilizan para las actividades de *ciberpatrullaje* –por naturaleza, menos intrusivas que las diligencias de investigación, que precisan de autorización judicial como regla general– son, en realidad, las mismas herramientas que se utilizan para llevar a cabo diligencias de investigación, conservando la potencialidad lesiva del derecho fundamental afectado y presentando como única diferencia el fin al que se las destina en ese momento concreto.

Estas circunstancias nos hacen concluir que es fundamental que se establezcan deberes de transparencia respecto de las herramientas utilizadas y del modo en que lo son. Ejemplo de ello es la iniciativa desarrollada por la *Public Oversight of Surveillance Technology Act*, en Nueva York (POST), que pretende obligar al departamento de policía a publicar información básica sobre las herramientas de vigilancia que utiliza y las medidas de seguridad adoptadas para proteger la libertad y derechos civiles de los ciudadanos[196].

2. CUERPOS ESPECIALIZADOS

En la lucha contra la ciberdelincuencia, la necesidad de conseguir la máxima eficacia y precisión técnica ha obligado tanto a crear grupos especializados dentro de las Fuerzas y Cuerpos de Seguridad nacionales, como a la constitución de organismos internacionales expertos en la materia.

Especialmente, estos grupos se encuentran especializados en transmisión de procedimientos y denuncias, intercambio espontáneo de información, notificación y traslado de documentos procesales y resoluciones judiciales, aseguramiento de pruebas, ejecución del auxilio judicial de las comisiones rogatorias para las diligencias de investigación y probatorias, medidas restrictivas de derechos fundamentales –intervenciones corporales, registro de lugar cerrado, intervención de telecomunicaciones, entrega y traslado de sujetos procesales–. la extradición, entrega temporal, e incluso la ejecución de sentencias firmes y el traslado de personas condenadas, a la vez que manteniendo la necesaria

[195] BECK, U., *La sociedad del riesgo: Hacia una nueva modernidad*, Grupo Planeta Spain, 2013.
[196] "The Public Oversight of Surveillance Technology (POST) Act: A Resource Page", *Brennan Center for Justice*, disponible en https://www.brennancenter.org/our–work/research–reports/public–oversight–surveillance–technology–post–act–resource–page, fecha de consulta 4 mayo 2020.

independencia del poder judicial para analizar el modo y validez de las pruebas obtenidas en el extranjero.[197]

A nivel nacional, los cuerpos expertos de que disponemos son, por un lado, la Unidad de Investigación Tecnológica de la Policía Nacional[198] y, por otro lado, el Grupo de Delitos Telemáticos de la Guardia Civil[199].

En cuanto al primero de ellos, la UIT fue creada en 2013 y sustituyó a la Brigada de Investigación Tecnológica, previamente denominada como Unidad de Investigación de la Delincuencia en Tecnologías de la Información. A su vez, esta última tuvo su origen en 1995, procedente del Grupo de Delitos Informáticos en el seno de la Brigada de Delincuencia Económica y Financiera de la Comisaría General de la Policía Judicial. Sus funciones principales son las de investigar los hechos que tengan que ver con la ciberdelincuencia, coordinar las operaciones nacionales, formar al personal del Cuerpo Nacional de Policía y representarlo en el ámbito internacional, incluyendo la ejecución y coordinación de otras investigaciones. A su vez, la UIT se encuentra subdividida entre la Brigada Central de Investigación Tecnológica, que se encarga de investigar las actividades delictivas relacionadas con la protección de los menores, intimidad, propiedad intelectual e industrial y fraudes en telecomunicaciones, y la Brigada Central de Seguridad Informática, que asume las funciones de investigación de actividades delictivas que afecten a la seguridad lógica, así como fraudes.[200]

En cuanto al segundo de ellos, la GTD está encuadrada dentro de la Unidad Central Operativa de la Guardia Civil, o UCO, que como unidad específica tiene como misión investigar y perseguir los asuntos relacionados con la delincuencia organizada, económica, internacional, y aquella otras cuyas especiales características asi lo aconsejen. El Grupo fue creado en 1996 con el nombre de Grupo de Delitos Informáticos, que cambió su denominación a la de Departamento de Delitos de Alta Tecnología en 1998, Departamento de Delitos Telemáticos en 2000, y finalmente en 2003 a su nombre actual. Se encarga de investigar hechos que tengan que ver con la ciberdelincuencia, apoyar los

---

[197] VELASCO NÚÑEZ, E., "Crimen organizado, internet y nuevas tecnologías", cit., p. 269.
[198] "Página oficial de la DGP–Comisaría General de Policía Judicial", fecha de consulta 1 mayo 2020, en https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html.
[199] "GDT – Grupo de Delitos Telemáticos", fecha de consulta 1 mayo 2020, en https://www.gdt.guardiacivil.es/webgdt/home_alerta.php.
[200] Disponible en https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html, fecha de consulta fecha de consulta 4 mayo 2020.

departamentos de la Unidad Central Operativa y fomentar un uso seguro de las nuevas tecnologías a través de funciones de formación y concienciación.

Ambos grupos gozan de representación provincial mediante los Equipos de Investigación Tecnológica, o EDITES.

Una de las reacciones de lo público frente a la cibercriminalidad ha consistido en la creación o aprovechamiento de órganos especializados ya existentes –como la Audiencia Nacional o los grupos policiales especializados– para asignarles, cuando menos, la investigación de estas modalidades de criminalidad, por los especiales requisitos que exigen en materia de medios materiales y de formación[201].

Hemos de hacer referencia también a los Fiscales de criminalidad informática[202], previstos mediante la Instrucción 2/2011, de la Fiscalía General del Estado, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de Criminalidad Informática de las Fiscalías.

Según esta Instrucción, al Fiscal de Sala Coordinador para la Criminalidad Informática le corresponden las siguientes funciones: 1) Practicar las diligencias a que se refiere el artículo cinco del Estatuto Orgánico del Ministerio Fiscal e intervenir directamente, o a través de instrucciones, en aquellos procesos penales de especial trascendencia apreciada por el Fiscal General del Estado, referentes a hechos delictivos relacionados con la Criminalidad Informática; 2) Supervisar y coordinar la actividad de las secciones de Criminalidad Informática y recabar informes de las mismas, dando conocimiento al Fiscal Jefe del órgano del Ministerio Fiscal en que se integran; 3) Coordinar los criterios de actuación de las distintas Fiscalías en materia de criminalidad informática, para lo cual podrá proponer al Fiscal General la emisión de las correspondientes Instrucciones y reunir cuando proceda a los Fiscales integrantes de las secciones especializadas; y 4) Elaborar anualmente y presentar al Fiscal General del Estado un informe sobre los procedimientos seguidos y actuaciones practicadas por el Ministerio Fiscal en materia de criminalidad informática que será incorporado a la Memoria anual presentada por el Fiscal General del Estado.

[201] VELASCO NÚÑEZ, E., "Crimen organizado, internet y nuevas tecnologías", cit., p. 263.
[202] QUEVEDO GONZÁLEZ, J., *Investigación y prueba del ciberdelito*, cit., p. 87.

Por otro lado, las secciones de criminalidad informática de las fiscalías articulan servicios territoriales de ámbito provincial integrados por uno o más fiscales y se encuentran dirigidas por un Fiscal Delegado Provincial, que opera bajo la dependencia del Fiscal Jefe respectivo. Según la referida Instrucción 2/2011, le corresponden las siguientes funciones:

– Velar por el cumplimiento de los criterios y pautas de actuación establecidos en materia de criminalidad informática por la Fiscalía General del Estado, facilitando a dicho fin el apoyo y colaboración necesarios a los restantes integrantes de la Fiscalía y a las secciones correspondientes a otras áreas de especialización asumiendo, en los casos en los que el Fiscal Jefe lo delegue, el visado de los escritos de acusación relativos a esta materia.

– Despachar e intervenir, previa determinación del Fiscal Jefe, en los procedimientos judiciales más importantes o de mayor complejidad de los comprendidos en el catálogo relacionado en el apartado II de esta Instrucción y en todo caso en los cometidos por una organización criminal, así como en las diligencias de investigación que se incoen por hechos de esta naturaleza.

– Procurar el adecuado control estadístico de los procedimientos judiciales y/o diligencias de investigación penal que se tramiten en el ámbito territorial de su competencia por los delitos anteriormente relacionados, proponiendo a tal fin al Fiscal Jefe Provincial y en su caso a los Fiscales Jefes de Área las medidas adecuadas para mantener actualizada dicha información y asumiendo las funciones que al respecto se le encomienden.

– Informar al Fiscal de Sala Coordinador de Criminalidad Informática, previo conocimiento del Fiscal Jefe respectivo, de las diligencias o procedimientos de especial trascendencia que se tramiten en el territorio provincial y de aquellos que por sus características hagan necesaria o conveniente la coordinación con otros órganos territoriales del Ministerio Fiscal.

– Participar activamente, prestando la colaboración y apoyo necesario, con conocimiento del Fiscal Jefe, en las actuaciones que, dirigidas por el Fiscal de Sala, se lleven a efecto para coordinar investigaciones por hechos relacionados con la criminalidad informática que afecten al territorio de más de una Fiscalía Provincial.

– Remitir al Fiscal de Sala Coordinador la información que específicamente demande sobre diligencias o procedimientos concretos y la que con carácter general se determine, respecto de la totalidad de los expedientes relativos a criminalidad informática, por decisión del Fiscal de Sala Coordinador o por acuerdo adoptado en las reuniones de Fiscales especialistas que periódicamente se celebren.

– Organizar bajo la superior dirección del Fiscal Jefe el funcionamiento de la propia sección y sus relaciones con otras secciones y/o áreas de actuación de la Fiscalía, trasladando al mismo las necesidades, propuestas o sugerencias que se consideren oportunas para la adecuada prestación del servicio y dando cuanta de las cuestiones esenciales en relación con ello al Fiscal de Sala Coordinador.

– Elaborar anualmente un informe sobre la actividad desarrollada, los datos estadísticos disponibles, los problemas jurídicos detectados y cuantas sugerencias se consideren oportunas sobre cuestiones organizativas y/o problemas técnico jurídicos detectados en el ámbito de actuación de la sección, dando traslado del mismo al Fiscal Jefe respectivo y al Fiscal de Sala Coordinador a los efectos de la elaboración de la correspondiente Memoria.

– Mantener las relaciones de colaboración oportunas con las unidades especializadas de las Fuerzas y Cuerpos de Seguridad del Estado ó, en su caso, de las Policías Autonómicas para garantizar la eficacia exigible en las investigaciones sobre hechos ilícitos relacionados con la criminalidad informática.

– Participar, a través de alguno de sus miembros, preferentemente el Delegado provincial, en las reuniones de especialistas que se celebren periódicamente para la unificación de criterios y en cuantas otras sean convocados por el Fiscal de Sala Coordinador para analizar cuestiones relacionadas con la actividad del área de especialización.

3. PREVISIÓN EN EL ORDENAMIENTO JURÍDICO

El régimen jurídico de la actividad de *ciberpatrullaje* puede extraerse de las siguientes disposiciones: 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.; Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones; Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico; Ley Orgánica 6/1985, de 1 de julio, del Poder

Judicial; Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal; Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad; Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal; e Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, celebrado en Budapest el 23 de noviembre de 2001, entre otras.

Las Fuerzas y Cuerpos de Seguridad del Estado en el desempeño de sus funciones como Policía Judicial, tienen entre sus atribuciones las de garantizar la seguridad ciudadana, averiguar la autoría y circunstancias de los delitos, y recoger los efectos, instrumentos y pruebas de ellos, poniéndolos a disposición de la autoridad judicial. Estas previsiones se establecen en los artículos 104 CE y 549.1 LOPJ.

Pues bien, si la función de averiguación de los delitos y puesta a disposición de sus efectos a la autoridad judicial sí goza de una regulación expresa y, en especial, respecto de las diligencias de investigación tecnológicas desde la entrada en vigor de la LO 13/2015, con el *ciberpatrullaje* no sucede lo mismo, no existiendo un cuerpo normativo específico y siendo necesario acudir, por analogía, a la regulación existente acerca del "patrullaje físico", que tampoco es muy abundante. Los preceptos que regulan esta actividad por parte de los Cuerpos y Fuerzas de Seguridad del Estado son los artículos 282 LECrim, 11.1 LOFFCCSS y 22.2 de la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (vigente conforme a la disposición transitoria de la Ley Orgánica 3/2018, de 5 de diciembre)[203].

La ausencia de normativa específica reguladora al respecto es destacable, porque, aunque es cierto que el monopolio jurisdiccional está previsto exclusivamente para cuando se afecta al derecho fundamental al secreto de las comunicaciones y para algunas manifestaciones del derecho a la intimidad, como la inviolabilidad del domicilio, también

[203] En tal sentido se pronunciaba la STC 115/2013: "En segundo término, los agentes policiales actuaron en el presente caso con el apoyo legal que les ofrecen el artículo 282 de la Ley de enjuiciamiento criminal, el artículo 11.1 de la Ley Orgánica 2/1986, de 13 de marzo, de fuerzas y cuerpos de seguridad, y el artículo 14 de la Ley Orgánica 1/1992, de 21 de febrero, sobre protección de la seguridad ciudadana, que conforman "una habilitación legal específica que faculta a la policía para recoger los efectos, instrumentos y pruebas del delito y ponerlos a disposición judicial y para practicar las diligencias necesarias para la averiguación del delito y el descubrimiento del delincuente" (SSTC 70/2002, FJ 10, y 173/2011, de 7 de noviembre, FJ 2). Entre estas diligencias se encuentra la de examinar o acceder al contenido de esos instrumentos o efectos, así como a los documentos o papeles que se le ocupen al detenido, realizando un primer análisis de los mismos, siempre que ello sea necesario de acuerdo con una estricta observancia de los requisitos dimanantes del principio de proporcionalidad (SSTC 70/2002, FJ 10, y 173/2011, FJ 2), extremo este sobre el que luego volveremos."

es cierto que toda injerencia en un derecho fundamental –con independencia de la exigencia de la previa autorización judicial o no– debe estar suficientemente prevista en el ordenamiento jurídico a fin de superar el triple requisito exigido por el artículo 8.2 CEDH[204].

Esta circunstancia, además, no es nueva, sino que ya ha sido puesta de manifiesto por la doctrina hace algún tiempo[205], incluso en relación con el patrullaje y las técnicas de investigación "tradicionales", señalándose el olvido casi crónico en que incurre el legislador a la hora de establecer una regulación específica sobre la actividad de investigación, vigilancia, seguimiento y averiguación de la policía y una suerte de asunción espontánea -a nuestro juicio, injustificada- por parte de los agentes policiales y judiciales de que, para mantener la eficacia de dichas actividades, es necesario que el detalle de las mismas permanezca en secreto. Este convencimiento, además, parece amparar no sólo los *modus operandi* en general, sino incluso las actividades concretas de investigación previa a la instrucción (patrullaje), en las que parece concluirse, insistimos que injustificadamente, que es necesario mantener cierto sigilo sobre la actuación policial.

4. INSTRUCCIONES DE SERVICIO

Las Fuerzas y Cuerpos de Seguridad cuentan con manuales de actuación que detallan los métodos y procedimientos que los funcionarios que los componen deben al realizar su actividad de *ciberpatrullaje* –así como en el resto de las diligencias de investigación tecnológica–. Estos manuales constituyen auténticas instrucciones de servicio y dictan las pautas de actuación que deben seguirse, por lo que contienen gran parte del *modus* operandi de la policía, y son una manifestación de la capacidad que tienen los órganos de la Administración de impartir órdenes a sus subordinados.

Así, por ejemplo, en el apartado 4.8 de la Orden INT/226/2020, de 15 de marzo, por la que se establecen criterios de actuación para las Fuerzas y Cuerpos de Seguridad

---

[204] Estos tres requisitos necesarios para que una injerencia en el derecho a la vida privada pueda considerarse legítima son los siguientes: i) que la injerencia esté prevista en la ley, que se identifica con el derecho nacional en una perspectiva material –puede admitirse dentro de dicho concepto los criterios jurisprudenciales asentados; ii) que la injerencia obedezca a uno de los fines legítimos previstos en el artículo 8.2 CEDH: seguridad nacional, seguridad pública, bienestar económico del país, defensa del orden y prevención del delito, protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás; y iii) que la injerencia sea necesaria en una sociedad democrática, elemento este en el que se ubica el principio de proporcionalidad en sentido estricto.

[205] NIEVA FENOLL, J., "La protección de derechos fundamentales en las diligencias policiales de investigación del proceso penal", *La ley penal: revista de derecho penal, procesal y penitenciario*, 50, 2008, Wolters Kluwer, p. 5.

en relación con el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID–19, se establecía: "Por parte de los Cuerpos policiales actuantes y los centros competentes de la Secretaría de Estado de Seguridad se impartirán directrices para prevenir y minimizar los efectos de la desinformación, extremándose la vigilancia y monitorización de las redes y páginas web en las que se difundan mensajes e informaciones falsas orientadas a incrementar el estrés social, e instando en su caso las medidas de intervención previstas en la legislación aplicable".

Sobre esta cuestión, huelga recordar que las instrucciones de servicio pueden ser objeto de impugnación en los casos en que pueda entenderse que innovan el ordenamiento jurídico, en su condición de instrumentos de *soft law*, como se señala en la STS de 18 de julio de 2012. El Tribunal Supremo, aun admitiendo que se trata de una cuestión polémica, subraya que ninguna duda ofrece la posibilidad de impugnar (tanto en vía administrativa como jurisdiccional) los concretos actos administrativos que puedan dictarse con base, por ejemplo, a una instrucción. En este sentido, alude a la STC 47/90, de 20 de marzo, que admitió, resolviendo un recurso de amparo, la impugnación directa de las instrucciones administrativas.

De esta cuestión es necesario destacar que las instrucciones administrativas no se ven afectadas por el principio de publicidad, al no constituir una innovación del ordenamiento jurídico, de manera que, al menos en nuestro país, no existe una iniciativa pública destinada a dar a conocer dichas instrucciones, también influido por una lógica de mantenimiento de su eficacia y seguridad.

En ese sentido, nos atrevemos a proponer la conveniencia de publicar los protocolos que inspiren la actividad de ciberpatrullaje de nuestras fuerzas policiales. Podemos hacer referencia, por ejemplo, al ejemplo iniciado con la resolución 144/2020, del Ministerio de Seguridad de Argentina, que establece algunas directrices si bien generales, que permite, al menos, delimitar los contornos de la actividad de ciberpatrullaje[206]:

[206] "Boletín Oficial República Argentina – Ministerio de Seguridad – Resolución 144/2020", fecha de consulta 6 enero 2021, en https://www.boletinoficial.gob.ar/detalleAviso/primera/230060.

- Que la prevención policial del delito en el espacio cibernético procurará el conocimiento de posibles conductas delictivas cuyo acaecimiento sea previsible en función de la emergencia pública en materia sanitaria establecida

- Que se deberá atender al desarrollo de la criminalidad vinculada a la comercialización, distribución y transporte de medicamentos apócrifos y de insumos sanitarios críticos; a la venta de presuntos medicamentos comercializados bajo nomenclaturas y referencias al COVID–19 o sus derivaciones nominales, sin aprobación ni certificación de la autoridad competente; y a los ataques informáticos a infraestructura crítica –especialmente a hospitales y a centros de salud.

- Que las tareas de prevención deberán omitir aquellas conductas susceptibles de ser consideradas regulares, usuales o inherentes al uso de Internet y que no evidencien una intención de delinquir.

- Que se descartará toda posibilidad de acumulación de registros relativos a las personas, debiéndose proceder a su efectiva destrucción luego de concluida la actividad preventiva.

- Que queda prohibido obtener información, producir inteligencia o almacenar datos sobre personas o usuarios por el sólo hecho de su raza, fe religiosa, acciones privadas, u opinión política, o de adhesión o pertenencia a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales, así como por la actividad lícita que desarrollen en cualquier esfera de acción.

- Qu queda prohibido "emplear métodos ilegales o violatorios de la dignidad de las personas para la obtención de información", "comunicar o publicitar información sin autorización", "incorporar datos o información falsos", "utilizar fuentes digitales abiertas para monitorear y observar detenidamente individuos o asociaciones" y "almacenar los datos personales relevados a través del uso de fuentes digitales abiertas en registros o bases de datos, cuando no dieran lugar a actuaciones judiciales".
- Que es obligación de los agentes policiales aplicar los principios de "protección de los datos personales", de "protección de la libertad de expresión", de

"no criminalización de las protestas en línea" y de "destrucción del material prevenido o judicializado".

Como venimos apuntando, en España, aunque disponemos de normas marco que establecen los principios que deben respetar las actuaciones de ciberpatrullaje y *ciberinvestigación*, lo cierto es que los protocolos concretos de investigación de las fuerzas policiales carecen de publicidad alguna.

A este respecto, merece la pena recordar que, cuando se aprobó la entonces moderna ley de Enjuiciamiento Criminal no existía realmente un cuerpo de policía judicial como el que anunciaba la ley. De esa forma, las diligencias de investigación quedaban reguladas como si las ejecutara un juez, cuando lo cierto y verdad es que gran parte de dicho trabajo lo realiza la policía sin que quede sujeta a procedimiento alguno, porque no hay norma que regule las actividades policiales, a diferencia de lo que ocurre en el Reino Unido, Irlanda, Malta, Chipre, Suecia, Finlandia, Dinamarca, Eslovaquia, Estonia, Letonia o Lituania. Esta situación, como se ha dicho, debe encontrar su fin, debiendo buscar la transparencia en la actuación policial salvo supuestos justificados[207].

5. LA INTELIGENCIA SOBRE FUENTES ABIERTAS

A. DEFINICIÓN Y CARACTERES FUNDAMENTALES

El contenido material del *ciberpatrullaje* puede identificarse con la llamada inteligencia sobre fuentes abiertas, u *open–source intelligence* (OSINT), que es una práctica consistente en recabar datos e información de fuentes disponibles al público con la finalidad de obtener información suficiente sobre una determinada circunstancia, escenario o decisión relacionada con la seguridad nacional, la aplicación del ordenamiento jurídico o, incluso, con la inteligencia de negocios. Su utilidad reside en que, mediante el tratamiento adecuado, permite extraer una funcionalidad no prevista de datos públicamente disponibles, aprovechando las sinergias que pasan desapercibidas al resto de ciudadanos.

[207] NIEVA FENOLL, J., "La instrucción como falsa "primera instancia" del proceso penal: La instrucción como falsa "primera instancia" del proceso penal", *Revista ítalo–española de Derecho Procesal*, 1, 2019, Marcial Pons, p. 54.

También ha sido definida como la actividad de obtener legalmente material verbal, escrito o electrónico disponible públicamente[208], cuyas características principales son la eficiencia, la rapidez, la intermediación, la dependencia, la accesibilidad y el volumen[209].

Aunque el origen de la práctica debe remontarse en el tiempo a la propia aparición de una estructura política mínimamente organizada, con el advenimiento de las redes de comunicación instantánea y la inmediata transmisión de información ha ganado un especial protagonismo, especialmente gracias a la disponibilidad de la información en internet.

En particular, se recuerda que cualquier información puede ser objeto de dicha recopilación, sin importar su soporte material, desde publicaciones en prensa a informes oficiales, documentos científicos e información de agentes comerciales, y se destaca que la principal baza de esta práctica es que no requiere ninguna actividad clandestina ni vulneración alguna de derechos de propiedad intelectual[210]. Nuestra doctrina también se refiere a ella como aquel conjunto de recursos documentales públicos, de pago o gratuitos, en cualquier soporte, formato y medio de acceso, como las obras de referencia, bases de datos, monografías, publicaciones seriadas, literatura gris, sitios y páginas web, colecciones de imágenes, emisiones radiofónicas o de televisión, grabaciones sonoras y audiovisuales y, que contenga datos políticos, culturales, económicos, militares, científicos, técnicos, sociológicos, geográficos, etc.[211]

El OSINT permite obtener más inteligencia con menor esfuerzo y en menor plazo, desde el punto de vista de la inversión en recursos y la relación de su coste con los beneficios generados. Además, el acceso a la información abierta es más ágil y rápido. Paralelamente, las técnicas OSINT dependen de intermediarios que se encarguen de publicar la información, y suelen enfrentar cantidades ingentes de información, que es necesario

---

[208] RICHELSON, J., *The U.S. Intelligence Community*, Hachette UK, 2015.
[209] RODRÍGUEZ RODRÍGUEZ, Y., "Inteligencia de fuentes abiertas (osint): Características, debilidades y engaño", *Análisis GESI*, 11, 2019, Departamento de Ciencia Política y de la Administración, en https://www.seguridadinternacional.es/?q=es/content/inteligencia-de-fuentes-abiertas-osint-caracter%C3%ADsticas-debilidades-y-enga%C3%B1o, fecha de consulta 20 de noviembre de 2020.
[210] GEORGE, R.; KLINE, R., *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, Rowman & Littlefield, 2006.
[211] FELIP I SARDÁ, J. M., "La gestión de fuentes abiertas por los servicios de Inteligencia y los equipos de investigación: el estado de la cuestión", *Cuadernos constitucionales de la Cátedra Fadrique Furió Ceriol*, 48, 2004, Departamento de Derecho Constitucional y Ciencia Política y de la Administración.

filtrar y procesar. En la actualidad, el alto volumen de información ha causado que los mayores esfuerzos se dirijan a la actividad de procesamiento de la información.

En ese sentido, la cantidad de datos disponibles de manera abierta expone a los organismos y agencias encargados de practicar esta inteligencia a quedar verdaderamente abrumados por el volumen de información a gestionar. Para tratar de solventar esta problemática, han surgido iniciativas de todo tipo, que persiguen dotar a los organismos competentes de las herramientas necesarias para automatizar los procesos de análisis e incluir en ellos el máximo volumen de información. Tal es el caso de In–Q–Tel, una entidad de capital riesgo vinculada con la CIA y cuya finalidad es identificar e invertir en las empresas que desarrollan tecnologías de vanguardia que puedan servir a los intereses de seguridad nacional de los Estados Unidos[212]. Lo mismo sucede con la empresa Palantir Technologies, especializada en el análisis de *big data*, a través de sus productos *Palantir Gotham, Palantir Metropolis y Palantir Foundry*.

Estas iniciativas, aunque se encuentren vinculadas con agencias gubernamentales, se desarrollan bajo el paraguas de entidades de derecho privado que, como tales, exportan sus servicios a cualquier país u organización del globo, incluida España[213].

Relacionado con esta figura, se encuentra el concepto de "inteligencia criminal", denominación con la que se alude al conjunto de actividades de inteligencia realizada por los servicios de información de la policía para prevenir y averiguar la comisión de delitos[214]. Es una figura en la que, como se puede apreciar, concurren una faceta preventiva –destinada a patrullar el espacio público en busca de hallazgos delictivos– y una resolutiva –destinada a obtener el material que pueda necesitar un proceso penal que se está sustanciando–.

En ese proceso de obtención de inteligencia para el proceso penal, pueden distinguirse las siguientes fases[215]:

---

[212] "In–Q–Tel", *Wikipedia*, 2020, fecha de consulta 19 marzo 2020, en https://en.wikipedia.org/w/index.php?title=In–Q–Tel&oldid=946318783.
[213] Como queda patente aquí, por ejemplo https://elpais.com/tecnologia/2020–04–02/palantir–misterioso–proveedor–del–pentagono–y–la–cia–ofrece–a–espana–sus–servicios–contra–el–coronavirus.html
[214] VALLÉS CAUSADA, L., "La polícia judicial en la obtención de inteligencia sobre comunicaciones electrónicas para el proceso penal", 2012, UNED. Universidad Nacional de Educación a Distancia (España), p. 447.
[215] *Ibid.*, p. 448.

- Evaluación: identificación y adquisición legítima de todas aquellas informaciones de cualquier naturaleza que, de una forma objetiva, puedan contribuir al cumplimiento de sus finalidades.

- Integración: contraste con otras cuyo contenido pueda concurrir a un mismo fin, esto es, a servir al esclarecimiento final, completo e inequívoco de los hechos delictivos.

- Análisis: descubrimiento y determinación del significado objetivo de las informaciones tras haberlas relacionado entre sí.

- Interpretación: concepción, ordenación y expresión intelectiva de la realidad desde las evidencias aportadas.

- Contradicción y valoración de la prueba: formación de la opinión jurisdiccional sin la contaminación de elementos subjetivos o cualesquiera otros que hayan sido deficientemente incorporados al proceso penal.

El principio de inteligencia estratégica en materia criminal persigue concentrar los esfuerzos de los cuerpos policiales en las actividades criminales y personas clave, a partir de la identificación y medición conforme a prácticas de inteligencia[216]. Dicho principio también ha sido definido como la aplicación del análisis de inteligencia criminal para la toma de decisiones, reducir la criminalidad y prevenirla a partir de estrategias efectivas, identificándose cuatro elementos fundamentales: concreción de los criminales, gestión de los puntos de conflicto, investigación de conductas delictivas y aplicación de medidas preventivas[217].

B. ORÍGENES DE LA PRÁCTICA MODERNA

En Estados Unidos, las prácticas OSINT se remontan al servicio *Foreign Broadcast Monitoring Service (FBMS) Office of Strategic Services (OSS)*, establecidos con la administración Roosevelt en el año 1941 con la finalidad de traducir, transcribir y analizar programas de radio de propaganda de onda corta que estaban siendo emitidos en los Estados Unidos por las potencias del Eje, encargándose incluso de traer prensa del bando

[216] COPE, N., "Intelligence led policing or policing led intelligence", *Dialnet*, 2, 2004.
[217] RATCLIFFE, J., *Intelligence-led policing*, Australian Institute of Criminology, Canberra, 2003, p. 3.

del Eje. Con el ataque a Pearl Harbor a finales del mismo año, el servicio ganó mayor importancia y pasó a *denominarse Foreign Broadcast Information Service (FBIS).*

Con el final de la segunda guerra mundial, pasó a quedar incluido dentro del organigrama de la CIA, y asumía las funciones de monitorear, traducir y diseminar dentro de los Estados Unidos las noticias e información que pudiera recabar desde fuentes extranjeras, desplegando importantes efectos durante el período de la guerra fría.

Posteriormente, en noviembre de 2005, el FBIS fue absorbido por el *Open Source Center*, que asumió expresamente la tarea de recolectar y analizar la información públicamente disponible en Internet, bases de datos, prensa, radio, televisión, video, geospatial data, photos and commercial imagery[218]. Con la *Intelligence Community Directive 301*, las funciones del FBIS adquirieron aún mayor relevancia, pues la información de libre acceso pasó a considerarse como una de las principales fuentes de inteligencia.

Otras agencias u organismos similares son la *BBC Monitoring*, en Reino Unido, con orígenes también en la Segunda Guerra Mundial, y el *Office of National Assessments*, en Australia, creada en 1974.

Algunas herramientas utilizadas son *Censys*, *Kali*, *Maltego*, *Shodan*, *Eleven Paths*, *OSFramework*[219], el comando *–nslookup* seguido del nombre del servidor o dirección de internet, la búsqueda *whois*, el *analyst's notebook* de IBM, el *IBM SPSS Modeler*, y la técnica de la desanonimización de los datos. Sobre esta última cuestión, merece la pena traer a colación un estudio en el que investigadores de la Universidad de Zurich consiguieron eliminar la anonimización de datos efectuada por los tribunales suizos[220], bastando a tal efecto con algunos *twits* para identificar fácilmente a su autor[221]. Tal es la preocupación al respecto que, ya en 1998, fue creado un índice que identificara el grado

---

[218] "Office of the Director of National Intelligence", 2006, fecha de consulta 19 marzo 2020, en https://web.archive.org/web/20060623072458/http://dni.gov/press_releases/20051108_release.htm.

[219] RUBIO VIÑUELA, Y.; BREZO FERNÁNDEZ, F., "La utilización de herramientas de monitorización de usuarios como base para el perfilado de identidades en fuentes abiertas: OSRFramework", en *Actas de las primeras Jornadas Nacionales de Investigación en Ciberseguridad: León, 14, 15, 16 de septiembre de 2015. I JNIC2015, 2015, pp. 32–38*, Servicio de Publicaciones, 2015, fecha de consulta 19 marzo 2020, en https://dialnet.unirioja.es/servlet/articulo?codigo=5469650.

[220] CHANDLER, S., "Researchers Use Big Data And AI To Remove Legal Confidentiality", *Forbes*, fecha de consulta 19 marzo 2020, en https://www.forbes.com/sites/simonchandler/2019/09/04/researchers–use–big–data–and–ai–to–remove–legal–confidentiality/.

[221] "How hard is it to «de–anonymize» cellphone data?", *MIT News*, fecha de consulta 19 marzo 2020, en https://news.mit.edu/2013/how–hard–it–de–anonymize–cellphone–data.

de seguridad que poseía determinada información anonimizada: k–anonyimty (posteriormente utilizado en el servicio *"Have I Been Pwned?"*[222]).

Esta práctica ha venido ganando mayor relevancia desde la comisión en el año 2001 de los atentados terroristas del 11S y la *"War on Terror"* que la administración Bush implantó en Estados Unidos. La aplicación de métodos más sofisticados, tanto para la recolección de datos como para su posterior análisis, así como la transgresión de la frontera de lo "públicamente accesible" ha conformado una nueva práctica modernamente conocida como *data mining*[223], que se ha convertido en una "dimensión esencial del contraterrorismo, la ciberseguridad, la aplicación de políticas de drogas, la seguridad fronteriza y la recopilación de información para fines de inteligencia"[224].

Merece la pena destacar que, suscitada por la irrupción de la crisis de la covid-19, parecen haberse puesto de manifiesto las bondades de las herramientas de vigilancia masiva[225]. Numerosos Estados (Israel, China y la India, entre otros[226]) afectados han adoptado medidas para aprovechar dichas fuentes de datos, sobre todo relativas a la movilidad de los ciudadanos[227]. Incluso la compañía Palantir ha llegado a ofrecer sus servicios a España, en un movimiento estratégico para aprovechar circunstancias que permitan exponer la cara amable de sus servicios[228].

C. PLATAFORMAS P2P

A través de las plataformas P2P, la Policía Judicial rastrea las fuentes abiertas existentes en la web. La red P2P es un servicio de intercambio gratuito de archivos entre

---

[222] "K–anonymity", *Wikipedia*, 2020, fecha de consulta 19 marzo 2020, en https://en.wikipedia.org/w/index.php?title=K–anonymity&oldid=944270840.
[223] "A Tech Fix For Illegal Government Snooping?", *NPR.org*, fecha de consulta 19 marzo 2020, en https://www.npr.org/templates/story/story.php?storyId=106479613.
[224] COHEN, S., "¿Quién necesita extraer inteligencia de fuentes abiertas (OSINT)?", *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones*, 84, 2019, Borrmart.
[225] BYUNG–CHUL, H., "La emergencia viral y el mundo de mañana. Byung–Chul Han, el filósofo surcoreano que piensa desde Berlín", *EL PAÍS*, 2020, fecha de consulta 2 abril 2020, en https://elpais.com/ideas/2020–03–21/la–emergencia–viral–y–el–mundo–de–manana–byung–chul–han–el–filosofo–surcoreano–que–piensa–desde–berlin.html.
[226] "Tecnología, la nueva tentación que acecha a la libertad", *abc*, 2020, fecha de consulta 3 mayo 2020, en https://www.abc.es/cultura/abci–tecnologia–nueva–tentacion–acecha–libertad–202004190256_noticia.html.
[227] MUÑOZ, R., "Más de 40 millones de teléfonos móviles serán usados para rastrear el coronavirus en toda España", *EL PAÍS*, 2020, fecha de consulta 2 abril 2020, en https://elpais.com/economia/2020–04–01/mas–de–40–millones–de–telefonos–moviles–seran–usados–para–rastrear–el–coronavirus.html.
[228] PÉREZ COLOMÉ, J., "Palantir, misterioso proveedor del Pentágono y la CIA, ofrece a España sus servicios contra el coronavirus", *EL PAÍS*, 2020, fecha de consulta 2 abril 2020, en https://elpais.com/tecnologia/2020–04–02/palantir–misterioso–proveedor–del–pentagono–y–la–cia–ofrece–a–espana–sus–servicios–contra–el–coronavirus.html.

sus usuarios, que realizan la comunicación entre sí de manera privada a través de un servidor–intermediario. Mediante esta herramienta, tiene lugar un intercambio de una ingente cantidad de información entre múltiples usuarios, que pueden descargar archivos de diferente tipo de manera compartida, a la vez que continúan manteniendo la cadena.

La técnica que utilizan las fuerzas policiales para investigar en las plataformas P2P puede resumirse conforme a los siguientes pasos[229]:

1. Identificación de "archivos de interés" (*file of interest* o *FOI*), ya sean archivos cuya posesión constituya por sí misma delito u otros archivos que revelen interés en ese tipo de contenidos. La policía recoge estos archivos navegando por internet a través de búsquedas, descargas P2P, o soportes intervenidos, y obtiene su *hash* único para poder identificarlos en el futuro.

2. Búsqueda de posibles sospechosos de la tenencia de dichos archivos en los registros públicamente accesibles de los protocolos P2P, sin necesidad de autorización judicial. Se obtiene también la IP y otra información identificativa en el protocolo P2P, como los Identificadores Únicos Globales o *Globally Unique Identifiers (GUIDs)*

3. Selección de principales sospechosos en función de distintos factores como el tamaño de las descargas, demás archivos compartidos por el usuario P2P, etc.

4. Validación de que los archivos delictivos son ofrecidos desde los sospechosos en concreto, por ejemplo, limitando la descarga P2P para que solamente utilice la semilla del usuario sospechoso.

5. Emitir requerimiento al correspondiente ISP para que facilite los datos identificativos de las IP sospechosas.

Es característico de este tipo de redes que el archivo se transmite entre el oferente y el interesado, de manera que la transmisión de datos tiene lugar entre los dos equipos

[229] LIBERATORE, M.; ERDELY, R.; KERLE, T.; LEVINE, B. N.; SHIELDS, C., "Forensic investigation of peer–to–peer file sharing networks", *Digital Investigation*, vol. 7, 2010, (The Proceedings of the Tenth Annual DFRWS Conference).

informáticos sin que el archivo quede almacenado en el servidor, donde únicamente queda una relación de los usuarios y los archivos transmitidos.

En general, la doctrina[230] entiende que, al insertar elementos en la web a los que pueda tener acceso a cualquier usuario, existe un consentimiento tácito que excluye la afectación del derecho a la intimidad y a la protección de datos personales de los artículos 18.1 y 18.4 CE. Tampoco se afectaría al derecho al secreto de las comunicaciones, en la medida en que no existiría un proceso de comunicación entre el emisor y una persona determinada o determinable, sino que se trata de un acto con un receptor, si existiera, indeterminado.

En ese sentido, la STS 752/2010, de 14 de julio, concluía que "en relación con la vulneración del derecho al secreto de las comunicaciones, no aporta dato alguno fuera de identificarla con la captación de los mensajes y contactos realizados por el mismo a través de internet, olvidando que el acceso a la información así producida puede efectuarla cualquier usuario, no precisándose autorización judicial para conseguir lo que es público cuando el propio usuario de la red ha introducido dicha información en la misma (ver STS 739/2008 y las citadas en la misma)". En este caso concreto, debe destacarse que fue el acusado el que contactó, inadvertidamente para él, con un agente policial australiano –camuflado bajo un pseudónimo–, remitiéndole fotografías de contenido pedófilo. A raíz de este encuentro, se acordó la entrada y registro en el domicilio del acusado, hallando archivos suficientes para un posterior juicio condenatorio.

Lo cierto es que casos como el expuesto evidencian la confusión que existe respecto a cuáles han de ser los límites de la actuación policial en internet en este tipo de supuestos. El mismo concepto "abierto" implica una interpretación de la actuación del ciudadano investigado que parece desatender el nivel de conocimientos técnicos que el mismo puede tener respecto del modo en que su información queda alojada en internet. El consentimiento tácito no puede atribuirse indiscriminadamente por el mero hecho de utilizar una red que, en absoluto, se anuncia como de contenido abierto.

A lo anterior habrá que añadir los supuestos de "pseudoincitación" en los que, en ocasiones, podría incurrir la Policía Judicial, que analizaremos con posterioridad.

---

[230] CALVO LÓPEZ, D., "Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (apartados K) a M) del art. 588 ter de la LECrim)", cit., p. 6.

También cabe la posibilidad de que el agente policial utilice, en esas redes abiertas, un *nickname* que impida identificarlo como agente de policía. Para ello no será necesario que cuente con autorización judicial. Como indicó la STS 173/2018, de 11 de abril, la regla general es el uso de *nicknames*, por lo que su uso no afecta a la confianza existente en el medio ni supone engaño por la autoridad pública. En nuestra opinión, sin embargo, sí podría apreciarse un mínimo engaño, toda vez que los únicos que utilizan *nicknames* son sujetos de derecho privado, que carecen de potestades públicas y ni las representan ni las ponen en ejercicio frente al resto de usuarios; por el contrario, los poderes públicos no se vienen manifestando a través de *nicknames* en la red.

Tampoco, en este sentido, parece entenderse que exista afectación al secreto de las comunicaciones cuando uno de los comunicantes sea el propio agente, de manera que no existe inmisión en una comunicación establecida entre terceros.

Los rastreos informáticos en redes P2P se efectúan mediante búsqueda de IP. Según la jurisprudencia, no afectan a los derechos fundamentales previstos en el artículo 18 CE, por lo que no es necesaria la autorización judicial para obtener esa dirección IP, pues se trata de datos públicos que el propio usuario ha introducido en la web[231].

La Policía Judicial dispone de medios técnicos para rastrear en los servidores según el contenido de los archivos compartidos, utilizando para ello el algoritmo *hash*, obteniendo la dirección IP del usuario en el momento de la transmisión correspondiente al fichero analizado, y así identificar una conexión. Los códigos *hash* que suelen utilizarse son los de los archivos que contienen material delictivo, especialmente en los supuestos de pornografía infantil.

Normalmente no se investiga una descarga puntual de un archivo concreto, sino que se trata de concretar una acción reiterada en el tiempo, a fin de acreditar una conducta intencional en el sujeto investigado. Se trata, pues, de una técnica que, en cierto modo, compromete el principio de especialidad que se predica de las diligencias de investigación tecnológicas.

La jurisprudencia entiende que obtener la dirección IP mediante el uso de estos rastreos en el espacio público no afecta a los derechos fundamentales del artículo 18 CE,

[231] STS 1299/2011, de 17 de noviembre, STS 680/2010, de 14 de julio, STS 739/2008, de 12 de noviembre, STS 236/2008, de 9 de mayo, o STS292/2008, de 28 de mayo

por lo que no es necesaria autorización judicial, en la medida en que se trata de datos públicos que el usuario ha introducido en la web[232]. La STS 1299/2011 establece que "no se precisa autorización judicial para conseguir lo que es público y el propio usuario interesado de la red es quien lo introduce en la misma. La huella de la entrada queda registrada siempre y ello lo sabe el interesado". Ese es el motivo de que el artículo 588 *ter* k) LECrim permita que la Policía utilice artificios técnicos para acceder a direcciones IP. Esta perspectiva se mantiene en el anteproyecto de LECrim de 2020, que únicamente prevé la necesidad de autorización judicial para identificar la dirección IP previamente obtenida por la policía en ejercicio de sus funciones generales de prevención.

También se afirma en estos supuestos que "el principio del consentimiento, bien expreso, bien presunto, por razón de la cognoscibilidad del usuario de tales redes de que cualquier persona puede acceder a buena parte de los datos que ha compartido o transmitido en abierto, se perfila como la clave para la solución propuesta por el Tribunal Supremo" y que, en fin, el consentimiento tácito del interesado excluye la afectación tanto del derecho a la intimidad como del derecho a la protección de datos personales[233].

La STS 680/2010, de 14 de julio, afirma que "quien utiliza un programa P2P, en nuestro caso EMULE, asume que muchos de los datos se convierten en públicos para los usuarios de Internet, circunstancia que conocen o deben conocer los internautas, y tales datos conocidos por la policía, datos públicos en Internet, no se hallaban protegidos por el artículo 18.1 ni por el artículo 18.3 CE". A nuestro juicio, esta interpretación desatiende la realidad de los conocimientos técnicos de muchos usuarios, a los que les atribuye una responsabilidad superior a la que corresponde a alguien con conocimientos medios.

En ese sentido, la STS 236/2008 considera válidos los rastreos de redes P2P efectuados por la policía de las redes P2P sin orden judicial previa, concluyendo que no vulneran el derecho al secreto de las comunicaciones porque i) no hay secreto sobre datos que el usuario aporta voluntariamente a la red de redes, que por tanto no pueden merecer la condición de confidenciales, ni preservados del conocimiento público y general; ii) la información obtenida era únicamente que direcciones IP accedían a determinados *hash*, información de público acceso en la red; iii) Las IP no concretan el usuario, sino sólo el

[232] STS 1299/2011, de 17 de noviembre, STS 680/2010, de 14 de julio, STS 739/2008, de 12 de noviembre, STS 236/2008, de 9 de mayo, o STS292/2008, de 28 de mayo

[233] RODRÍGUEZ LAINZ, J. L., "Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas", *Diario La Ley*, 7086, 2009, Wolters Kluwer, p. 3.

ordenador asociado a una línea de acceso a internet, lo que hace necesaria la intervención judicial para conocer al titular del contrato.

En definitiva, el Tribunal Supremo concluye que los rastreos que realiza el equipo de delitos telemáticos de la Guardia Civil en Internet tienen por objeto desenmascarar la identidad críptica de los IP (*Internet protocols*) que habían accedido a los *hash* investigados. El acceso a dicha información puede efectuarla cualquier usuario. No se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma.

Por nuestra parte, entendemos que el usuario no asume que los datos necesarios para establecer una conexión IP sean públicos para el resto de usuarios, pues, por un lado, generalmente desconoce lo suficiente de la tecnología como para ignorar tal circunstancias y, por otro lado, lo cierto es que se confía en el desinterés del resto de usuarios respecto a dichos datos[234].

En relación con la obtención de información de servicios de inteligencia, el TEDH acepta que se pueda utilizar no sólo como pista secreta en investigaciones penales, sino como prueba que genere una sospecha razonable de culpabilidad[235].

D. PERICIALES DE INTELIGENCIA

El entramado de circunstancias que venimos comentando permite apreciar que, si bien en tiempos pasados podía establecerse una clara separación entre las funciones preventivas y las investigadoras dentro de los cuerpos policiales y de inteligencia, en la actualidad dicha distinción ha comenzado a desdibujarse, existiendo la posibilidad de que los resultados obtenidos con investigaciones de inteligencia tengan acceso a un posterior proceso penal.

En nuestro ordenamiento, el principio de especialidad establecido en el apartado 2 del artículo 588 *bis* a) LECrim establecería, en principio, una separación estricta entre las funciones de inteligencia y las funciones de investigación de los delitos. A ello apunta, también la vaguedad del artículo o11.1.f) LOFCS, que no puede entenderse como norma habilitante para adoptar tales medidas. Por otro lado, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y la Ley Orgánica 2/2002, de 6 de mayo,

---

[234] MAEZTU, D., "El rastreo de usuarios en internet por la policia. Sentencia del TS 236/2008".
[235] ARMENTA DEU, T., "Prueba ilícita y regla de exclusión", cit., p. 132.

reguladora del control judicial previo del Centro Nacional de Inteligencia, prevén la necesidad de que, para adoptar medidas de inteligencia que afecten a la inviolabilidad del domicilio y al secreto de las comunicaciones, sea necesaria autorización del Magistrado del Tribunal Supremo competente[236].

Ahora bien, y como ha puesto de relieve la doctrina[237] concurren algunas circunstancias que impiden gozar de mayor tranquilidad en este ámbito.

Así, por un lado, la referida Ley Orgánica 2/2002 únicamente se refiere a los derechos fundamentales a la inviolabilidad del domicilio y al secreto de las comunicaciones a la hora de exigir la previa autorización judicial, pero no se pronuncia respecto del derecho al propio entorno virtual ni tampoco respecto del derecho a la intimidad, cuando ambos podrían quedar vulnerados en una actuación de inteligencia.

Por otro lado, existe el riesgo[238] de que los hallazgos de las actuaciones de inteligencia tengan acceso a un posterior proceso penal a través de los denominados "informes policiales de inteligencia", que consiste en un informe detallado compuesto por el estudio, obtención de datos y documentos vinculados, conexión de actos y conclusiones indiciarias sobre la composición, participación y atribución de participación delictiva de concretos integrantes en actos criminales de grupos u organizaciones realizada por expertos policiales[239]. Cuanto menos, merece la pena señalar que el referido informe pericial debería ser ratificado posteriormente en el acto de juicio[240].

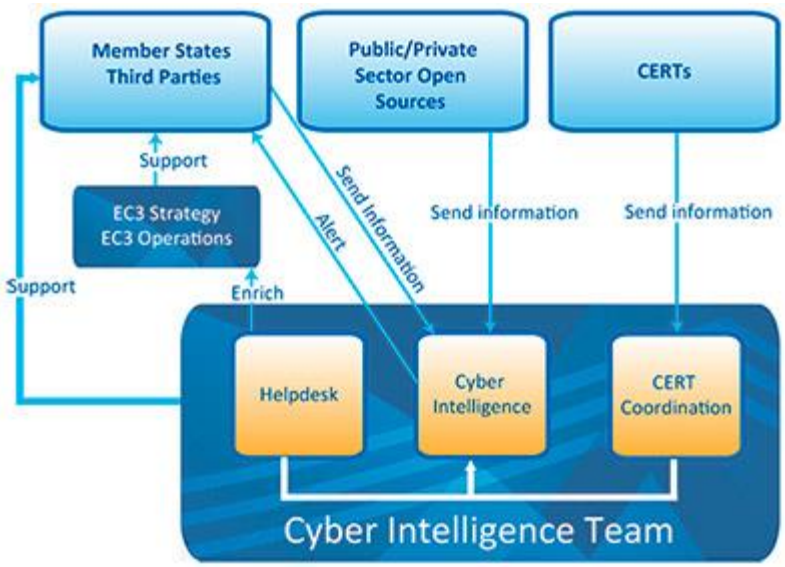
E. ACTIVIDADES DE EUROPOL

Las actividades de inteligencia sobre fuentes abiertas constituyen una de las ramas de actuación de Europol, procurando recoger la información públicamente disponible, procesarla y analizarla para otorgar una ventaja a las fuerzas policiales en la tarea de prevención del cibercrimen.

---

[236] Competencia que resulta, a su vez, de los artículos 598.9ª y 599.1.4ª LOPJ.
[237] GONZÁLEZ NAVARRO, A., "Servicios de inteligencia y orden europea de investigación", en *Orden europea de investigación y prueba transfronteriza en la Unión Europea, 2019, pp. 225–238*, Tirant lo Blanch, 2019, p. 235, fecha de consulta 15 noviembre 2021, en https://dialnet.unirioja.es/servlet/articulo?codigo=6949798.
[238] STS, Sala 2ª, de 25 de octubre de 2011.
[239] Un estudio pormenorizado de esta diligencia puede encontrarse en las STS 13/12/2001; 7/06/2002; 19/06/2002; 29/05/2003, 6/05/2004; 21/05/2004; 22/04/2005; 1/10/2007 y 22/05/2009 citadas en el estudio que sobre esta diligencia procesal realiza GÓMEZ BERMÚDEZ, No destruirán nuestra libertad, pp. 151–157, Premio de Hoy de Editorial Planeta, Madrid, 2010.
[240] VELASCO NÚÑEZ, E., "Crimen organizado, internet y nuevas tecnologías", cit., p. 264.

Para ello, Europol emite notificaciones regulares en materia de inteligencia sobre criminalidad (*cyber–bits*), elabora un sistema de captura y procesamiento de la información disponible en las fuentes abiertas (*OSINT Dashboard*), y coordina los equipos de respuesta (*CERT coordination*).



Los *CyberBits* son notificaciones emitidas por Europol para mantener tanto a los diferentes agentes ocupados de la ciberseguridad como incluso al público en general en la actualidad del sector. Los clasifica en: *trends*, que son actualizaciones sobre patrones emergentes o modus operandi nuevos utilizados por los cibercriminales; *knowledge*, que son guías sobre diferentes aspectos del cibercrimen; *technology*, que constituyen recopilatorios de desarrollos tecnológicos de interés en la lucha contra el cibercrimen; y *tools*, que son nuevas herramientas elaboradas por el Centro Europeo de Cibercrimen (EC3) específicamente al efecto de la lucha contra la ciberdelincuencia.

Por su parte, el *OSINT dashboard* consiste en una actualización semanal que recoge los eventos más importantes en materia de ciberseguridad y cibercrimen.

Finalmente, en materia de coordinación de la red de CSIRTS, Europol elabora guías que permiten la clasificación homogénea de ciberataques y otros incidentes y actores, además de subsumir los eventos que tengan lugar en el marco normativo establecido por la Directiva 2013/40/EU y el Convenio de Budapest, todo ello con la finalidad de proporcionar un frente común y unido en la lucha contra el cibercrimen[241].

[241]https://www.europol.europa.eu/activities–services/services–support/intelligence–analysis/cyber–intelligence

6. OBTENCIÓN DE DIRECCIONES IP

A. CONCEPTUALIZACIÓN DE LA MEDIDA

Nos referimos con esto a los diversos casos en los que la policía obtiene la dirección IP del espacio público de internet, sin dirigirse específicamente contra un usuario en concreto.

B. CONCEPTO DE DIRECCIÓN IP

La dirección IP es una etiqueta numérica que se asigna a la interfaz de red de un dispositivo que utilice el protocolo de internet (*Internet Protocol*) que, a su vez, está formado por el conjunto de protocolos de comunicación utilizados en internet, y es más conocido por las siglas TCP/IP, en la medida en que sus protocolos fundamentales son el protocolo de control de transmisiones (*Transmission Control Protocol*) y el protocolo de internet (*Internet Protocol*), cuyos orígenes se remontan a ARPANET, una red de computadoras y primera red de área amplia (*wide area network*) que fue desarrollada por encargo de DARPA (*Defense Advanced Research Projects Agency*)[242], agencia incluida en el Departamento de Defensa de los Estados Unidos, motivo por el que también se conoce como modelo DoD (*Department of Defense*)[243].

La versión 4 del protocolo de internet, IPv4 (*Internet Protocol version 4*) define la dirección IP como un número binario de 32 bits permitiendo un espacio de direcciones de hasta 4.294.967.296 (es decir, 2^{32}) direcciones posibles[244]. Para expresarse en notación decimal, los 32 bits son divididos en 4 octetos o bytes, de 8 bits cada uno, lo que determina que cada octeto o byte pueda tener un valor de entre 0 y 255 (esto es así porque con 8 bits el número más alto que puede representarse es 255, toda vez que en notación binaria las posiciones 11111111 tienen valores decimales, de derecha a izquierda, de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma un total de 255). Ante el previsible agotamiento del protocolo IPv4 se está implantando progresivamente el protocolo IPv6[245], que prevé direcciones IP compuestas por 128 bits en lugar de 32 bits, cuya ventaja en cuanto a capacidad de direccionamiento respecto del protocolo IPv4 se evidencia desde el momento en que admite 340.282.366.920.938.463.463. 374.607.431.768.211.456 direcciones posibles (es decir,

---

[242] POSTEL, J., "DoD standard Internet Protocol".
[243] POSTEL, J., "Internet Protocol".
[244] ARREOLA GARCÍA, A., *Ciberseguridad: ¿Por qué es importante para todos?*, Siglo XXI Editores México, 2019.
[245] "Internet Protocol, Version 6 (IPv6) Specification", fecha de consulta 14 abril 2020, en https://tools.ietf.org/html/rfc2460.

2^{128}), número completamente inconmensurable cuya duración se estima en 480 años antes de su agotamiento que permite el desarrollo del internet de las cosas (Internet of Things, IoT), entre otros elementos y sustanciales mejoras[246].

La dirección IP no debe confundirse con la dirección MAC, que no depende del protocolo de conexión utilizado en la red. También es posible que la dirección IP de un mismo dispositivo varíe con cada sesión de conexión, toda vez que el protocolo DHCP permite liberar de manera dinámica las IP no utilizadas y asignarlas conforme vaya resultando necesario. Por otro lado, en 1981 el direccionamiento de internet fue revisado y se introdujo la arquitectura de clases (*Classful Network Architecture*), que preveía las clases A, B, C, D y E.[247]

Toda la estructura expuesta precisa de un organismo que asuma la coordinación y gestión de dicho protocolo de internet. A esa finalidad se dedicaba la *Internet Assigned Numbers Authority* (*IANA*), entidad internacional que supervisa la asignación global de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio DNS y otros recursos relativos a los protocolos de Internet[248] que, posteriormente, fue integrada en la *Internet Corporation for Assigned Names and Numbers* (*ICANN*), entidad sin ánimo de lucro constituida en 1998, radicada en el Estado de California y sujeta a las leyes de dicho Estado[249]. A su vez, la ICANN, a través de la IANA, delega sus paquetes de recursos en Registros Regionales de Internet o RIR (*Regional Internet Registry*), que son los que asignan definitivamente dichos recursos a los usuarios de su zona de competencia. Actualmente existen los cinco siguientes: *American Registry for Internet Numbers* (*ARIN*)[250] para Norteamérica, *RIPE Network Coordination Centre* (*RIPE NCC*)[251] para Europa, el Oriente Medio y Asia Central, *Asia–Pacific Network Information Centre* (*APNIC*)[252] para Asia y la Región Pacífica, *Latin American and Caribbean Internet Address Registry*

[246] "Razones para la transición – IPv6", 2016, fecha de consulta 14 abril 2020, en https://web.archive.org/web/20161104001553/http://www.ipv6.es/es–ES/transicion/quees/Paginas/10razones.aspx.
[247] ANDREU, J., *Instalación de equipos de red. Configuración (Redes locales)*, Editex, 2011.
[248] "Internet Assigned Numbers Authority", 2017, fecha de consulta 14 abril 2020, en https://web.archive.org/web/20170920185613/http://www.iana.org/.
[249] "Beginner's Guides – ICANN", fecha de consulta 14 abril 2020, en https://www.icann.org/resources/pages/beginners–guides–2012–03–06–en.
[250] "American Registry for Internet Numbers", fecha de consulta 14 abril 2020, en https://www.arin.net/.
[251] "RIPE Network Coordination Centre", fecha de consulta 14 abril 2020, en https://www.ripe.net/.
[252] "APNIC", fecha de consulta 14 abril 2020, en https://www.apnic.net/.

(*LACNIC*)[253] para América Latina y el Caribe, y *African Network Information Centre* (*AfriNIC*)5 para África[254].

Precisamente la dependencia de la ICANN respecto de la normativa estadounidense, unida a su competencia respecto de los servidores raíz de nombres de dominio, ha sido fuente de controversia en relación con la gobernanza de internet[255].

C. PROTECCIÓN DISPENSADA AL DATO DE LA IP

En realidad, y como se ha destacado en ocasiones[256], el precepto sigue el criterio jurisprudencial marcado por el Tribunal Supremo (en sus SSTS 342/2013, de 17 de abril, y 680/2010, de 14 de julio) en cuanto a la falta de necesidad de contar con autorización judicial para proceder a obtener una dirección IP. Como hemos indicado con anterioridad, tal número únicamente identifica un dispositivo electrónico, y no a la persona que lo utiliza, ni revela información de las comunicaciones realizada por ella.

En este sentido, generalmente[257] se entiende que la dirección IP no ha de considerarse amparada por el derecho al secreto de las comunicaciones del artículo 18.3 CE, en la medida en que no supone contenido comunicativo alguno. Aunque podría estar protegida por el artículo 18.4 CE, creemos que la protección dispensada sería insuficiente, al tratarse de un dato público. Al ser internet una red pública y abierta de comunicaciones basada en el protocolo TCP/IP, ampara una expectativa de privacidad por parte del usuario prácticamente inexistente por lo que se refiere a ese código.

En ese sentido, la STC 173/2011, indica que *"*el consentimiento eficaz del sujeto particular permitirá la inmisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno (SSTC 83/2002, de 22 de abril, FJ 5 y 196/2006, de 3 de julio, FJ 5), aunque este consentimiento puede ser revocado en cualquier momento (STC 159/2009, de 29 de junio, FJ 3). Ahora bien, se vulnerará el derecho a la intimidad personal cuando la penetración en el ámbito propio y reservado del sujeto "aun autorizada, subvierta los términos y el

---

[253] "LACNIC Inicio", fecha de consulta 14 abril 2020, en https://www.lacnic.net/.
[254] "AFRINIC – Regional Internet Registry for Africa", *AFRINIC – Regional Internet Registry for Africa*, fecha de consulta 14 abril 2020, en https://www.afrinic.net/.
[255] TAYLOR, E.; HOFFMANN, S., "EU–US Relations on Internet Governance", fecha de consulta 14 abril 2020, en https://www.chathamhouse.org/sites/default/files/publications/research/2019–11–14–EU–US–Relations–Internet–Governance2.pdf.
[256] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 460.
[257] *Ibid.*

alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida" (SSTC 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 5; y 70/2009, de 23 de marzo, FJ 2). En lo relativo a la forma de prestación del consentimiento, hemos manifestado que este no precisa ser expreso, admitiéndose también un consentimiento tácito. Así, en la STC 196/2004, de 15 de noviembre, en que se analizaba si un reconocimiento médico realizado a un trabajador había afectado a su intimidad personal, reconocimos no sólo la eficacia del consentimiento prestado verbalmente, sino además la del derivado de la realización de actos concluyentes que expresen dicha voluntad (FJ 9). También llegamos a esta conclusión en las SSTC 22/1984, de 17 de febrero, y 209/2007, de 24 de septiembre, en supuestos referentes al derecho a la inviolabilidad del domicilio del artículo 18.2 CE, manifestando en la primera que este consentimiento no necesita ser "expreso" (FJ 3) y en la segunda que, salvo casos excepcionales, la mera falta de oposición a la intromisión domiciliar no podrá entenderse como un consentimiento tácito (FJ 5).*"*

En similar sentido, la STS 1299/2011, de 17 de noviembre, declaraba que los rastreos realizados por la policía con el objeto de averiguar los IP que hubieran accedido a archivos de pornografía infantil no se diferenciaban de la que podía realizar cualquier usuario, en la medida en que es el propio usuario el que introduce su IP en la red, a sabiendas de que la huella de entrada queda registrada, como cuando, en el caso de un programa P2P, los usuarios asumen que muchos de sus datos se convierten en públicos, entendiendo el tribunal que dicha circunstancia es conocida o debe ser conocida por los internautas.

A nuestro juicio, se trata un argumento discutible, no sólo porque implique asumir la existencia de un consentimiento tácito respecto de la disposición de un derecho que es irrenunciable por su carácter fundamental, sino porque los usuarios tienen la posibilidad de adoptar medidas para proteger su IP del conocimiento de terceros, lo que –precisamente con base en el mismo argumento de la expectativa de privacidad– determinaría que la misma fuera un dato que el usuario pretende y desea mantener reservado respecto del

público conocimiento (lo que sucede, por ejemplo, en el caso de los servicios VPN[258]), a pesar del uso de un programa P2P.

Debe destacarse la distinción de este tratamiento respecto del que se hace del supuesto de obtención de los datos de titularidad de un dispositivo que fuese identificado mediante número IMEI[259]. Como veremos, en este último supuesto no sería preciso autorización judicial para que los prestadores de servicios facilitaran dicha información a la policía[260]. No obstante, para lo que en todo caso no es necesaria autorización judicial es para la obtención de una dirección IP.

Se hace necesario recordar que, de conformidad con el artículo 22.2 LO 15/1999, "La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad*"*.

Esa disposición ha mantenido su vigencia con la entrada en vigor de la nueva LO 3/2018, en cuanto que su D.T. 4ª establece específicamente que *«Los tratamientos sometidos a 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, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva.»*

[258] Tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que el ordenador en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada, con toda la funcionalidad, seguridad y políticas de gestión de una red privada.
[259] El IMSI, por su parte, sirve para identificar al usuario de dicho dispositivo.
[260] –elemento este no exento de controversia, por otro lado–

Lo que resulta claro es que la policía puede obtener la dirección IP de un sistema informático sin necesidad de previa autorización judicial, sea mediante actividad de *ciberpatrullaje* o por cualquier otro medio. Sí será necesaria la intervención judicial en el momento de requerir a los obligados por el deber de colaboración para que cedan los datos que permitan localizar al terminal y determinar al usuario al que fue asignada dicha dirección. Ahora bien, si la Policía Judicial no puede obtener la dirección IP por sí misma, deberá recabar autorización judicial para acceder a los datos que se hubieran conservado con sometimiento al régimen de la Ley 25/2007, toda vez que el artículo 3 de la referida ley obliga a conservar dicho dato.

Abundando en esta línea, interesa mencionar la STEDH de 24 de abril de 2018 (caso *Benedik c. Eslovenia*), en la que el tribunal concluyó, en un supuesto de requerimiento dirigido directamente por la policía al ISP, sin contar con autorización judicial, para que proporcionara datos suficientes para identificar al usuario al que se había atribuido la dirección de una IP dinámica en un determinado momento, que la expectativa de privacidad del investigado respecto a su actividad online no puede considerarse injustificada o irrazonable, considerando que la privacidad de la actividad online queda protegida por el concepto de vida privada del artículo 8 CEDH, que solamente puede ser restringido de conformidad con el principio de legalidad invocado en el artículo 8.2 CEDH, por lo que, al carecer la legislación eslovena de normativa específica habilitante de dicha capacidad investigadora, provoca que la ley sobre la que se basa la medida controvertida, es decir la obtención por parte de la policía de información de abonado asociada a la dirección IP dinámica en cuestión, y la forma en que fue aplicada por los tribunales nacionales, carecía de claridad y no ofrecía suficientes salvaguardas contra la injerencia arbitraria en los derechos del artículo 8.

En todo caso, la obtención de la dirección IP por la Policía Judicial no está prevista en el ordenamiento jurídico más allá de este artículo 588 *ter* k LECrim que, como hemos visto, lo refiere únicamente de manera indirecta.

D. UTILIDAD DE LA DIRECCIÓN IP EN UNA INVESTIGACIÓN

La dirección IP permite identificar al dispositivo electrónico que establece la conexión a través de la entidad prestadora de servicios (ISP). De esta manera, en el proceso de averiguación de un determinado hecho delictivo, lo que permite la IP es determinar el dispositivo desde el que se produjo la conexión y, previa autorización judicial, la persona

titular de la relación contractual que ha dado lugar a la asignación de dicha dirección IP, pero nada más.

En ese sentido, tal averiguación no permite acreditar la persona que estaba utilizando el dispositivo electrónico en el momento del hecho delictivo, que podría haber sido cometido por cualquier sujeto distinto del usuario que conste en los archivos del ISP, que podría haber utilizado el dispositivo sin consentimiento del titular mediante un acceso no autorizado por vía física o, incluso, telemática. Como declara la STS 8316/2012, de 3 de diciembre, el hecho de que una persona sea titular de una línea con una concreta dirección IP desde la que se ha cometido un delito no es un dato suficiente para culpabilizar al titular de la línea de la comisión del delito, ante la inexistencia de otras pruebas[261].

En suma, la problemática que surge en relación a las averiguaciones de IP es que no siempre quien aparece formalmente como titular de la línea a la que se asigna dicha IP va a ser el autor material de la actividad ilícita investigada. En consecuencia, las medidas de investigación tecnológica tienen que complementarse con otras más tradicionales y, en general, las posibilidades de autoencubrimiento y ocultación son muy numerosas. Es por ello que la investigación relativa a la dirección IP debe rodearse de otras fuentes de prueba, obtenidas tanto de forma tradicional (seguimientos, registros, etc.) como virtuales (*ciberpatrullaje*, intervención de comunicaciones, etc.) que permitan imputar los hechos investigados a una persona concreta[262].

Además de la necesidad de practicar diligencias de investigación complementarias, la investigación a través de la dirección IP se encuentra con otras dificultades propias de la técnica, y que perjudican directamente a la construcción indiciaria, entre otras, las siguientes[263]: i) la atribución de direcciones IP dinámicas, que provoca que la dirección IP asignada por el proveedor de acceso a internet al equipo conectado varíe con cada sesión, por lo que la averiguación debe dirigirse no sólo a la identificación de un equipo concreto, sino de un equipo concreto en un momento determinado; ii) el uso de servidores proxy, que permiten a varios equipos utilizar la misma dirección IP; iii) las conexiones WiFi con pobres configuraciones de seguridad, que permiten ser utilizadas por usuarios terceros sin consentimiento del titular; iv) los propios establecimientos cibercafés o

---

[261] QUEVEDO GONZÁLEZ, J., *Investigación y prueba del ciberdelito*, cit., p. 136.
[262] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 457.
[263] DELGADO MARTÍN, J., "La prueba digital. Concepto, clases, aportación al proceso y valoración", cit., p. 457.

similares, que carecen de debido control sobre la persona que utiliza cada equipo en un momento determinado, pues la IP permitirá tan sólo identificar al negocio; y v) la tecnología NAT, que permite que una misma dirección IP sea utilizada por multitud de equipos que formen parte de una red local, y que prolifera debido a que ninguna normativa obliga a las operadoras a registrar los puertos que acceden a internet en cada momento, ni tampoco son datos que queden conservados en el *router*.

En cualquier caso, conocer la IP utilizada por los equipos informáticos no solo puede ser por sí mismo un elemento fundamental dentro de toda investigación referida al *ciberespacio* sino que, también, es un dato previo que ha de conocerse para poder requerir a la empresa de telecomunicaciones –previa autorización judicial– que reporte los datos de abonado correspondientes a la misma, de donde puede resultar la mayor parte de la utilidad de esta capacidad autónoma de investigación policial[264].

E. MODALIDADES DE OBTENCIÓN DE LA IP

La dirección IP puede obtenerse de diferentes modos: a través de la actividad de ciberpatrullaje, a través de la víctima, en supuestos de hallazgos casuales, en supuestos de urgencia, mediante cesión previa autorización judicial y mediante cesión voluntaria.

En cuanto a la obtención mediante fuentes abiertas, lo cierto es que, como se ha visto, las Fuerzas y Cuerpos de Seguridad del Estado desarrollan continuamente rastreos y sondeos en el *ciberespacio* público, todo ello en cumplimiento de sus funciones de prevención e investigación de los delitos.

En el rastreo de estas *"fuentes abiertas"* o ámbito público de internet, la policía puede hallar direcciones IP públicamente registradas en conexiones que puedan tener contenido delictivo. Ya nos hemos referido en el capítulo anterior a esta cuestión, por lo que ahora nos limitamos a exponer el razonamiento de la STS 842/2010, de 7 de octubre, por lo ilustrativo que resulta, cuando indica que *"*los rastreos que realizan en estos casos los agentes policiales tienen por objeto desenmascarar la identidad críptica de los IP que habían accedido a los hush que contenían pornografía infantil. El acceso a dicha información calificada por el recurrente de ilegítima o irregular, puede efectuarla cualquier usuario. No se precisa de autorización judicial para conseguir lo que es público y el propio

[264] CALVO LÓPEZ, D., "Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (apartados K) a M) del art. 588 ter de la LECrim)", cit., p. 12.

usuario de la red es quien lo ha introducido en la misma […] quien utiliza un programa P2P asume que muchos de los datos que él mismo incorpora a la red con su actividad se convierten en públicos para los usuarios de Internet, circunstancia que conocen o deben conocer los internautas, y tales datos conocidos por la policía no se hallaban protegidos por el artículo 18.1 ni por el 18.3 CE.*"*

Una vez obtenida la dirección IP, bastaría con acudir a las bases de datos *WhoIs* para conocer el ISP que habría asignado dicha dirección IP y, con ello, ya podría solicitarse la autorización judicial para que se requiriera al ISP para que aportara los datos del usuario al que correspondiera dicha dirección IP. Merece la pena destacar que las bases de datos *WhoIs* también están disponibles para el público[265].

En otras ocasiones, es la propia víctima del delito la que aporta la dirección IP del dispositivo utilizado para la comisión del hecho delictivo. La doctrina refiere, por ejemplo, el supuesto de correos electrónicos de extorsión que incorporan la dirección IP del remitente.[266] En definitiva, es un caso de acceso por una persona distinta del emisor de la conexión al dato de la dirección IP, que se encuentra públicamente disponible en el *ciberespacio*.

En tal sentido, la Fiscalía General del Estado ya afirmaba en su Circular 1/2013[267] que la garantía del secreto de las comunicaciones sólo opera cuando la injerencia es realizada por una persona ajena al proceso de comunicación, ya que lo que persigue la norma es garantizar la impenetrabilidad de la comunicación por terceros ajenos a la misma. Del mismo modo, la STC núm. 56/2003, de 24 de marzo, concluía que no existe prohibición para conocer, por parte de uno de los interlocutores, el número de teléfono desde el que se establece comunicación con él; en otro caso, todos los teléfonos que muestran el número desde el que están siendo llamados infringirían el secreto de las comunicaciones amparado por el artículo 18.3 CE.

Lo fundamental es, a fin de cuentas, que se trataría de una información pública introducida en el espacio público del *ciberespacio* por la persona que cometió el delito, que la víctima únicamente pone a disposición de la autoridad correspondiente en el

---

[265] *Ibid.*, p. 15.
[266] *Ibid.*
[267] "BOE.es – Documento FIS–C–2013–00001", fecha de consulta 15 abril 2020, en https://www.boe.es/buscar/doc.php?coleccion=fiscalia&id=FIS–C–2013–00001&tn=2.

momento de formular su denuncia y, por tanto, respecto del que la persona investigada no podrá alegar después una expectativa razonable de privacidad.

En otros casos ocasiones, la policía conoce una dirección IP no a través de fuentes abiertas, sino como consecuencia de un hallazgo casual. Llegados a este punto, interesa traer a colación la ya clásica STS 786/2015, que concluye que *"*no puede obtener el mismo tratamiento jurídico la accidental apertura de un sobre introducido por error en un buzón que no es el de su destinatario –equivocación que permite el descubrimiento de un hecho de relieve penal–, frente a la fractura intencionada del buzón de un vecino con la finalidad de acceder a su correspondencia y vulnerar así su intimidad*."* En consecuencia, debe tenerse presente la imposibilidad de acudir a la figura del hallazgo casual para intentar solventar posibles dudas de ilicitud que puedan surgir en la práctica de las diligencias policiales oportunas.

En cuanto a los supuestos de urgencia, en el apartado tercero del artículo 588 *ter* d) LECrim se prevé la posibilidad de efectuar interceptación de comunicaciones telefónicas y telemáticas en los supuestos de delitos de terrorismo o en los que intervengan bandas armadas, previa orden del Ministro del Interior y posterior comunicación al juez en el plazo de 24 horas como máximo.

Por otro lado, debemos señalar que la alternativa más plausible en la práctica, cuando la policía no puede obtenerla a través del *ciberpatrullaje*, es la obtención mediante autorización judicial. En la medida en que es uno de los datos que los ISP están obligados a conservar, de conformidad con el artículo 3 de la Ley 25/2007, basta con obtener la autorización judicial prevista en el artículo 6 de la referida ley. La necesidad de obtener previa autorización judicial para que el ISP remita la información de identificación del cliente al que esté asignada la dirección IP en cuestión viene establecida no sólo en la Ley 25/2007, sino también en el artículo 588 *ter* k LECrim incorporado con la nueva LO 13/2015, que sigue la línea de las SSTS 292/2008, de 28 de mayo, 236/2008, de 9 de mayo y 680/2010, de 14 de julio.

Por último, ha de plantearse, igualmente, la hipótesis de la cesión voluntaria del dato de la dirección IP por parte del ISP. Nos referimos, así, a los casos en que se facilita la IP asociada a la conducta investigada sin que haya existido requerimiento al efecto y sin, en consecuencia, recabar la autorización judicial previa. Interesa destacar la

controversia que surge a este respecto, pues en ocasiones se entiende[268] que dicha obtención contravendría lo dispuesto en el artículo 588 *ter* k LECrim y en el artículo 6 de la Ley 25/2007, por lo que sería necesario no utilizar dicha dirección IP, o de lo contrario se correría el riesgo de viciar de nulidad el procedimiento. Entre los argumentos que se aportan para mantener esa postura, se indican i) la redacción de los propios artículos citados; ii) el principio existente en la normativa comunitaria y nacional de que los datos de tráfico estén protegidos; iii) la inexistencia de consentimiento del interesado para que el dato sea tratado de esa manera, al margen de que no constituya un dato de carácter personal; y iv) la inexistencia de razones de urgencia, con carácter general.

A nuestro juicio, resulta especialmente relevante establecer los mecanismos que sean necesarios para garantizar que la colaboración extrajudicial entre los ISP y demás proveedores de servicios relativos al ciberespacio, por un lado, y las Fuerzas y Cuerpos de Seguridad, por otro, no se constituya en una práctica común o cotidiana, a fin de garantizar la vigencia efectiva de los derechos fundamentales recogidos en el artículo 18 CE.

7. OBTENCIÓN DE IMÁGENES PÚBLICAS EN EJERCICIO DE FUNCIONES DE PREVENCIÓN DEL DELITO

A. RÉGIMEN JURÍDICO

La LO 4/2015 regula el uso de las videocámaras al establecer en su artículo 22 que "La autoridad gubernativa y, en su caso, las Fuerzas y Cuerpos de Seguridad podrán proceder a la grabación de personas, lugares u objetos mediante cámaras de videovigilancia fijas o móviles legalmente autorizadas, de acuerdo con la legislación vigente en la materia".

La regulación a la que hace referencia es la incorporada en la Ley Orgánica 4/1997, de 4 de agosto, en la que se contempla la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

A este respecto, debemos destacar las siguientes reglas[269]:

---

[268] CALVO LÓPEZ, D., "Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (apartados K) a M) del art. 588 ter de la LECrim)", cit., p. 18.
[269] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 494.

El artículo 1.2 contiene una cláusula abierta a nuevos elementos tecnológicos, cuando indica que "2. Las referencias contenidas en esta Ley a videocámaras, cámaras fijas y cámaras móviles se entenderán hechas a cualquier medio técnico análogo y, en general, a cualquier sistema que permita las grabaciones previstas en esta Ley".

Su objeto queda delimitado en el artículo 1.1, que regula "la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública".

Se prevé un régimen específico de autorización de cámaras fijas en su artículo 3, según el cual "La instalación de videocámaras o de cualquier medio técnico análogo en los términos del artículo 1.2 de la presente Ley está sujeta al régimen de autorización, que se otorgará, en su caso, previo informe de un órgano colegiado presidido por un Magistrado y en cuya composición no serán mayoría los miembros dependientes de la Administración autorizante"

Las cámaras móviles, conforme al artículo 5, podrán utilizarse en los lugares donde se hayan autorizado las fijas, así como en otros lugares previa autorización del máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad, debiendo dar traslado de dicha resolución a la misma comisión que autoriza el uso de las fijas en el plazo de 72 horas. Destaca que, en casos excepcionales de urgencia máxima o de imposibilidad de obtener a tiempo la autorización indicada en razón del momento de producción de los hechos o de las circunstancias concurrentes, se podrán obtener imágenes y sonidos con videocámaras móviles, dando cuenta, en el plazo de setenta y dos horas, mediante un informe motivado, al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad y a la Comisión, debiendo proceder a la destrucción de las grabaciones si las mismas no resultaran autorizadas.

En cuanto a su incorporación al proceso penal, el artículo 7.1 determina que "realizada la filmación de acuerdo con los requisitos establecidos en la Ley, si la grabación captara la comisión de hechos que pudieran ser constitutivos de ilícitos penales, las Fuerzas y Cuerpos de Seguridad pondrán la cinta o soporte original de las imágenes y sonidos en su integridad a disposición judicial con la mayor inmediatez posible y, en todo caso,

en el plazo máximo de setenta y dos horas desde su grabación. De no poder redactarse el atestado en tal plazo, se relatarán verbalmente los hechos a la autoridad judicial, o al Ministerio Fiscal, junto con la entrega de la grabación"[270].

Ese régimen jurídico se completa con el artículo 588 *quinquies* a) LECrim, que establece que "La Policía Judicial podrá obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos".

B. RÉGIMEN EN LA LEY ORGÁNICA 7/2021

Posteriormente, y en materia de obtención de imágenes públicas en ejercicio de funciones de prevención del delito, dicho régimen jurídico ha quedado completado con la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Dicha Ley Orgánica tiene por objeto establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública. Hay que recordar, a este respecto, que la imagen facial constituye un dato personal conforme al artículo 4.1 RGPD y, una vez es sometida a un tratamiento técnico, pasa a tener la consideración de dato biométrico del artículo 4.4 RGPD, por lo que la Ley Orgánica en cuestión persigue, en definitiva, cumplir con la normativa en materia de protección de datos, carencia esta que ya fue denunciada por la doctrina[271].

Resultan especialmente interesantes los artículos 15 y siguientes, relativos al tratamiento de datos personales en el ámbito de la videovigilancia por Fuerzas y Cuerpos de Seguridad, que ayudan a dibujar la silueta de dicha actividad policial.

---

[270] *Ibid.*, p. 473.

[271] ETXEBERRIA GURIDI, J. F., "Inteligencia Artificial aplicada a la videovigilancia: tecnologías de reconocimiento facial", en *Justicia algorítmica y neuroderecho: una mirada multidisciplinar, 2021, pp. 443–467*, Tirant lo Blanch, 2021, p. 449, fecha de consulta 30 noviembre 2021, en https://dialnet.unirioja.es/servlet/articulo?codigo=8102538.

De conformidad con el apartado primero artículo 15, la captación, reproducción y tratamiento de datos personales por las Fuerzas y Cuerpos de Seguridad en los términos previstos en esta Ley Orgánica, así como las actividades preparatorias, no se considerarán intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Llama la atención que este precepto haga referencia al artículo 2.2 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, que a su vez dispone la imposibilidad de apreciar intromisión ilegítima cuando el titular del derecho hubiera otorgado al efecto su consentimiento expreso. También es de destacar que la Ley Orgánica 7/2021 no contenga una definición del concepto de "actividades preparatorias".

En cuanto a los criterios a tener en cuenta en el momento de instalar sistemas de grabación de imágenes y sonidos, el artículo 15.2 señala, conforme al principio de proporcionalidad, los siguientes criterios: asegurar la protección de los edificios e instalaciones propias; asegurar la protección de edificios e instalaciones públicas y de sus accesos que estén bajo custodia; salvaguardar y proteger las instalaciones útiles para la seguridad nacional y prevenir, detectar o investigar la comisión de infracciones penales y la protección y prevención frente a las amenazas contra la seguridad pública.

La instalación de sistemas fijos también queda prevista en la Ley Orgánica que analizamos, y a tal efecto el artículo 16 prevé que en las vías o lugares públicos puedan instalarse videocámaras fijas previa valoración del principio de proporcionalidad, junto con un un análisis de los riesgos o una evaluación de impacto de protección de datos relativo al tratamiento que se pretenda realizar, en función del nivel de perjuicio que se pueda derivar para la ciudadanía y de la finalidad perseguida. En el precepto se define el concepto de videocámara fija como un análisis de los riesgos o una evaluación de impacto de protección de datos relativo al tratamiento que se pretenda realizar, en función del nivel de perjuicio que se pueda derivar para la ciudadanía y de la finalidad perseguida, y se prevé expresamente que los ciudadanos serán informados de manera clara y permanente de la existencia de estas videocámaras fijas, sin especificar su emplazamiento.

C. TÉCNICAS DE RECONOCIMIENTO FACIAL

Los sistemas de reconocimiento facial intentan identificar o verificar la identidad de las personas en función de su rostro. Diferentes sistemas analizan las características del rostro en fotos o vídeos almacenados en bases de datos, o a través de la vigilancia en

tiempo real. De conformidad con el Dictamen 2/2012 del GT29, el reconocimiento facial puede describirse como aquel "tratamiento automático de imágenes digitales que contienen las caras de personas con fines de identificación, autenticación/verificación o categorización de dichaspersonas".

La tecnología de reconocimiento facial funciona en cuatro fases diferenciadas: i) detección del rostro de la persona que se va a identificar; ii) extracción de las características faciales que conforman el denominado patrón biométrico facial; iii) cotejo del patrón biométrico facial obtenido con la existente en bases de datos, obteniendo un porcentaje de similitud; y iv) toma de decisión automatizada conforme al porcentaje de solicitud obtenido. En el Dictamen 2/2012 del GT29 dichos pasos se dividen en los siguientes: a) obtención de la imagen; b) detección dela cara; c) normalización; d) extracción de características; e) registro; f) comparación.

Se distinguen diferentes modalidades de reconocimiento facial[272]:

a) Medio de autenticación o verificación: se comparan dos plantillas biométricas pertenecientes a la misma persona para determinar si la persona que aparece en ambas es la misma. Generalmente, una de las plantillas o modelos se encuentra almacenada con antelación a la comprobación, pero no siempre es necesario que sea así, como en los casos en que dichas características biométricas se incorporen a documentos de identidad, pasaportes, etc.[273] Es la técnica empleada, por ejemplo, para desbloquear terminales particulares.

b) Medio de identificación: se compara la plantilla biométrica obtenida con plantillas almacenadas previamente en uno o varios ficheros que corresponden a personas diferentes. Como consecuencia, el resultado se emite con un porcentaje de acierto. Es posible que en dichas bases de datos se encuentre la plantilla biométrica de la persona a identificar (*closed–set identification*), o que no sea así o se desconozca tal circunstancia (*open–set identification*). Esta técnica viene siendo empleada con fines policiales, empleando para ello bases de datos de personas buscadas o sospechosas y cámaras de vigilancia pública. Como se podrá suponer, el porcentaje de falsos positivos es una de sus

[272] *Ibid.*, p. 451.
[273] "Facial recognition technology: fundamental rights considerations in the context of law enforcement", *European Union Agency for Fundamental Rights*, 2019, fecha de consulta 30 noviembre 2021, en https://fra.europa.eu/en/publication/2019/facial–recognition–technology–fundamental–rights–considerations–context–law.

grandes críticas (debido, entre otras causas, a la calidad de las imágenes obtenidas), así como la posible discriminación y vulneración de garantías en que se pueda incurrir al introducir a determinados individuos en dichas bases de datos.

c) Medio de categorización: la tecnología de reconocimiento facial se emplea para obtener características de un individuo con el fin de categorizarlo y asignarlo a un grupo con particularidades concretas (grupo étnico, edad, sexo, etc.)

El reconocimiento facial es una herramienta que puede revestir gran utilidad para nuestra sociedad, considerado de forma separada. Así, en los trámites aeroportuarios puede incrementar la agilidad de los trámites de llegada o salida, al sustituir la comprobación documental manual con verificaciones automáticas; en cuestiones sanitarias, pueden controlar la extensión de pandemias y diagnosticar con mayor precisión enfermedades; a las personas con capacidad visual reducida, puede reportarles información importante sobre escenas; en conducción y transporte, incrementará la seguridad de las vías públicas y carreteras al detectar el cansancio o las distracciones en los conductores; en las transacciones, puede permitir que se implemente el pago a través de la cara, del mismo modo que sucede ahora con la huella dactilar (aunque tendría que implementarse de un modo que permitiera descartar posibles consentimientos erróneos); en materia de seguridad personal, puede constituir una clave de bloqueo que impida el acceso al dispositivo, e incluso de cifrado. Igualmente, la relevancia y utilidad de dicha tecnología también se manifiesta en el ámbito de la investigación policial, a través de la sincronización con bases de datos policiales, permitiendo tanto la rápida verificación de la identidad de sospechosos como la alerta automática en vídeos grabados públicamente.

La importancia de esta tecnología ya fue advertida por el actual Comité Europeo de Protección de Datos, antiguo Grupo de Trabajo del Artículo 29, en su dictamen 3/2012 acerca del reconocimiento facial en los servicios en línea y móviles: el seguimiento, localización o establecimiento del perfil automatizados de las personas y, como tal, sus efectos potenciales sobre la intimidad y el derecho a la protección de datos personales son importantes[274].

Las tecnologías de reconocimiento facial plantean problemas en relación con la raza, género y edad, habiéndose demostrado que funciona defectuosamente al analizar los

[274] "Dictamen 3/2012 sobre la evolución de las tecnologías biométricas", fecha de consulta 3 mayo 2020, en https://www.aepd.es/sites/default/files/2019–12/wp193_es.pdf.

rostros de las mujeres, los niños y las personas con tonos de piel más oscuros[275]. También perjudican el derecho al derecho a la libertad de expresión y manifestación, al exponer a los integrantes de manifestaciones a vigilancia e identificación persistentes. Adicionalmente, supone crear el riesgo del uso indebido de los datos generados, además de poder generar errores y casos de falsos positivos. [276]

Igualmente, afecta de manera general a la privacidad de las personas. El rostro tiene la condición de dato personal conforme al artículo 4 RGPD y, además, tiene la consideración de dato biométrico, pues es un dato personal obtenido a partir de un tratamiento técnico específico, relativo a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos. En tanto dato biométrico, se encuentra especialmente protegido y equiparado en su régimen a los de salud, ideología, creencias religiosas, etc. Estos datos merecen una especial defensa por tener una relación muy sensible con los derechos y libertades fundamentales, y el artículo 9 RGPD prohíbe su tratamiento salvo en alguno de los supuestos del artículo 9.2: consentimiento explícito del interesado, cumplimiento de obligaciones y derechos del responsable del tratamiento o del interesado, protección de intereses vitales, tratamiento por fundaciones o asociaciones sin ánimo de lucro –respecto de los miembros de dichos organismos–, tratamientos de datos personales hechos públicos por el interesado –atención a las aplicaciones que simulan el envejecimiento de las personas[277]–, interés público esencial o salud pública, medicina preventiva o laboral, investigación científica, histórica o estadística, y ejercicio del derecho de defensa ante los tribunales.

Sobre ese escenario, la problemática principal del reconocimiento facial es que el rostro, en cuanto dato biométrico, puede recolectarse de manera automatizada y sin consentimiento del titular –hasta qué punto, en una interpretación torticera, no podría entenderse que con nuestra mera existencia hacemos pública nuestra cara–. China, por ejemplo,

---

[275] HAMED ABDURRAHIM, S.; SAMAD, S. A.; HUDDIN, A. B., "Review on the effects of age, gender, and race demographics on automatic face recognition", *The Visual Computer*, vol. 34, 11, 2018.

[276] "La doble cara del reconocimiento facial: entre las ventajas de su uso y el impacto en nuestra privacidad", fecha de consulta 3 mayo 2020, en http://www.legaltoday.com/blogs/nuevas–tecnologias/blog–prodat/la–doble–cara–del–reconocimiento–facial–entre–las–ventajas–de–su–uso–y–el–impacto–en–nuestra–privacidad.

[277] "Privacy Policy – FaceApp", fecha de consulta 5 mayo 2020, en https://www.faceapp.com/privacy–en.html.

ha adoptado sin tapujos las bondades de dicha tecnología, y Estados Unidos y la India también están integrando sus funciones, además de otros muchos países.[278]

Destaca, entre otras, la aplicación *Clearview AI*, que utiliza las fotografías colgadas en Facebook, Instagram, YouTube y demás redes y webs para identificar a las personas[279]. Los detalles de la aplicación han generado alarma en EEUU, ya que hasta ahora la policía contaba con sistemas de reconocimiento facial, pero limitados a buscar en fotografías de detenidos en poder de las autoridades. Clearview les permite buscar en los miles de millones de imágenes que circulan por la red. Con independencia de que ello vulnera el derecho a la privacidad, lo cierto es que también aumenta significativamente la posibilidad de una identificación errónea.

En San Francisco[280] ha sido prohibido el uso de sistemas de reconocimiento facial por la policía y otras administraciones locales, como elemento de un conjunto de medidas destinadas a regular la adopción de tecnología de cibervigilancia por la administración local[281].

En la Unión Europea, de momento, se plantea la posibilidad de demorar su admisión por un plazo de cinco años[282], reconociéndose siete elementos necesarios para su establecimiento con garantías: acción y supervisión humana, gestión de la privacidad y de los datos, transparencia, diversidad, no discriminación y equidad, bienestar social y medioambiental, y rendición de cuentas[283]. Asimismo, el Parlamento Europeo, en su Resolución de 6 de octubre de 2021 (2020/2016(INI)), ha expresado su gran preocupación por el uso por parte de las fuerzas del orden y los servicios de inteligencia de bases de datos de reconocimiento facial privadas, como Clearview AI y ha pedido a los Estados miembros que obliguen a los agentes de garantía del cumplimiento de la ley a revelar si están utilizando la tecnología Clearview AI o tecnologías equivalentes de otros

---

[278] "AI Global Surveillance (AIGS) Index".
[279] HILL, K., "The Secretive Company That Might End Privacy as We Know It", *The New York Times*, 2020, fecha de consulta 3 mayo 2020, en https://www.nytimes.com/2020/01/18/technology/clearview–privacy–facial–recognition.html.
[280] RUBIO, I., "Reconocimiento facial: la tecnología que lo sabe todo", *El País*, 2019, Madrid, fecha de consulta 4 mayo 2020, en https://elpais.com/tecnologia/2019/05/21/actualidad/1558455279_966010.html.
[281] HAR, J., "San Francisco becomes the first US city to ban the use of facial recognition software by police", *Business Insider*, fecha de consulta 3 mayo 2020, en https://www.businessinsider.com/san–francisco–bans–facial–recognition–software–by–police–2019–5.
[282] VEGA, G., "La UE plantea prohibir hasta cinco años el reconocimiento facial en lugares públicos", *El País*, 2020, Madrid.
[283] "Libro blanco sobre la inteligencia artificial", 2020, fecha de consulta 5 mayo 2020, en https://ec.europa.eu/info/sites/info/files/commission–white–paper–artificial–intelligence–feb2020_es.pdf.

proveedores, recordando que el uso de un servicio como Clearview AI por parte de las autoridades policiales en la Unión probablemente no sería compatible con el régimen de protección de datos de la Unión.

Alemania lo prohíbe para su policía y Francia veda su uso en las instituciones educativas, mientras ciudades como Londres, han iniciado el camino contrario. En concreto, la Policía Metropolitana londinense anunció a principios de año que la tecnología de reconocimiento facial en las calles ha superado la etapa de prueba previa y está lista para integrarse permanentemente en la vigilancia diaria de la ciudad.[284]

Mientras, en España se adoptan estrategias de dudosa legitimidad para sortear la prohibición de utilización. Así sucede con el sistema implantado en Marbella, que a través del software Avigilon[285] consigue identificar a ciudadanos a través del resto de sus características físicas, excluyendo el rostro. Como venimos destacando a lo largo de esta investigación, el *hardware* instalado permite un alcance mucho mayor –identificar las caras de las personas– al uso que se le está dando[286].

La controversia generada por los sistemas de reconocimiento facial ha provocado respuestas en la ciudadanía. Entre ellas, se cuenta el proyecto *Where are the eyes,* que es una iniciativa colectiva para detectar y mapear cámaras de vigilancia por parte de los ciudadanos[287].

Asimismo, los sistemas descritos analizan las imágenes de las cámaras de vigilancia e intentan aislar a personas y objetos dentro del vídeo. Los análisis de vídeo utilizan algoritmos para detectar artículos particulares de ropa y equipaje. Ciertas versiones

[284] "Así funciona el reconocimiento facial y por qué debería preocuparte", *ELMUNDO*, 2020, fecha de consulta 3 mayo 2020, en https://www.elmundo.es/tecnologia/2020/02/24/5e4fb4c3fc6c83821f8b4642.html.
[285] "Facial Recognition » Avigilon", 2020, fecha de consulta 3 mayo 2020, en https://www.avigilon.com/products/ai–video–analytics/facial–recognition.
[286] PÉREZ COLOMÉ, J., "Marbella, el mayor laboratorio de videovigilancia de España", *El País*, 2019, Madrid, fecha de consulta 3 mayo 2020, en https://elpais.com/tecnologia/2019/11/21/actualidad/1574348695_231540.html.
[287] "Where are the Eyes?", fecha de consulta 3 mayo 2020, en https://eyes.daylightingsociety.org/.

afirman que pueden encontrar personas en imágenes de vigilancia que coinciden con un color de cabello particular, vello facial e, incluso, tono de piel[288].

Debe reconocerse que estas técnicas plantean problemas en materia de falsos positivos, pues la información de los análisis de vídeo puede ser incorrecta y provocar actuaciones policiales innecesarias. Se afecta, igualmente, a la libertad de expresión y manifestación, pues exponen a los ciudadanos a una vigilancia persistente mientras se mueven por espacios públicos. Al dirigirse a personas en función del origen racial percibido, puede ocasionar problemas de discriminación. Por último, al someter a las personas a vigilancia persistente es evidente que se están excediendo los posibles límites que se hayan autoimpuesto los particulares por aplicación de la expectativa de privacidad.[289]

D. EMPLEO DE DRONES CON INTELIGENCIA ARTIFICIAL

Los drones continúan mejorando su abanico de prestaciones y con ello cada vez se expanden más hacia otros usos, entre los que se encuentra el de prevención e investigación policial.

En Estados Unidos han empezado a usar drones con inteligencia artificial, capaces de esquivar, volar, volver a base y tomar fotografías de manera autónoma, en una iniciativa conocida como *Drone as First Responder*[290].

La capacidad de tener cierta autonomía de los drones policiales despierta cierta inquietud. Las dudas, naturalmente, surgen en cuanto a la privacidad y al hecho de que los drones puedan seguir a ciudadanos por sí solos, incrementándose así la posibilidad de que se esté grabando y vigilando el día a día de mucha gente (sin motivo) y la posibilidad de que pueda haber "falsos positivos" de delitos si falla supervisión humana durante alguno de los vuelos[291].

---

[288] STANLEY, JAY, "The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy", 2019, fecha de consulta 4 mayo 2020, en https://www.aclu.org/sites/default/files/field_document/061119–robot_surveillance.pdf.

[289] "Static camera analytic profiles", 2014, fecha de consulta 4 mayo 2020, en www.ibm.com/support/knowledgecenter/en/ss88xh_2.0.0/iva/ref_analyticp.html.

[290] "UAS Drone Program | City of Chula Vista", fecha de consulta 21 julio 2021, en https://www.chulavistaca.gov/departments/police–department/programs/uas–drone–program.

[291] RICE, S., "Eyes In The Sky: The Public Has Privacy Concerns About Drones", *Forbes*, fecha de consulta 5 mayo 2020, en https://www.forbes.com/sites/stephenrice1/2019/02/04/eyes–in–the–sky–the–public–has–privacy–concerns–about–drones/.

La doctrina[292] ha entendido incluido en el artículo 588 *quinquies* a) LECrim, al permitir a la policía la captación de imágenes en lugares o espacios públicos "por cualquier medio técnico", la posibilidad de realizar dichas grabaciones mediante el empleo de drones.

El artículo 17 de la Ley Orgánica 7/2021 se refiere a la posibilidad de utilizar dispositivos de toma de imágenes y sonido de carácter móvil para el mejor cumplimiento de los fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

Ahora bien, la toma de imagen y sonido, que ha de ser conjunta, queda supeditada, en todo caso, a la concurrencia de un peligro o evento concreto. El uso de los dispositivos móviles deberá estar autorizado por la persona titular de la Delegación o Subdelegación del Gobierno, quien atenderá a la naturaleza de los eventuales hechos susceptibles de filmación, adecuando la utilización de dichos dispositivos a los principios de tratamiento y al de proporcionalidad. Las autorizaciones no se podrán conceder en ningún caso con carácter indefinido o permanente, siendo otorgadas por el plazo adecuado a la naturaleza y las circunstancias derivadas del peligro o evento concreto, por un periodo máximo de un mes prorrogable por otro.

Como excepción, en casos de urgencia o necesidad inaplazable será el responsable operativo de las Fuerzas y Cuerpos de Seguridad competentes el que podrá determinar su uso, siendo comunicada tal actuación con la mayor brevedad posible, y siempre en el plazo de 24 horas, al Delegado o Subdelegado del Gobierno o autoridad competente de las comunidades autónomas.

8. POLICÍA PREDICTIVA E INTELIGENCIA ARTIFICIAL

A. PRÁCTICA DE LA INTELIGENCIA ARTIFICIAL

La inteligencia artificial, como nueva tecnología, se está incorporando de manera progresiva a los flujos de trabajo de la policía, basada en el acceso y tratamiento a

[292] BUENO DE MATA, F., "Peculiaridades probatorias del dron como diligencia de investigación tecnológica", en *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas, 2018, pp. 169–204*, Tirant lo Blanch, 2018, p. 182, fecha de consulta 1 diciembre 2021, en https://dialnet.unirioja.es/servlet/articulo?codigo=7751711.

cantidades ingentes de datos, en lo que ha venido en denominarse como *big data policing*[293]. No en vano, se ha concluido que constituye una ayuda muy eficaz en la detección de actividades ilegales en materia financiera[294].

La información obtenida por la policía sirve también para alimentar programas de policía predictiva. Por un lado, están los programas que intentan predecir las tendencias criminales de las personas, como el programa *Compass*, y por el otro, los que pretenden elaborar mapas de potenciales áreas de tensión en las ciudades, donde las posibilidades de cometer un delito son estadísticamente mayores.

Por ello, se dice que generalmente este tipo de programas funcionan en relación a dos variables: las personas y los lugares. Los sistemas de policía predictiva orientados sobre lugares utilizan algoritmos para analizar conjuntos de datos con la intención de predecir los tipos de delitos que podrán cometerse en determinados lugares. Estas estimaciones son utilizadas posteriormente para decidir la distribución de agentes y operativos. Los sistemas de policía predictiva orientados sobre personas utilizan algoritmos para analizar conjuntos de datos que permitan construir listas de individuos que se consideren propensos a cometer algún delito.

Con estos instrumentos surgen alarmas respecto del riesgo de discriminación por razones de origen racial, siendo muy posible que provoquen un exceso de actividad policial en determinadas comunidades. Además de lo anterior, desnaturaliza el requisito de la especialidad en las investigaciones policiales, pues las sospechas basadas en extremos de hecho pasan a ser sustituidas por conclusiones obtenidas por la aplicación de un algoritmo cuyo funcionamiento no es público.

De hecho, el elevado impacto de estas medidas ha provocado que surjan demandas para conocer el funcionamiento de dichas herramientas[295]. Como consecuencia de ello,

---

[293] MERKEL, L., *Derechos humanos e investigaciones policiales*, Marcial Pons, Madrid, 2022, p. 288, fecha de consulta 16 junio 2022, .
[294] GARCÍA, J., "La inteligencia artificial se viste de policía para atrapar a los malos", *El País*, 2019, Madrid.
[295] DWYER, J., "Showing the Algorithms Behind New York City Services", *The New York Times*, 2017, fecha de consulta 4 mayo 2020, en https://www.nytimes.com/2017/08/24/nyregion/showing–the–algorithms–behind–new–york–city–services.html.

en ocasiones se ha resuelto ordenar a la policía publicar registros sobre las pruebas, desarrollo y utilización de las herramientas de policía predictiva[296].

En relación con el sistema *Compass*, puede señalarse el caso de Eric Loomis, que fue acusado y declarado culpable de participar en un tiroteo y, posteriormente, sometido a una evaluación algorítmica del riesgo de reincidencia a través del software *Compass*. El programa estimó un alto riesgo de reincidencia y, sobre esta base, se impuso una condena de 6 años de prisión, más 5 de libertad condicional. Loomis impugnó la sentencia, alegando que no había tenido la oportunidad de evaluar el funcionamiento del algoritmo que, por ser un secreto comercial, no es público. El tribunal, la corte de apelaciones y la Corte Suprema rechazaron su apelación. Aun así, alegaron que podía ser complicado para los jueces tomar decisiones sobre la base de una tecnología cuyo real funcionamiento era desconocido. El caso sentó un precedente importante en la jurisprudencia de Estados Unidos, además de poner de manifiesto las evidentes carencias del sistema en cuestión[297].

Encontramos también el ejemplo de *Predpol*, un software desarrollado por la Universidad de California–Los Ángeles y utilizado por más de 60 departamentos de Policía en los Estados Unidos, que parte de un historial de delitos pasados (entre dos y cinco años de datos), enriquecido a lo largo del tiempo. Con esta información, el algoritmo intenta predecir dónde y cuándo será más probable que ocurra un cierto tipo de crimen.[298] *PredPol* puede incluso indicar los perfiles de personas que más se corresponden a la identidad estadística del delincuente, así como mapear en tiempo real la criminalidad potencial de las ciudades. El área controlada por *PredPol* está divida en una cuadrícula, con celdas de 150 por 150 metros. Para cada celda es posible obtener la probabilidad de que un delito concreto ocurra en un período de tiempo determinado. Estas estimaciones deberían servir a las policías locales para optimizar la distribución de los efectivos y prevenir algunos tipos de crimen.

---

[296] "Court: Public Deserves to Know How NYPD Uses Predictive Policing Software", *Brennan Center for Justice*, fecha de consulta 4 mayo 2020, en https://www.brennancenter.org/our–work/analysis–opinion/court–public–deserves–know–how–nypd–uses–predictive–policing–software.

[297] Enumerados con precisión científica por NIEVA FENOLL, J., "Inteligencia artificial y proceso judicial: perspectivas tras un alto tecnológico en el camino.", *Revista General de Derecho Procesal*, 57, 2022, Iustel, p. 15. Entre ellos, se destaca la falta de transparencia en el modo en que el sistema valora los criterios de control, la clara tendencia racista del sistema y, en fin, la ausencia de fiabilidad en sus predicciones.

[298] "Law Enforcement | PredPol Law Enforcement Intelligence Led Policing Software | PredPol Law Enforcement Intelligence Led Policing Software", *PredPol*, fecha de consulta 21 julio 2021, en https://www.predpol.com/law–enforcement/.

De hecho, según varios estudios en materia de criminología ambiental[299], existen correlaciones entre la estructura del entorno urbano y la distribución de los delitos que, en parte, también responden al simple sentido común: es lógico que ciertos tipos de infracciones sean más frecuentes, por ejemplo, en áreas poco iluminadas o densamente pobladas[300].

Una de las principales críticas que se levantan contra este tipo de programas es que los datos en que suele basarse la vigilancia predictiva casi nunca son objetivos. Algunas áreas urbanas se caracterizan por una mayor cantidad de pequeños delitos simplemente porque han sido sometidas a un mayor control policial. Como en todas las aplicaciones del *machine learning*, un "prejuicio" inicial en los datos produce algoritmos ineficaces.

La asociación *Human Rights*[301], por ejemplo, sostiene que *PredPol* se centra casi solo en los barrios más pobres, discriminando a las comunidades afroamericana e hispana. De hecho, si un modelo predictivo enfocado en los delitos mayores con toda probabilidad produciría un mapa desordenado y completamente inútil, uno centrado en los delitos menores y el comportamiento antisocial compone un mapa que, inevitablemente, apunta a barrios específicos: aquellos más desfavorecidos y con menos recursos.

Una duda similar en cuanto a la objetividad del algoritmo ha sido planteada con respecto a los programas utilizados para la predicción de reincidencia. Por ejemplo, según un estudio de 2016[302], el software *Compass* parece tener prejuicios contra las minorías al haber etiquetado a las personas negras como posibles delincuentes reincidentes en el doble de casos que las blancas.

---

[299] "Criminología ambiental: breve historia de su evolución", *Cuadernos de Criminología*, 2017, fecha de consulta 11 noviembre 2021, en https://cuadernosdecriminologia.blogspot.com/2017/09/criminologia–ambiental–breve–historia.html.

[300] SAN JUAN GUILLÉN, C., "Criminología ambiental: un área en expansión", *Ars Iuris Salmanticensis: AIS : revista europea e iberoamericana de pensamiento y análisis de derecho, ciencia política y criminología*, vol. 1, 1, 2013, Ediciones Universidad de Salamanca, p. 15.

[301] "PredPol amplifies racially biased policing", *HRDAG – Human Rights Data Analysis Group*, fecha de consulta 21 julio 2021, en http://hrdag.org/pressroom/predpol–amplifies–racially–biased–policing/.

[302] LARSON MATTU, J.; OTROS, O.; OTROS, O., "How We Analyzed the COMPAS Recidivism Algorithm", *ProPublica*, fecha de consulta 21 julio 2021, en https://www.propublica.org/article/how–we–analyzed–the–compas–recidivism–algorithm?token=jRdnwabwdw5HLiHY–R3nqWS5DOjEM7W–.

Existen otros ejemplos, como el alemán *Precobs* o el italiano *XLAW*, mientras que la asociación Liberty ha denunciado[303] con preocupación el hecho de que al menos catorce fuerzas de policía británicas hayan utilizado programas predictivos. También en este caso se trata de dos tipos de enfoque: el mapeo y la evaluación del riesgo individual. En este segundo caso, el software utilizado en Gran Bretaña se llama Hart y fue desarrollado por la Universidad de Cambridge. También para Liberty el riesgo es que estas políticas acaben avalando estrategias discriminatorias.[304]

El entusiasmo generalizado por los algoritmos hace que algunos pretendan usar el aprendizaje automático para leer las caras de las personas y adivinar sus intenciones más secretas. *Vaak* es un software creado por una *startup* japonesa que analiza el lenguaje corporal e identifica las actitudes más sospechosas. Inquietud, incertidumbre, movimientos inusuales son captados por las cámaras y analizados por el *software* para evitar, por ejemplo, los robos en los supermercados.

Cortica[305], una empresa israelí que se ocupa de seguridad e inteligencia artificial, ha firmado recientemente un acuerdo para analizar las imágenes recopiladas por las cámaras de seguridad en áreas públicas de la India. El *software* de la compañía promete buscar anomalías de comportamiento que indiquen que alguien está a punto de cometer un crimen violento. El programa se basa en los sistemas militares desarrollados para identificar terroristas. Busca las llamadas microexpresiones, pequeños espasmos o gestos que pueden revelar las intenciones de una persona. Según sus desarrolladores, Cortica puede incluso aprender a predecir cuándo un mercado pacífico y lleno de personas o una manifestación política están a punto de volverse violentos. Una aplicación potencialmente muy útil en Israel.

Igualmente, podemos señalar también la existencia de la plataforma denominada "POL-INTEL" en Dinamarca, que cruza datos alojados en bases de datos de la policía procedentes de investigaciones con otros captados a través de videocámaras, internet, redes sociales y *databrokers*, todo ello al amparo de una nueva legislación que refuerza las

---

[303] "La policía británica quiere usar IA para predecir delitos antes de que ocurran", *La Vanguardia*, 2018, fecha de consulta 21 julio 2021, en https://www.lavanguardia.com/tecnologia/20181202/453268636098/policia–britanica–uso–inteligencia–artificial–delitos–crimenes–delincuencia.html.

[304] "Predictive policing", *Liberty*, fecha de consulta 20 agosto 2021, en https://www.libertyhumanrights.org.uk/fundamental/predictive–policing/.

[305] "Cortica – Autonomous AI", fecha de consulta 21 julio 2021, en https://www.cortica.com/.

capacidades de intrusión de la policía y servicios secretos en el ejercicio de sus funciones de prevención de la delincuencia[306].

En España, entre otras aplicaciones, puede señalarse la existencia de VeriPol, que, aunque no constituye una aplicación en materia de ciberpatrullaje como tal, sí supone un caso de integración de la tecnología de inteligencia artificial en las funciones de la policía.[307]

A pesar de todas estas dudas, el *software* predictivo se abre camino en todo el mundo. En España aún no se utilizan de manera oficial, pero el programa *Eurocop*[308], un proyecto de la Universidad de Castellón, está diseñado para elaborar un mapa de previsión de riesgo en lugares concretos de una ciudad y en determinados horarios.

De igual modo, el Área de Violencia de Género, Estudios y Formación de la Secretaría de Estado de Seguridad ha incorporado la plataforma analítica de la empresa de *software* SAS Iberia, que facilitará actualizaciones mucho más rápidas y eficaces del Protocolo de Valoración Policial de Riesgo del Sistema VioGén. Hasta ahora, los algoritmos matemáticos de los dos formularios de valoración policial del riesgo de reincidencia del Sistema VioGén (VPR y VPER) se han actualizado mediante la selección de muestras de casos y el análisis manual de algunos indicadores de riesgo, tras su seguimiento durante varios años. Con el *software* de SAS Iberia se va a incorporar tecnología de analítica avanzada e inteligencia artificial que automatizará el análisis de una mayor cantidad de datos de criminalidad, combinados incluso con datos de fuentes abiertas, lo que ayudará a ponderar mejor los algoritmos, identificando nuevos indicadores de riesgo, y en periodos de tiempo mucho más cortos. Además, son algoritmos más sensibles a la evolución de la criminalidad y mejoran con ello la predicción de aquellos casos en los que quepa que se produzcan agresiones reincidentes.[309]

---

[306] MERKEL, L., *Derechos humanos e investigaciones policiales*, cit., p. 292.
[307] GARCÍA, J., "VeriPol, el polígrafo 'inteligente' de la policía, puesto en cuestión por expertos en ética de los algoritmos", *EL PAÍS*, 2021, fecha de consulta 21 julio 2021, en https://elpais.com/tecnologia/2021–03–08/veripol–el–poligrafo–inteligente–de–la–policia–puesto–en–cuestion–por–expertos–en–etica–de–los–algoritmos.html.
[308] "Inicio", *Eurocop | Software de Gestión Policial*, fecha de consulta 21 julio 2021, en https://www.eurocop.com/.
[309] "Interior recurre a la tecnología de inteligencia artificial para mejorar la valoración policial de riesgo en casos de violencia de género", *Noticias Jurídicas*, noticias.juridicas.com, fecha de consulta 21 julio 2021, en https://noticias.juridicas.com/actualidad/noticias/15848–interior–recurre–a–la–tecnologia–de–inteligencia–artificial–para–mejorar–la–valoracion–policial–de–riesgo–en–casos–de–violencia–de–genero/.

En la reunión mundial de INTERPOL y el UNICRI sobre inteligencia artificial y aplicación de la ley se determinó que la perturbación de los sistemas controlados por inteligencia artificial, la generación de noticias falsas por medio de la inteligencia artificial y el uso de sistemas autónomos a modo de armas podrían ser algunos de los delitos del futuro propiciados por la inteligencia artificial.[310]

Cesare Lombroso sostenía que las conductas delictivas son determinadas por predisposiciones fisiológicas, que a menudo se revelan también externamente en la configuración del cráneo. A través de la observación de algunas características anatómicas, por lo tanto, sería posible desenmascarar a un futuro criminal. Lombroso era positivista, esa corriente filosófica convencida de que la respuesta a todas las preguntas de la especie humana se encontrase en la ciencia. Hoy vivimos una era de positivismo digital y la fe puesta en las oportunidades ofrecidas por el *big data* y los algoritmos es casi infinita. Sin embargo, el optimismo tecnológico choca contra la pesadilla de un futuro similar al descrito por George Orwell en 1984, con una "policía del pensamiento" que puede llegar a actuar no sólo sobre delitos, sino también las intenciones[311].

Es de destacar que la Ley Orgánica 7/2021 establece en su artículo 14 que están prohibidas las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o que le afecten significativamente. Ahora bien, establece como salvedad la posibilidad de que ello se autorizado, expresamente por una norma con rango de ley o por el Derecho de la Unión Europea, que deberá establecer las medidas adecuadas para salvaguardar los derechos y libertades del interesado, incluyendo el derecho a obtener la intervención humana en el proceso de revisión de la decisión adoptada.

De igual modo, prohíbe en todo caso, salvo que se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, que dichos tratamientos automatizados utilicen las categorías especiales de datos personales previstas en el artículo 13. Esto es, datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la

---

[310] "Inteligencia artificial y aplicación de la ley: desafíos y oportunidades", fecha de consulta 21 julio 2021, en https://www.interpol.int/es/Noticias–y–acontecimientos/Noticias/2020/Inteligencia–artificial–y–aplicacion–de–la–ley–desafios–y–oportunidades.

[311] "¿Puede predecirse un crimen antes de suceder con un algoritmo?", *La Vanguardia*, 2019, fecha de consulta 21 julio 2021, en https://www.lavanguardia.com/tecnologia/20190318/461013536935/inteligencia–artifical–vigilancia–predictiva–policia.html.

afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, los datos relativos a la salud o a la vida sexual o a la orientación sexual de una persona física.

En todo caso, se ha recordado que las investigaciones policiales basadas en sistemas de inteligencia artificial aún generan muchos errores y falsos positivos, por lo que se hace necesaria la constante revisión y supervisión humanas[312].

B. INTELIGENCIA ARTIFICIAL Y DERECHOS FUNDAMENTALES

Como se ha destacado[313], las nuevas técnicas de inteligencia artificial, aplicadas a las funciones policiales de investigación y averiguación de delitos, pueden suponer un compromiso para los derechos fundamentales, como el derecho a la tutela judicial efectiva, a la intimidad y la presunción de inocencia.

En cuanto al derecho a la tutela judicial efectiva, del que se propone una evolución hacia un derecho a Justicia[314], impide que las herramientas de inteligencia artificial puedan suponer una barrera o impedimento para acceder a la tutela de los tribunales o a métodos alternativos de resolución de conflictos. Además, podría quedar gravemente vulnerado si las herramientas de inteligencia artificial dispensaran a los órganos enjuiciadores de dotar de la necesaria justificación a sus decisiones[315].

La afectación al derecho fundamental a la intimidad por parte del empleo de inteligencia artificial deriva, fundamentalmente, de que los algoritmos que los conforman necesitan grandes acumulaciones de datos, *big data*, para funcionar y de los que extraer las correspondientes conclusiones. Estas ingentes acumulaciones de datos exigen, por su parte, que exista una actividad indiscriminada de recolección de datos sobre las propias conductas y actividades de las personas, actividad esta que, claro está, se hace especialmente posible gracias al auge de internet y el comportamiento en línea, en sus múltiples variantes (realizar compras, chatear, visitar páginas web, realizar búsquedas en motores

---

[312] CHEN, H.; GENG, L.; ZHAO, H.; ZHAO, C.; LIU, A., "Image recognition algorithm based on artificial intelligence", *Neural Computing and Applications*, vol. 34, 9, 2022, p. 47.
[313] NIEVA FENOLL, J., *Inteligencia artificial y proceso judicial*, Marcial Pons, Madrid, 2018, p. 150.
[314] MARTÍN DIZ, F., "El derecho fundamental a justicia: Revisión integral e integradora del derecho a la tutela judicial efectiva", *Revista de derecho político*, 106, 2019, Universidad Nacional de Educación a Distancia – UNED, p. 69.
[315] MARTÍN DIZ, F., "Modelos de aplicación de Inteligencia Artificial en justicia: asistencial o predictiva versus decisoria", en *Justicia algorítmica y neuroderecho: una mirada multidisciplinar, 2021, pp. 65–85*, Tirant lo Blanch, 2021, p. 75, fecha de consulta 30 noviembre 2021, en https://dialnet.unirioja.es/servlet/articulo?codigo=8102554.

creados al efecto, reiterar visitas a determinadas páginas web, consumir determinado contenido de manera reiterada, emplear más tiempo en unos sitios frente a otros, subir fotos a redes sociales indicando, incluso, la ubicación en que fueron tomadas, etc.).

Se ha dicho que, del mismo modo que en el pasado se buscaban piedras y metales preciosos, hoy se buscan datos[316]. A este respecto, quizás pueda decirse que la actividad particular de cada ser humano es el campo perfecto para desplegar nuestro instinto de cada y recolección, pues al ser aquel inmaterial, constantemente renovable y, en fin, inagotable, permite a este expandirse hasta tanto como nuestra naturaleza pueda dar de sí. No es de extrañar, por tanto, el auge de las normativas en materia de protección de datos, que persiguen restringir dicha actividad de captación indiscriminada de datos, así como la declaración de un derecho fundamental de nuevo acuñamiento, como es el del propio entorno virtual.

Lo que es evidente es que los grandes motores de inteligencia artificial exigen como combustible grandes cantidades de datos, y con ello se construyen perfiles, tanto individuales como colectivos, que incluyen patrones de tendencias predefinidos o predeterminados, que pueden coincidir, o no, con los hábitos de cada una de las personas que reciben la etiqueta dispensada por el motor de inteligencia artificial.

Además, y como se ha puesto de manifiesto[317], los algoritmos sufren del denominado "sesgo algorítmico"[318], que ocurre cuando reflejan los valores de los humanos que están implicados en la codificación y recolección de datos usados para entrenar el algoritmo.

Todo ello determina que los motores de inteligencia artificial, aunque presenten determinadas utilidades en el ámbito político o comercial, no puedan, o no deban, ser empleados en materia de investigaciones de delitos, toda vez que, aunque dotan a sus resultados de una apariencia de verdad científica objetiva, en realidad suele tratarse de conclusiones sesgadas, influidas específicamente por los prejuicios[319] de los propios

---

[316] *Ibid.*, p. 65.
[317] VEALE, M.; EDWARDS, L., "Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision–making and profiling", *Computer Law & Security Review*, vol. 34, 2, 2018, p. 2.
[318] MORATINOS, G. L., "Modelos algorítmicos, sesgos y discriminación", en *FODERTICS 9.0: Estudios sobre tecnologías disruptivas y justicia, 2021, pp. 283–294*, Comares, 2021, p. 2, fecha de consulta 30 noviembre 2021, en https://dialnet.unirioja.es/servlet/articulo?codigo=7991762.
[319] MERKEL, L., *Derechos humanos e investigaciones policiales*, cit., p. 293.

creadores del algoritmo y por las bases de datos que han sido empleadas para alimentar su funcionamiento. De ahí que se exija máxima transparencia en el funcionamiento de tales sistemas[320].

Por otro lado, el establecimiento de patrones de conducta para detectar a posibles delincuentes no sólo puede afectar a la intimidad de las personas, sino también al propio derecho a la presunción de inocencia, si en la práctica judicial el órgano enjuiciador permite que su decisión judicial quede sostenida, aunque fuera de manera indirecta, por un previo informe emitido por un sistema de inteligencia artificial empleado por la policía del que resulte específicamente la condición de sospechoso de la persona investigada, y todo ello sin haberse practicado ni una sola prueba.

Además, y a nuestro juicio, para que esta lesión se produjera no serías necesario que los jueces confiasen ciegamente en el informe emitido por el sistema, sino que bastaría con que la mera existencia de dicho informe influyera en el entendimiento del juez, de suerte que valorara la prueba practicada en el acto del juicio sin partir de una posición imparcial. En este sentido, podría incluso afectarse, desde una perspectiva más genérica, al derecho a un juez imparcial como tal, aun cuando en el plenario se hubiera practicado suficiente prueba de cargo.

C. INTELIGENCIA ARTIFICIAL A OJOS DE LA UNIÓN EUROPEA

En la perspectiva de la Unión Europea, debemos hacer referencia a la Comunicación de la Comisión al Parlamento Europeo, el Consejo Europeo, el Comité Económico y Social Europeo y el Comité de las Regiones sobre Inteligencia Artificial para Europa (COM (2018) 237 final), que definen el término inteligencia artificial como aquellos "sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción –con cierto grado de autonomía– con el fin de alcanzar objetivos específicos".

Asimismo, la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y el Comité de las Regiones sobre generar confianza en la inteligencia artificial centrada en el ser humano (COM(2019) 168 final) señalaba siete requisitos esenciales que deben respetar las aplicaciones de IA para ser

[320] ARECES, F. R., "Más transparencia sobre el uso de los algoritmos", *Revista de Occidente*, 479, 2021, p. 2.

consideradas fiables: i) intervención y supervisión humanas, ii) solidez y seguridad técnicas, iii) privacidad y gestión de datos, iv) transparencia, v) diversidad, no discriminación y equidad, vi) bienestar social y medioambiental, y vii) rendición de cuentas.

Con posterioridad, el 19 de febrero de 2020 fue aprobado el Libro blanco sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza (COM(2020) 65 final), que reconocía que el uso de la inteligencia artificial puede provocar la conculcación de derechos fundamentales como la libertad de expresión, la libertad de reunión, la dignidad humana, la ausencia de discriminación por razón de sexo, raza u origen étnico, religión o credo, discapacidad, edad u orientación sexual, y, en su aplicación en determinados ámbitos, la protección de los datos personales y de la vida privada, el derecho a una tutela judicial efectiva y a un juicio justo.

Adicionalmente, debemos hacer también referencia a la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre el marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas, en la que, entre otros pronunciamientos, recordaba que la inteligencia artificial, dependiendo de su desarrollo y de su uso, puede crear y reforzar sesgos, también a través de sesgos inherentes a los conjuntos de datos subyacentes, y, por lo tanto, crear diversas formas de discriminación automatizada, incluida la discriminación indirecta. Asimismo, se reconocía expresamente el carácter necesario de los datos para la existencia de sistemas de inteligencia artificial, al señalar que "sin datos, no hay inteligencia artificial".

Por último, la Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016(INI)) contiene pronunciamientos no desdeñables al respecto[321].

En dicha Resolución, el Parlamento Europeo vuelve a tomar conocimiento de varias realidades, de las que destacamos que la IA no debe considerarse un fin en sí misma,

[321] Partiendo de otras elaboraciones, como la Carta ética europea sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno de la Comisión Europea para la Eficacia de la Justicia (CEPEJ) del Consejo de Europa, la Comunicación de la Comisión, de 8 de abril de 2019, titulada «Generar confianza en la inteligencia artificial centrada en el ser humano» (COM(2019)0168), las directrices éticas para una IA fiable publicadas por el Grupo de expertos de alto nivel sobre inteligencia artificial de la Comisión el 8 de abril de 2019 y el Libro Blanco de la Comisión, de 19 de febrero de 2020, titulado «Inteligencia artificial – Un enfoque europeo orientado a la excelencia y la confianza» (COM(2020)0065).

sino un instrumento al servicio de las personas, con el objetivo primordial de aumentar el bienestar humano, las capacidades humanas y la seguridad (apartado A), que las decisiones relativas al ciclo de vida de las aplicaciones de IA en el ámbito de las actuaciones judiciales y policiales se deben adoptar de forma transparente, salvaguardando plenamente los derechos fundamentales y, en particular, no perpetuando discriminaciones, sesgos o prejuicios allá donde existan (apartado G), que sería desproporcionada toda aplicación generalizada de la IA para fines de vigilancia masiva, aunque se reconozca que pueden ofrecer grandes oportunidades en el ámbito de la garantía del cumplimiento de la ley, en particular en lo que respecta a la mejora de los métodos de trabajo de las autoridades policiales y judiciales y al aumento de la eficacia de la lucha contra determinados tipos de delitos, especialmente los delitos financieros, el blanqueo de capitales y la financiación del terrorismo, los abusos sexuales y la explotación sexual en línea (apartado H), que la utilización rutinaria de algoritmos, incluso con una pequeña tasa de falsos positivos, puede dar lugar a que las falsas alertas superen con creces las alertas correctas (apartado M), lo que debe tenerse en cuenta en los casos en que la IA es utilizada por autoridades policiales, como las tecnologías de reconocimiento facial (por ejemplo, para buscar en bases de datos de sospechosos e identificar a víctimas de trata de seres humanos o abuso y explotación sexual infantiles), el reconocimiento automático de matrículas, la identificación por voz, el reconocimiento del habla, las tecnologías de lectura de labios, la vigilancia auditiva (es decir, algoritmos de detección de disparos), la investigación y el análisis autónomos de bases de datos identificadas, la predicción (actuación policial predictiva y análisis de puntos críticos de delincuencia), los instrumentos de detección del comportamiento, las herramientas avanzadas de autopsia virtual para ayudar a determinar la causa de la muerte, las herramientas autónomas para detectar fraudes financieros y la financiación del terrorismo, la vigilancia de las redes sociales (rastreo [scraping] y recopilación de datos para detectar conexiones) y los sistemas automatizados de vigilancia que incorporan diferentes capacidades de detección (como la detección del latido cardíaco y las cámaras térmicas).

Sobre dichas consideraciones, el Parlamento subraya el derecho de las partes en un procedimiento penal a tener acceso al proceso de recopilación de datos y a las evaluaciones conexas realizadas u obtenidas mediante el uso de aplicaciones de inteligencia artificial (apartado 14), resalta las consecuencias negativas potencialmente graves, particularmente en el ámbito de las actividades policiales y judiciales, que pueden derivarse

de una confianza excesiva en la naturaleza aparentemente objetiva y científica de las herramientas de IA, sin tener en cuenta la posibilidad de que sus resultados sean incorrectos, incompletos, irrelevantes o discriminatorios; hace hincapié en que debe evitarse el exceso de confianza en los resultados ofrecidos por sistemas de IA y destaca la necesidad de que las autoridades adquieran confianza y conocimientos para poner en cuestión recomendaciones algorítmicas o hacer caso omiso de ellas (apartado 15), pide que los algoritmos sean explicables, transparentes, trazables y comprobables como parte necesaria de la supervisión, recomendando el uso de *software* de código abierto (artículo 17), recuerda que, como mínimo, el uso de la tecnología de reconocimiento facial debe cumplir los requisitos de minimización de datos, exactitud de los datos, limitación del almacenamiento, seguridad de los datos y rendición de cuentas, además de ser legal, justo y transparente y perseguir un fin específico, explícito y legítimo (apartado 28).

Para cerrar este capítulo debemos hacer también, aunque se trate de una perspectiva regional, a la Carta ética europea sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno, aprobada en Estrasburgo los días 3 y 4 de diciembre de 2018 por el Consejo de Europa, que establecía cinco principios fundamentales en el empleo de tecnologías de inteligencia artificial: i) principio de respeto de los derechos fundamentales, conforme al cual debe asegurarse que los sistemas de inteligencia artificial estén construidos para respetar los derechos fundamentales "por defecto", ii) principio de no discriminación, para prevenir de manera específica cualquier tratamiento discriminatorio a individuos o grupos; iii) principio de calidad y seguridad, a fin de que el procesamiento de decisiones judiciales se realice a partir de fuentes certificadas y modelos de datos plurales; iv) principio de transparencia, imparcialidad y equidad, a fin de que los sistemas de inteligencia artificial utilicen métodos de procesamiento de datos que no sean oscuros y permitan la realización de auditorías externas; y v) principio de "bajo control del usuario", a fin de que todos aquellos afectados por el empleo de sistemas de inteligencia artificial puedan conocer dicha circunstancia en todo momento y estén en control de sus elecciones.

D. OTROS USOS DE LA INTELIGENCIA ARTIFICIAL

La investigación policial es tan sólo uno de los múltiples ámbitos en los que la tecnología de la inteligencia artificial viene introduciéndose en el ámbito del derecho. Así, vienen sucediéndose inmisiones en materia de predicción del riesgo, resolución de disputas online, diligencia y práctica de pruebas, impulso procesal, y jurisprudencia. A

pesar de ello, los avances en dicha materia vienen produciéndose muy lentamente, consecuencia de la dificultad de aunar las disciplinas informática y jurídica[322].

En materia de automatización de procedimientos, experiencias como las de Estonia, Argentina y Estados Unidos han servido para señalar uno de los principales efectos beneficiosos derivados de la aplicación de la inteligencia artificial a los procedimientos de mero trámite, como es la rapidez en su resolución y, en consecuencia, el efecto disuasorio en las conductas d quienes se aprovechaban en las carencias y lentitud del sistema judicial para evitar sufrir las consecuencias legalmente anudadas a sus propias conductas. Paralelamente también, se pone de manifiesto la dependencia de dichos sistemas de que la documentación aportada y los extremos de hecho respondan a los patrones habituales necesitados por la herramienta en cuestión, así como la ineludible consecuencia de reducir el trabajo disponible para los operadores jurídicos[323].

Por su parte, la preparación de escritos judiciales constituye uno de los ámbitos en los que parece apreciarse con mayor intensidad las bondades de las tecnologías de inteligencia artificial. La sistematización de pronunciamientos judiciales y artículos doctrinales, llevada a cabo incluso antes de la aparición de estos sistemas informáticos, ha facilitado enormemente la aplicación de sistemas automatizados de tratamiento de la información, sistemática esta que, si se expandiera al resto de áreas de la práctica jurídica, permitiría un avance mucho más veloz de la implantación de las tecnologías de inteligencia artificial.

Por lo que se refiere a la cuestión de la prueba, se ha adelantado que la inteligencia artificial puede ayudar en tres campos fundamentales: la revisión de los parámetros de valoración de la prueba[324], la elaboración de hipótesis[325] y la estandarización y control del empleo de los estándares probatorios[326]. Se trata, en definitiva, de desplegar un

---

[322] NIEVA FENOLL, J., "Inteligencia artificial y proceso judicial: perspectivas tras un alto tecnológico en el camino.", *Revista General de Derecho Procesal*, 57, 2022, Iustel, p. 3.
[323] *Ibid.*, p. 6.
[324] Elaborado "listas numeradas" que permitan señalar al tribunal posibles elementos de riesgo o pautas sobre la objetividad con la que el medio de prueba en concreto aporta la fuente de prueba al proceso, como indica NIEVA FENOLL, J., "Inteligencia artificial y proceso judicial: perspectivas tras un alto tecnológico en el camino.", *Revista General de Derecho Procesal*, 57, 2022, Iustel, p. 11.
[325] Como el sistema ALIBI, que permite elaborar argumentos y estrategias de acusación y defensa a partir de los elementos probatorios que se introduzcan.
[326] NIEVA FENOLL, J., "Inteligencia artificial y proceso judicial", cit., p. 12.

aparato auxiliar para el tribunal que permita garantizar una mayor pulcritud en las valoraciones y motivaciones judiciales.

La predicción del riesgo se encuentra íntimamente vinculada a las utilidades de la inteligencia artificial en funciones de investigación policial. En general, en estos casos, los sistemas de inteligencia artificial atienden a un conjunto de datos objetivos para arrojar un resultado sobre el riesgo de comisión delictiva de un determinado perfil, sustituyendo de esta manera las evaluaciones que, de igual modo, pero con menor celeridad, venían elaborando los psicólogos especializados en la materia. Las críticas surgen, a nuestro entender, desde una doble perspectiva: por un lado, no está claro que determinados datos (raza, religión, sexo, etc.) resulten verdaderamente relevantes para calcular el riesgo delictivo que presenta una persona determinada; por otro, tampoco existe control suficiente sobre el modo en que dichos datos se trasladan en variables numéricas susceptibles de valoración por los algoritmos correspondientes[327].

La resolución de conflictos online, por último, también supone un amplio espacio para la aplicación de la tecnología de inteligencia artificial. En ello tienen cabida no sólo la mera resolución de disputas en línea, sino el tratamiento automatizado de determinados procedimientos -o, al menos, fases iniciales de los mismos- que permitirá desplegar una función jurisdiccional de gran inmediatez. Piénsese en juicios monitorios, divorcios de mutuo acuerdo, procedimientos de jurisdicción voluntaria en los que sea necesario el consentimiento previo del afectado, o incluso la fase de conciliación previa en según qué procedimientos. De igual modo, no sólo cabe la posibilidad de una tramitación automática de dichos procedimientos, sino que a través de tecnologías como la *blockchain* y los *smart contracts* sea posible que ante determinadas circunstancias los procesos judiciales se inicien de manera automática[328].

En definitiva, la inteligencia artificial constituye una tecnología con amplias posibilidades para el ámbito jurídico. Su adopción constituye, desde luego, un proceso lento no sólo por la propia idiosincrasia de la ciencia jurídica, sino por circunstancias socioeconómicas ajenas que determinan el ritmo de la innovación.

---

[327] *Ibid.*, p. 16.
[328] *Ibid.*, p. 18.

Independientemente de ello, resulta necesario generar un cambio de paradigma en la práctica jurídica para que la práctica jurídica pueda convertirse en datos objetivos que sean posibles de introducir y analizar por algoritmos.

Paralelamente, se hace necesario establecer un férreo control sobre, cuanto menos, tres aspectos: i) en primer lugar, la recolección de los datos necesarios para alimentar los sistemas de inteligencia artificial; ii) en segundo lugar, la determinación de los datos que se consideren relevantes para el funcionamiento de los sistemas de inteligencia artificial; y iii) en tercer lugar, el proceso de evaluación de dichos datos y de aportación de la correspondiente conclusión por los sistemas de inteligencia artificial. Todo ello acompañado de la posibilidad de disponer de revisiones no automatizadas de dichas decisiones.

Solamente con dicho control podrá garantizarse el respeto y vigencia de los derechos y libertades de los ciudadanos y de las garantías procesales.

9. OTRAS TÉCNICAS POLICIALES UTILIZADAS EN LA CIBERVIGILANCIA

Según se ha indicado, "la policía utiliza varias herramientas en sus fines investigativos y preventivos del delito en la red. Por un lado, utiliza con carácter general herramientas que sirven para realizar búsquedas, identificaciones y monitorizaciones de perfiles, personas, eventos, etc. Estas herramientas son *opensource*, de libre acceso y sirven para recabar y analizar información que se encuentra publicada en la red. Por otro lado, la policía utiliza también herramientas de búsqueda más especializadas cuando existe constancia de que se está cometiendo un delito o se está compartiendo una información que pudiera tener contenido sensible o delictivo, o cuando se le asigna un objetivo específico a investigar, pero lo que está claro es que nunca realizan monitorizaciones masivas ni identificaciones extrañas…"[329].

En este apartado trataremos de aportar una relación de técnicas e instrumentos que se emplean en el desarrollo de la cibervigilancia. Ha de reseñarse, igualmente, que existen iniciativas particulares que persiguen concienciar a la ciudadanía de los intentos por parte de los poderes públicos de establecer redes de vigilancia. Por ejemplo, la EFF ha puesto

[329] "¿Cómo vigila la policía los delitos en internet? Silvia Barrera, de la UIT de @policia, responde", fecha de consulta 2 mayo 2020, en https://www.youtube.com/watch?v=ijjBiSu57SE.

en marcha un entorno de entrenamiento utilizando tecnología de realidad virtual[330], dentro del programa "*Street–Level Surveillance*"[331].

Monitorización de redes sociales: Facebook, Twitter, Instagram y otras redes sociales constituyen auténticas fuentes de datos muy valiosos en la actividad de *ciberpatrullaje*, hasta el punto de existir departamentos específicos dentro de los cuerpos policiales que se ocupan de esta materia[332]. Como es fácil de suponer, uno de los elementos más valiosos es el hecho de que las redes sociales están diseñadas para que la información sea pública por defecto, por lo que el usuario que ha publicado los datos podría entenderse que ha consentido su acceso por terceros, incluyendo el poder público[333]. Es conocida, igualmente, la práctica policial consistente en añadir como amigos o contactos en las diferentes redes sociales a usuarios que, por uno u otro motivo, se consideren de interés[334].

El rastreo de redes sociales se puede dividir en tres categorías: i) rastreo de un individuo, un grupo o una afiliación (por ejemplo, un *hashtag* o etiqueta en línea) a través de información disponible públicamente; ii) uso de un informante, un amigo del objetivo o una cuenta encubierta para obtener información de una cuenta protegida o privada; y iii) uso de software para monitorizar individuos, grupos, asociaciones o ubicaciones. Aparte de estas actuaciones, debe recordarse que las redes sociales, en tanto prestadores de servicios de la sociedad de la información, están sometidos al deber de colaboración con la Policía Judicial[335].

Estas técnicas de cibervigilancia relativas al patrullaje de redes sociales plantea, ciertamente, no pocos problemas. Por un lado, surgen casos de falsos positivos, en la medida en que el contenido puede resultar difícil de interpretar correctamente, circunstancia esta que se ve también afectada por el empleo de programas o técnicas de recogida

---

330 "Spot the Surveillance: A VR Experience for Keeping an Eye on Big Brother", *Electronic Frontier Foundation*, 2018, fecha de consulta 11 mayo 2020, en https://www.eff.org/pages/descubra–la–vigilancia–una–experiencia–de–realidad–virtual–para–no–perder–de–vista–al–gran.

331 "Street–Level Surveillance", *Electronic Frontier Foundation*, fecha de consulta 11 mayo 2020, en https://www.eff.org/issues/street–level–surveillance.

332 "¿Cómo vigila la policía los delitos en internet? Silvia Barrera, de la UIT de @policia, responde".

333 "Government Monitoring of Social Media: Legal and Policy Challenges", *Brennan Center for Justice*, fecha de consulta 4 mayo 2020, en https://www.brennancenter.org/our–work/research–reports/government–monitoring–social–media–legal–and–policy–challenges.

334 "The Wildly Unregulated Practice of Undercover Cops Friending People on Facebook", *The Root*, fecha de consulta 4 mayo 2020, en https://www.theroot.com/the–wildly–unregulated–practice–of–undercover–cops–frie–1828731563.

335 "New York City Police Department Surveillance Technology", *Brennan Center for Justice*, fecha de consulta 4 mayo 2020, en https://www.brennancenter.org/our–work/research–reports/new–york–city–police–department–surveillance–technology.

y análisis automatizado de datos. Por otro lado, entra también en conflicto con la privacidad de los ciudadanos, pues es perfectamente posible que los usuarios, aun utilizando una red social, no tengan intención de consentir el acceso público a sus datos, y, sin embargo, por mero desconocimiento de la plataforma, lo estén permitiendo *de facto*. Por último, plantea también graves problemas en materia de discriminación por motivos raciales, género, o de ideología, al ser unos tipos de perfiles de internauta más propensos a ser objeto de más investigaciones que otros. Asimismo, en el ámbito de la libertad de expresión, pues puede provocar que los individuos, por temor a las consecuencias derivadas de una investigación oficiosa, se autocensuren en sus contenidos y protestas.

Simuladores de antenas de telefonía: Los simuladores de antenas de telefonía (*stingrays o IMSI–catchers*) son dispositivos que engañan a los teléfonos dentro de un radio determinado para que el dispositivo se conecte a ellos creyendo que es uno de los repetidores de telefonía de su operador[336].

Estos sistemas son utilizados no sólo para obtener el IMSI e IMEI de los dispositivos móviles a los que se conectan –lo que pueden realizar de manera masiva–, sino que permiten también acceder a su contenido e interceptar sus procesos comunicativos[337]. Se trata, por tanto, de una herramienta cuya utilización no precisa de autorización judicial para la Policía Judicial en los supuestos de obtención de IMSI o e IMEI pero que, sin embargo, podría afectar al secreto de las comunicaciones o registrar el dispositivo, resultando imposible controlar cuál es el acceso efectivo realizado por la Policía. Por esta potencialidad lesiva hemos de hacer constar nuestras reticencias respecto a su uso carente de control.

Estas medidas afectan, fundamentalmente, a los derechos de los artículos 18.1, 18.3 y 18.4 CE, en la medida en que estos dispositivos pueden localizar y seguir a los individuos mientras se mueven en espacios públicos y privados, incluso cuando se encuentren en lugares en los que sería necesaria autorización judicial para acceder.

Programas de identificación de archivos: *PhotoDNA Cloud Service*[338] es un *software* desarrollado por Microsoft que tienen las principales policías del mundo y las

---

[336] "3G–GSM Tactical Interception & Target Location", fecha de consulta 5 mayo 2020, en https://info.publicintelligence.net/Gamma–GSM.pdf.
[337] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 452.
[338] "PhotoDNA Cloud Service | Microsoft", fecha de consulta 5 mayo 2020, en https://www.microsoft.com/en–us/photodna/cloudservice.

grandes compañías de aplicaciones sociales, incluyendo Facebook y Twitter, que lo adoptaron en 2013.[339] También lo utilizan Google, Adobe y Reddit, además de la propia Microsoft en sus servicios en la nube.

Este programa actúa a dos niveles. Por un lado, almacena la huella digital de las imágenes o vídeos que reciben, calculando su identificador *hash*, lo que permite que el sistema reconozca el material si vuelve a interceptarlo. Por otro lado, y en ese segundo nivel, el sistema reconoce formas y situaciones compatibles con pornografía infantil y abusos sexuales. Por supuesto, la detección puede dar lugar a falsos positivos.

Así, el *PhotoDNA* realiza "un chequeo automático" de internet, escaneado de webs, correos electrónicos y redes sociales. Cuando detecta un contenido que podría ser de pornografía infantil, lo remite al *National Center for Missing and Exploited Children* (Centro Nacional de Niños Desaparecidos y Explotados) de Estados Unidos, entidad a la que Microsoft donó esta tecnología, que identifica la IP del usuario y el país desde el que se está compartiendo, notificándolo a las autoridades correspondientes para que comiencen la investigación.

Desde su creación, el programa ha recibido mejoras paulatinas para poder examinar y reconocer grabaciones de vídeos y sonidos, y no sólo fotografías, y ha pasado a formar parte del conjunto de servicios *Azure* prestado por Microsoft. En la actualidad, se realizan intentos para que el programa sirva para reconocer otro tipo de contenidos, al margen de pornografía infantil (por ejemplo, contenido extremista y actuaciones de reclutamiento para grupos terroristas). En la Unión Europea se plantea su conveniencia en un marco jurídico que sitúe como responsables a las plataformas que actúan como intermediarias en internet.[340]

---

[339] "PhotoDNA, el sistema que chiva a las policías y redes sociales de todo el mundo quién comparte pornografía infantil", *La Vanguardia*, 2017, fecha de consulta 2 mayo 2020, en https://www.lavanguardia.com/sucesos/20170307/42577580221/photodna–sistema–pornografia–infantil.html.

[340] "The EU's horizontal regulatory framework for illegal content removal in the DSM | Hearings | Events | IMCO | 8ª legislatura (2014 – 2019) | Committees | European Parliament", fecha de consulta 5 mayo 2020, en https://www.europarl.europa.eu/committees/en/product–details/20180613CHE04321.

Similar utilidad presenta el programa *GnuWatch*, utilizado ampliamente por la policía en España, aunque parece que este último requiere ser alimentado previamente de forma "manual", introduciendo los archivos que deba rastrear en las redes P2P .[341]

Destacan dos cuestiones problemáticas que plantea este sistema: por un lado, la existencia de falsos positivos en los reconocimientos del programa; por otro lado, la innegable realidad de que, para que el programa funcione, necesariamente debe tener acceso al contenido de los archivos de los usuarios, y no sólo respecto de aquellos subidos a redes sociales, sino también los que se encuentren en carpetas privadas en servicios de alojamiento en la nube, etc. Este acceso, además, debe ser absoluto y para todos los archivos, pues la única forma de comprobar el contenido de los mismos es, precisamente, accediendo a ellos.

Bases de datos de delincuentes y redes criminales: Las bases de datos de delincuentes contienen información sobre las personas que la policía considera como pandilleros confirmados o sospechosos. Los criterios para su inclusión en la base de datos no siempre se conocen, pero pueden incluir actividades mal definidas, como asociaciones con presuntos miembros de grupos criminales, varios estilos de vestimenta, numerosos colores de ropa y ciertos tatuajes, además de localización geográfica[342].

Como con el resto de las medidas analizadas, se plantean cuestiones en relación con la posible discriminación por razón de la raza, así como la existencia de falsos positivos. Esta cuestión ha generado que grupos sociales hayan solicitado en ocasiones conocer los criterios aplicados para ser incluidos en dichas bases de datos[343], cuya gestión es criticada en todo caso[344].

Lectores automáticos de matrículas: Los lectores automatizados de matrículas son dispositivos que están conectados a coches de policía o fijados en postes para capturar las matrículas de todos los coches que circulan por ese punto. Las lecturas de matrículas también se ejecutan con frecuencia contra una "lista activa" de, por ejemplo, coches

---

[341] "Nueva arma policial: un «GPS» para buscar pedófilos", *La Razón*, 2011, fecha de consulta 2 mayo 2020, en https://www.larazon.es/historico/6205–nueva–arma–policial–un–gps–para–buscar–pedofilos–ILLA_RAZON_363956/.

[342] WINSTON, A., "Vague Rules Let ICE Deport Undocumented Immigrants as Gang Members", *The Intercept*.

[343] RUMMELL, N., "Groups Demand to See Criteria for NYPD Gang Database".

[344] "Spotlight: The Dangers of Gang Databases and Gang Policing", *The Appeal*, fecha de consulta 4 mayo 2020, en https://theappeal.org/spotlight–the–dangers–of–gang–databases–and–gang–policing/.

robados. Estos sistemas, además, permiten capturar fotografías de los vehículos, sus conductores y pasajeros, y esa información es acumulada en bases de datos para estudiar movimientos, asociaciones y relaciones con otros delitos. Como sucede con el resto de herramientas, el peligro aparece ante una doble posibilidad: por un lado, el acceso a la información construida; por otro, los errores en los propios sistemas[345].

Sistemas integrados de vigilancia: El *Domain Awareness System* (DAS)[346] es una red de cámaras, *software*, sensores, bases de datos, dispositivos e infraestructura relacionada que proporciona información y análisis a la policía para cumplir su función de "seguridad pública" y para "detectar, disuadir y prevenir posibles actividades aterrorizadas". El sistema, establecido en Nueva York, está conectado a 18.000 cámaras de video CCTV alrededor de la ciudad. También tiene acceso a datos de al menos 2 mil millones de lecturas de matrículas, 100 millones de citaciones, 54 millones de 911 llamadas, 15 millones de quejas, 12 millones de informes de detectives, 11 millones de arrestos y 2 millones de órdenes. Los datos de las cámaras de CCTV se conservan durante 30 días, las lecturas de LPR durante al menos 5 años. Los registros de texto están preparados para soportar búsqueda OCR.[347]

La tecnología plantea grandes conflictos en materia de falsos positivos al realizar detecciones automáticas erróneas, así como en materia de privacidad de los ciudadanos, al cubrir gran parte del espacio público. Igualmente, se plantean cuestiones relativas a la posibilidad de ceder los datos a otros organismos públicos.

También existen torres de vigilancia, que permiten a los oficiales monitorear áreas de varias historias sobre el nivel de la calle, así como registrar movimientos dentro de un área específica. Las torres *SkyWatch,* por ejemplo. contienen luces de inundación, un escritorio de comandos, dispositivos para detectar velocidades de vehículos, ventanas tintadas, grabadoras de vídeo digitales y cámaras de vigilancia personalizadas[348]. El equipo estándar colocado en las torres *TerraHawk* es desconocido, pero su tecnología patentada

---

[345] LECHER, C., "Privacy advocate held at gunpoint after license plate reader database mistake, lawsuit alleges", *The Verge*, 2019, fecha de consulta 5 mayo 2020, en https://www.theverge.com/2019/2/21/18234785/privacy–advocate–lawsuit–california–license–plate–reader.
[346] MERKEL, L., *Derechos humanos e investigaciones policiales*, cit., p. 290.
[347] "New York City Police Department Surveillance Technology", fecha de consulta 5 de mayo de 2020, en https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology.
[348] "FLIR Skywatch options", fecha de consulta 5 mayo 2020, en https://www.flir.com/globalassets/imported-assets/document/skywatch-options.pdf.

contempla el uso de cámaras de vigilancia junto con detectores infrarrojos, detectores de movimiento y un dispositivo de imágenes térmicas.

Drones y vehículos autónomos: Los drones son aparatos voladores operados de forma remota, con un tamaño que varían en tamaño, que pueden equiparse con varias cámaras, sensores y otros dispositivos. Por ejemplo, pueden desplegar cámaras capaces de reconocimiento facial, y también pueden contener rastreadores GPS, e incluso dispositivos Stingray.

Del mismo modo, también se emplean furgonetas y otros vehículos con sistemas de rayos X. Estas furgonetas utilizan rayos X que rebotan en objetos, lo que permite a la policía ver en los vehículos y detrás de las paredes mientras la furgoneta pasa, incluyendo domicilios y otros lugares privados. En consecuencia, plantea también graves conflictos en cuanto a la privacidad de los ciudadanos, pues tiene la potencialidad de examinar cualquier detalle de la vida íntima de los mismos, dentro de sus domicilios, vehículos, cuerpos, etc. Asimismo, también surgen conflictos en materia de salud, pues al fin y al cabo se expone a los ciudadanos a radiación ionizante sin su consentimiento[349].

Sistemas de detección de disparos: El sistema *ShotSpotter*, de desarrollo privado, utiliza sensores para captar sonidos que parecen ser disparos. Los fragmentos de audio se envían automáticamente a los empleados del proveedor que intentan verificar si el sonido representa un disparo realmente. A continuación, el empleado del proveedor transmite información sobre el posible disparo a los agentes de policía. La tecnología plantea graves cuestiones en materia de falsos positivos, pues el sistema puede confundir sonidos, y también en materia de un uso ilícito de la herramienta, pues los dispositivos preparados para detectar disparos podrían detectar y grabar también conversaciones[350].

Equipos y redes trampas (*honeypots* y *honeymonkeys*): Un *honeypot*[351] es un equipo o red trampa utilizado como herramienta de la seguridad informática dispuesto en una red o sistema informático para ser el objetivo de un posible ataque informático y, así,

---

[349] FRIEDERSDORF, C., "The NYPD Is Using Mobile X–Ray Vans to Spy on Unknown Targets", *The Atlantic*, 2015, fecha de consulta 5 mayo 2020, en https://www.theatlantic.com/politics/archive/2015/10/the–nypd–is–using–mobile–x–rays–to–spy–on–unknown–targets/411181/.

[350] "Privacy Audit & Assessment of ShotSpotter, Inc.'s GunshotDetection Technology", fecha de consulta 5 mayo 2020, en https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5d40c3693d74b7000160dfbc/1564525424759/Privacy+Audit+and+Assessment+of+Shotspotter+Flex.pdf.

[351] GALLEGO, E., "Honeynets: Aprendiendo del Atacante".

poder detectarlo y obtener información del mismo y del atacante[352]. La característica principal de este tipo de programas es que están diseñados para servir de señuelo invisible al atacante y permitir posteriormente el análisis de dicho ataque[353]. Además, también se utilizan para alertar de la existencia del ataque u obtener información sin interferir en el mismo, e incluso ralentizar el ataque (*sticky honeypots*)[354]. No es necesario que tengan ningún tipo de soporte material, pudiendo ser enteramente digitales, denominándose entonces *honeytokens*. Sirven, también, para crear registros falsos en una base de datos y así detectar posibles accesos no autorizados[355]

Desde el año 2000 existe el llamado "*Honeynet Project*", que es una organización internacional sin ánimo de lucro dedicada a investigar la actualidad de los ciberataques y desarrollar herramientas de código abierto que mejoren la seguridad de internet[356].

Como ventajas de los sistemas *honeypot* se refiere: i) que recogen pocos datos de la red, al activarse exclusivamente cuando alguien o algo entra en contacto con ellos; ii) que reducen los supuestos de falsos positivos, pues es difícil que por error se entre en contacto con dichos sistemas; iii) que aun cuando el ataque se encuentra encriptado la actividad queda registrada; iv) que funcionan con el protocolo IPv6; y v) que pueden adaptarse a las diferentes necesidades de las organizaciones.

Paralelamente, se identifican como desventajas el limitado campo de visión que aportan desde el punto de vista de la seguridad informática y el riesgo de que, a su vez, el propio sistema *honeypot* sea asimilado por el atacante, sirviéndole a sus propias finalidades.

Desde el punto de vista jurídico, son destacables las dudas que puedan surgir en cuanto a la verificación de tipos penales cuando un individuo entra en contacto con un *honeypot*. Desde el punto de vista de la incitación al delito, entendemos que eso no

---

[352] "Tracking down hi–tech crime", 2006, fecha de consulta 4 mayo 2020, en http://news.bbc.co.uk/2/hi/technology/5414502.stm.
[353] De ahí su nombre, pues atrae a los delincuentes como la miel a las abejas.
[354] "Trapping hackers in the honeypot", 2006, fecha de consulta 4 mayo 2020, en http://news.bbc.co.uk/2/hi/technology/6035455.stm.
[355] "Linux.com :: «Know Your Enemy»: Everything you need to know about honeypots", 2008, fecha de consulta 4 mayo 2020, en https://web.archive.org/web/20080202010804/http://www.linux.com/articles/39244.
[356] "The Honeynet Project – Honeypot research", fecha de consulta 4 mayo 2020, en //www.honeynet.org/.

sucederá mientras el sistema permanezca en una posición pasiva hasta ser objeto de alguna interacción.

En cuanto los tipos de *honeypots*, en función del nivel de intensidad de la actividad que permita por parte del atacante, se distinguen entre *honeypots* de alta, media y baja interacción.

En nuestra opinión, el empleo de este tipo de herramientas[357], resultan especialmente importantes desde el punto de vista de los derechos fundamentales, por el compromiso del principio de especialidad que suponen y por cómo se acerca a la propia figura de la provocación del delito. La falta de previsión normativa en nuestro país respecto de estos supuestos obliga a estar a las circunstancias de cada caso para comprobar si las pruebas obtenidas con el empleo de estos cebos trampa pueden tenerse por válidamente aportadas o si responden, por el contrario, a una provocación policial.

Debemos recordar que, de acuerdo con el principio de especialidad, cualquier actuación de investigación tecnológica debe estar encaminada a obtener información sobre la comisión de unos hechos concretos que tengan la apariencia de delito. No está admitido en nuestro ordenamiento jurídico las llamadas intervenciones prospectivas o previas al delito, si bien es necesario reconocer que en la práctica es muy difícil trazar la línea que distingue las actuaciones de policía preventiva de las actuaciones de averiguación de los delitos, aunque deban rechazarse, en todo caso, aquellas actuaciones de prevención que afecten a derechos fundamentales. Esto contrasta, por ejemplo, con supuestos como el del ordenamiento jurídico alemán, en el que se admiten ciertas medidas preventivas cando concurran un peligro futuro que amenace la seguridad del Estado, la vida, la salud o la libertad de las personas o propiedades de un valor importante, aun cuando no haya proceso penal abierto por no estarse persiguiendo un delito concreto[358].

---

[357] Junto con las actuaciones de rastreo e inserción que los agentes policiales realizan en determinadas comunidades virtuales, en las que proceden a intercambiar o solicitar archivos de carácter ilícito con la finalidad de detectar posibles conductas delictivas.

[358] GONZÁLEZ NAVARRO, A., "Medios tecnológicos de investigación en el proceso penal alemán: Una visión comparada", en *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas, 2018, pp. 233–282*, Tirant lo Blanch, 2018, p. 239, fecha de consulta 15 noviembre 2021, en https://dialnet.unirioja.es/servlet/articulo?codigo=7751709.

Como, ilustremente a nuestro entender, se ha puesto de manifiesto[359], el gran problema se plantea porque muchas de estas actuaciones policiales tienen lugar cuando aún no se ha cometido delito alguno –o no existe sospecha razonablemente fundada–, lo que supone una auténtica vulneración del principio de especialidad.

Soluciones del centro criptológico nacional: Con el objetivo de facilitar las labores de supervisión del entorno para la detección de amenazas, el CCN–CERT, Centro Criptológico Nacional, ha desarrollado ELISA, estudio simplificado de fuentes abiertas, una nueva herramienta de cibervigilancia dirigida a establecer "los marcadores preventivos, los indicadores de presencia y las características constituyentes que permitan identificar, de una manera temprana, consensuada y basada en la evidencia, las nuevas amenazas que se ciernen sobre el *ciberespacio*".

ELISA pretende facilitar la monitorización de fuentes abiertas, así como el perfilado de medios y entidades de redes sociales. Para ello, cuenta con una base de datos normalizada para el intercambio de información y explotación de los datos a través de indicadores de desconfianza. De esta forma, la herramienta contribuye a la mejora de las capacidades de cibervigilancia, permitiendo realizar un seguimiento e interpretación de lo que sucede en el *ciberespacio*, y, así, efectuar una prospectiva digital[360]. ELISA es una de las múltiples soluciones adoptadas por el CCN–CERT en materia de ciberseguridad[361].

No ha sido posible conocer cuáles son esos indicadores de desconfianza, marcadores preventivos e indicadores de presencia empleados, lo que revela la falta de control en estos aspectos relativos a la actividad de *ciberpatrullaje*.

Durante el año 2020, INCIBE-CERT gestionó un total de ciento treinta y tres mil ciento cincuenta y cinco incidentes de ciberseguridad en España, siendo los más frecuentes los de tipo malware, seguidos de los fraudes[362].

Por último, merece la pena señalar que no existe información pública relativa a las técnicas específicas utilizadas por la policía en España.

---

[359] MARTÍN RÍOS, P., "El necesario enfoque procesal de la Digital Forensics", en *El sistema jurídico ante la digitalización. Estudios de Derecho Público y Criminología, 2021, pp. 265–286*, Tirant lo Blanch, 2021, p. 282, fecha de consulta 15 noviembre 2021, en https://dialnet.unirioja.es/servlet/articulo?codigo=7964426.
[360] "ELISA", fecha de consulta 4 mayo 2020, en https://www.ccn–cert.cni.es/soluciones–seguridad/elisa.html.
[361] Otras son Amparo, Ana, Atenea, Carmen, CCN–Droid, Clara, Claudia, Microclaudia, Elisa, Emma, Gloria, Inés, Loreto, Lucía, María, Marta, Mónica, Reyes, Pilar, Rocío y Vanesa.
[362] GUTIÉRREZ, J. L. Y OTROS, "Estudio sobre la Cibercriminalidad en España", cit., p. 20.

A pesar de la falta de información al respecto ofrecida por las autoridades policiales, puede extraerse alguna información de los datos disponibles en las plataformas de contratación públicas.

Así, sabemos que se gestionan contratos para las siguientes finalidades, según información disponible en el portal web contrataciondelestado.es:

- Adquisición de software para visualizar y programar los dispositivos de seguimiento que utilizan la red IRIDIUM para su comunicación para ser utilizado por la Sala Operativa de la Jefatura de Sistemas Especiales.
- Suscripción de licencias de software para la D.G.P.
- Adquisición de licencias de tecnología Software AG, con destino al Cuerpo Nacional de Policía.
- Mantenimiento de licencias de tecnología BMC TRUESIGHT para el Área de Informática de la D.G.P.
- Suministros de software y de análisis forense acústico, sistema de recuperación de discos.
- Mantenimiento de licencias de gestión tecnologías de información y comunicaciones en tecnología BMC Remedy para la DGP.
- Contratación de los servicios de mantenimiento de licencias de software de tecnología "Software AG".
- Servicio de Mantenimiento de los equipos de los Laboratorios de Acústica Forense, sistema BATVOX para la identificación biométrica de locutores.
- Servicio de Mantenimiento de Hardware y Software corporativo de Buck up deduplicador basado en tecnología Dell/EMC2 para la Dirección General de la Policía.
- Suministro de hardware de análisis forense de imagen de datos (lote 1) y software de análisis forense de gestión de datos (lote 2).
- Adquisición de 3 BTS *trackar standalone* para la DGP.
- Suministro de hardware de análisis forense de imagen de datos (lote 1) y software de análisis forense de gestión de datos (lote 2).
- Adquisición de 3 BTS *trackar standalone* para la DGP.

Asimismo, y aunque escape al concepto estricto de ciberpatrullaje como tal, no podemos dejar de hacer referencia a los casos recientemente llegados a conocimiento público relativos al empleo del programa *Pegasus*, un programa espía ofrecido por la

empresa israelí NSO Group, en los que se ha puesto de manifiesto la capacidad operativa de este tipo de herramientas[363].

[363] Disponible en https://12ft.io/proxy?q=https%3A%2F%2Felpais.com%2Fespana%2F2022-05-06%2Fpegasus-al-desnudo-un-intruso-silencioso-y-con-boton-de-autodestruccion.html, fecha de consulta 15 de junio de 2022.

CAPÍTULO IV
ACTIVIDAD DE LA POLICÍA JUDICIAL EN EL PROCESO PENAL: LAS DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICA O CIBERINVESTIGACIÓN

Las Fuerzas y Cuerpos de Seguridad, en el desempeño de sus funciones de Policía Judicial, cuentan entre sus funciones con las de garantizar la seguridad ciudadana, averiguar la autoría y circunstancias de los delitos, y recoger los efectos, instrumentos y pruebas de ellos, poniéndolos a disposición de la autoridad judicial. Estas funciones quedan previstas en los artículos 104 CE, 549.1 LOPJ, 34.2 LO 2/1086, LOPD 15/1999 (ex DA 14ª LO 3/2018), así como en la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana[364].

En este capítulo nos referiremos a aquellas diligencias de investigación tecnológica propiamente dichas que, previstas en los artículos 588 *bis* y siguientes LECrim, pueden ser llevadas a cabo por la Policía Judicial sin necesidad de autorización judicial previa.

Dentro de ese grupo de diligencias de investigación tecnológica, además, habrá que distinguir, por un lado, entre aquellas que pertenecen de manera originaria a la esfera de autonomía de dichos poderes investigadores, y que, por tanto, serán ejecutadas sin necesidad de autorización judicial en ningún momento, y, por otro lado, aquellas otras que, exigiendo con carácter general autorización judicial previa a su ejecución, en determinadas circunstancias –vinculadas a la noción de urgencia[365], como veremos– permiten que la Policía Judicial las ejecute sin necesidad de habilitación previa, aunque sí precisen de la ratificación judicial *ex post*.

En el primer grupo se distinguen las diligencias de investigación reguladas en los artículos 588 *ter* k), 588 *ter* l) y 588 *ter* m) LECrim, que componen la sección 3ª, "Acceso

[364] Por su parte, el Ministerio Fiscal queda también habilitado para el desempeño de tales funciones en virtud de lo dispuesto en los artículos 773.2 LECrim y 5 EOMF.
[365] O de flagrancia, incluso.

a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad", del capítulo V, "La interceptación de las comunicaciones telefónicas y telemáticas", del título cuyo estudio nos ocupa, y se refieren respectivamente, a: i) la identificación mediante número IP (aunque, más bien, consistiría en la obtención de la dirección IP); ii) la identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes; y iii) la identificación de titulares de terminales o dispositivos de conectividad. Se trata, en suma, de "capacidades de investigación tecnológica que desempeñan el Ministerio Fiscal y la Policía Judicial sin necesidad de recabar autorización judicial"[366]. También habría que añadir aquí, por la falta de exigencia de autorización judicial al respecto, la captación de imágenes en lugares o espacios públicos, conforme al artículo 588 *quinquies* a) LECrim.

En el segundo grupo, por su parte, se incluyen las medidas de intervención de comunicaciones, conforme al apartado 3 del artículo 588 *ter* d LECrim, la utilización de dispositivos o medios técnicos de seguimiento y localización, conforme al apartado 4 del artículo 588 *quinquies* b, y el registro de dispositivos de almacenamiento masivo de información, de acuerdo con los apartados 3 y 4 del artículo 588 *sexies* c. Todas estas medidas contienen una cláusula de urgencia en su regulación, que habilita que en determinadas circunstancias el control judicial de la medida se efectúe tras su realización.

Debe mencionarse, además, que ni las diligencias consistentes en la captación y grabación de comunicaciones orales (artículos 588 *quater* LECrim) ni los registros remotos sobre equipos informáticos (artículos 588 *septies* LECrim) gozan de cláusula de urgencia en sus respectivas regulaciones. Conforme a ello, quedarían, en principio fuera de toda posibilidad de ejecución autónoma por la Policía Judicial y el Ministerio Fiscal[367]. Incluso, se ha apuntado que la medida consistente en la captación y grabación de las comunicaciones orales supone "una vulneración que no creo que pueda ser sanada o salvada por la orden judicial. Además, (…), no creo que esta sea una medida útil en la medida que una vez puesta en marcha esta posibilidad va a ser difícil que aquellos que infringen la ley vayan a descuidar sus actos y comentarios ni siquiera en su domicilio. Y esto será

---

[366] CALVO LÓPEZ, D., "Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (apartados K) a M) del art. 588 ter de la LECrim)", cit., p. 12.

[367] VELASCO NÚÑEZ, E., "Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos", en *Investigación Tecnológica y Derechos Fundamentales*, Aranzadi, Navarra, 2017, p. 230.

así porque se habrá creado un sentimiento general en la sociedad de que el Estado puede meterse en tu casa e instalar dispositivos que captan y graban las conversaciones y las imágenes de lo que sucede. De modo que, finalmente, el delincuente hallará la forma de seguir haciendo sus negocios y la sociedad entera habrá quedado sometida al miedo genérico de ser espiada en su propio domicilio con base en sospechas de la comisión de un delito que tampoco tiene que ser excesivamente grave"[368].

Ahora bien, tampoco puede olvidarse que el artículo 55 CE prevé la posibilidad de suspender los derechos reconocidos, entre otros, en los apartados 2 y 3 del artículo 18 CE, mediante la declaración del estado de excepción o de sitio o mediante la aprobación de una ley orgánica que establezca la forma y los casos en los que tales derechos pueden ser suspendidos. Un sector de la doctrina ha entendido que, existiendo dicha habilitación en la Constitución, así como un régimen normativo que podría aplicarse analógicamente[369], es posible realizar este tipo de diligencias también sin autorización judicial previa en supuestos de urgencia. Entre otros argumentos, se aduce el contrasentido que supondría que se pudiese intervenir una comunicación telefónica de un terrorista y no una conversación oral entre dos terroristas planeando un atentado[370].

En todo caso, entendemos también que no puede olvidarse que este último tipo de diligencias de investigación puede afectar de manera más intensa al derecho a la intimidad personal, previsto en el artículo 18.1 CE, que no es susceptible de ser suspendido, de conformidad con lo dispuesto en el propio artículo 55 CE. Algunos autores señalan, en ese sentido, que la restricción de derechos que supone la captación y grabación de comunicaciones orales directas es más intensa que la producida por la interceptación de comunicaciones telefónicas o telemáticas, porque la expectativa de privacidad de quien se encuentra en su propio domicilio desarrollando su vida privada y familiar es mucho más evidente que la de aquel que emplea medios telemáticos para comunicarse con otro interlocutor. Estas interpretaciones, no obstante, deben actualizarse conforme a la realidad

[368] RICHARD GONZÁLEZ, M., "Conductas susceptibles de ser intervenidas por medidas de investigación electrónica: presupuestos para su autorización", *Diario La Ley*, 8808, 2016, Wolters Kluwer, p. 6.
[369] Las prescripciones establecidas por la LECrim para la medida de intervención de las comunicaciones telefónicas y telemáticas, donde se permite la intervención de la grabación antes de producirse la autorización judicial, una vez que sea aprobada por el Ministerio del Interior o por el Secretario de Estado y siempre que se comunique de forma inmediata, y en todo caso antes de las 24 horas siguientes, al Juez.
[370] ROSALES LEAL, M. Á., "Captación y grabación de comunicaciones orales directas", *Revista de derecho constitucional europeo*, 30, 2018, Instituto Andaluz de Administración Pública.

social, en una cotidianeidad de conversaciones telemáticas en soportes que se anuncian como privados, cifrados y, en fin, a salvo de observaciones de terceros.

1. PRINCIPIOS GENERALES

En los artículos 588 *bis* a) y siguientes LECrim se contiene el régimen jurídico común a las medidas de investigación tecnológica que, como sabemos, suponen una injerencia en los derechos fundamentales del artículo 18 CE. La propia ubicación sistemática del precepto evidencia que su contenido es de aplicación a todas las medidas de investigación digitales: interceptación de las comunicaciones telefónicas y telemáticas, interceptación de las comunicaciones telefónicas y telemáticas, captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, registro de dispositivos de almacenamiento masivo de información, y registros remotos sobre equipos informáticos, así como a las medidas de aseguramiento. Esto es necesariamente destacable porque, como hemos expuesto anteriormente, determinaría qué medidas, que no son objeto de autorización judicial[371], sí deben someterse a los principios previstos en dichos artículos.

El capítulo IV se encuentra estructurado en once artículos que, respectivamente, se refieren a los principios rectores generales (artículo 588 *bis* a), la solicitud de autorización judicial (artículo 588 *bis* b), la resolución judicial que acuerde la medida (artículo 588 *bis* c), el carácter secreto de las actuaciones (artículo 588 *bis* d), la duración de la medida (artículo 588 *bis* e), la solicitud de prórroga de la medida (artículo 588 *bis* f), las formas de control de la medida (artículo 588 *bis* g), la afectación a terceras personas (artículo 588 *bis* h), la posibilidad de utilizar la información obtenida en la ejecución de la medida en un procedimiento distinto, así como el tratamiento que deba darse a los descubrimientos casuales (artículo 588 *bis* i), el cese de la medida (artículo 588 *bis* j), y la destrucción de registros originales que se hubieran originado (artículo 588 *bis* k).

Al referirse a las medidas de investigación tecnológica, la doctrina entiende que "el denominador común a todas las diligencias reguladas en la Ley es la utilización de tecnología electrónica digital para la obtención de evidencias con valor probatorio en el proceso penal. Ello implica y supone la aptitud de esa tecnología para traducir las señales

[371] Y, por tanto, conforman el núcleo de nuestro objeto de estudio.

electrónicas digitales basadas en el álgebra de Boole (0 y 1) en lenguaje humano susceptible de ser entendido y valorado en los tribunales de Justicia."[372]

El artículo 588.bis.a.1 LECrim establece que, durante la instrucción de las causas, "[…] se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida". La importancia de que la reforma haya concretado en una norma de rango de ley los principios que deben inspirar la adopción y ejecución de las medidas de investigación tecnológica evidencia la potenciación del elemento jurisdiccional como compensatorio de la disminución que las otras garantías del Estado de derecho soportan en el campo de la prevención *ante delictum*, recordando el creciente papel garantista asumido por el poder judicial[373].

El resto de los apartados del artículo 588 *bis* a contiene una breve reseña de lo que implica cada uno de esos principios, aplicados de manera específica a la adopción y ejecución de este tipo de medidas.

En todo caso, hay que tener en cuenta que la redacción del artículo nace también de la normativa internacional aplicable y, particularmente, del CEDH. A este respecto, el artículo 8 del CEDH no establece un derecho a la intimidad absoluto, sino que prevé una serie de condiciones que, si se reúnen cumulativamente, podrían justificar una intromisión en dicho derecho. El TEDH, para comprobar si en los supuestos que llegan a su conocimiento se han satisfecho dichos requisitos, se plantea tres interrogantes: 1) si está la intromisión prevista en la ley; 2) si la intromisión persigue un objetivo legítimo; y 3) si la intromisión es necesaria en una sociedad democrática[374]. Este último requisito se conoce como como "test de proporcionalidad en sentido genérico", e incluye la verificación de la idoneidad, necesidad y proporcionalidad en sentido estricto[375].

---

[372] RICHARD GONZÁLEZ, M., "La investigación y prueba de hechos y dispositivos electrónicos", *Revista General de Derecho Procesal*, 43, 2017, Iustel.
[373] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 342.
[374] POOL, R. L. D.; CUSTERS, B. H. M., "The police hack back: legitimacy, necessity and privacy implicationis of the next step in fighting cybercrime", *European Journal of Crime, Criminal Law and Criminal Justice*, vol. 25, 2, 2017, Martinus Nijhoff Publishers.
[375] ALEXY, R., "Constitutional Rights, Balancing, and Rationality", *Ratio Juris*, vol. 16, 2, 2003.

A. PRINCIPIO DE ESPECIALIDAD

Respecto del principio de especialidad, el apartado segundo del artículo 588 *bis* a LECrim exige que la medida esté relacionada con la investigación de un delito concreto, sin que puedan autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva.

En ese sentido, lo que prohíbe el principio de especialidad es adoptar de manera prospectiva una medida de investigación, con la limitación de derechos fundamentales que ello implica. Lo contrario, en palabras de la sentencia del Tribunal Supremo núm. 393/2012, de 29 de mayo, "supondría conceder autorizaciones en blanco […] antes al contrario se precisa indicar el tipo delictivo que se está investigando que algunas veces puede incluso modificarse posteriormente, no por novación de dicho tipo sino por adición o suma de otras peculiaridades penales".

La sentencia del Tribunal Supremo núm. 272/2017, de 18 de abril, desarrolla tal principio cuando indica que "los poderes públicos no pueden inmiscuirse en la intimidad de los sospechosos, interceptando sus comunicaciones, con el exclusivo propósito u objeto de indagar a ciegas en su conducta, por lo que la decisión jurisdiccional de intervención de las comunicaciones telefónicas tiene que estar siempre relacionada con la investigación de un delito concreto al menos en el plano indiciario".

Esta prohibición de prospección implica, igualmente, una obligación de delimitación. Así, la sentencia del Tribunal Supremo núm. 195/2010, de 28 de enero, indica que la medida debe delimitarse objetivamente "a través de la precisión del hecho que se trata de investigar" y, subjetivamente, "mediante la suficiente identificación del sospechoso, vinculando con él las líneas telefónicas que se pretende intervenir", si bien la filiación subjetiva no implica que deba procederse a la identificación completa de los sujetos afectados, pero sí al menos que se indiquen "las señas o datos indiciarios que se puedan conocer en el momento de adopción de la medida".

Por otro lado, como indica la sentencia del Tribunal Supremo núm. 412/2011, de 11 de mayo, "el objeto del proceso no responde a una imagen fija. Antes, al contrario, se trata de un hecho de cristalización progresiva, con una delimitación objetiva y subjetiva que se verifica de forma paulatina, en función del resultado de las diligencias", por lo que no queda infringido el principio de especialidad cuando, en una diligencia de investigación válidamente adoptada, se descubre otro delito diferente del que justificó la adopción

de la medida, pues "si los hechos ocasionalmente conocidos no guardasen esa conexión con los causantes del acuerdo de la medida y aparentan una gravedad penal suficiente como para tolerar proporcionalmente su adopción, se estimarán como mera *notitia criminis* y se deducirá testimonio para que, siguiendo las normas de competencia territorial y en su caso las de reparto, se inicie el correspondiente proceso", según la sentencia del Tribunal Supremo núm. 71/2017, de 8 de febrero, que así alude a la figura del hallazgo casual, regulado en el artículo 579 *bis* LECrim.

Una de las conclusiones más directas que derivan de esta redacción es la prohibición de que las medidas de investigación tecnológicas se utilicen como instrumento de averiguaciones prospectivas sobre la conducta o el comportamiento de una persona u grupo de personas de las que no exista una base objetiva y razonable para sospechar de un individuo determinado[376]. En ese sentido, el principio de especialidad prohíbe las medidas de investigación tecnológica prospectivas sobre la conducta de una persona o grupo[377].

B. PRINCIPIO DE IDONEIDAD

Respecto del principio de idoneidad, el apartado tercero del artículo 588 *bis* a LECrim dispone que "servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad." Como se puede comprobar, el precepto se limita a describir su finalidad y no entra a definir el principio, pero el apartado segundo del artículo 588 *quater* b LECrim, referido a la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, contiene una breve referencia al mismo, al indicar que esas medidas solamente podrán autorizarse cuando "pueda racionalmente preverse que aportará datos esenciales y de relevancia probatoria para el esclarecimiento de los hechos y la identificación de su autor". Por su parte, el artículo 579.1 LECrim también podría contener una definición de la idoneidad, cuando establece que la medida podría acordarse "si hubiera indicios de obtener por estos medios el descubrimiento o la comprobación del algún hecho o circunstancia relevante para la causa"[378].

---

[376] DELGADO MARTÍN, J., "Investigación del entorno virtual", cit., p. 343.
[377] Así se ha sostenido, entre otras, en las SSTC 184/2003, de 23 de octubre, 261/2005, de 24 de octubre y las SSTS 695/2013, de 22 de julio; 689/2014, de 21 de octubre y 675/2015, de 10 de noviembre.
[378] "Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal.", fecha de consulta 22 abril 2020, en https://www.boe.es/diario_boe/txt.php?id=BOE–A–2019–4240.

En ese sentido, el Tribunal Supremo y el Tribunal Constitucional han señalado que la medida es idónea cuando: i) parece adecuada a los fines de la instrucción (SSTS 85/2017, de 15 de febrero, 993/2016, de 12 de enero de 2017); ii) permite seguir avanzando en la instrucción (STS 982/2016, de 11 de enero de 2017); iii) y es susceptible de conseguir el objetivo propuesto (STC 207/1996, de 16 de diciembre).

Por otro lado, la idoneidad forma parte de las tres exigencias del principio de proporcionalidad en sentido amplio: idoneidad de la medida, necesidad de la misma y juicio de proporcionalidad en sentido estricto (SSTC 173/2011, de 7 de noviembre y 115/2013, de 9 de mayo).

La aplicación de este principio determina que la resolución que lo acuerde debe valorar la aptitud potencial para la obtención de resultados relevantes tanto en atención al objeto y sujeto investigado como, en su caso, a la duración de la medida.

C. PRINCIPIO DE EXCEPCIONALIDAD Y NECESIDAD

Respecto de los principios de excepcionalidad y necesidad, el apartado cuarto del artículo 588 *bis* a) dispone que "solo podrá acordarse la medida: a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida." La idea detrás de esta regulación de supuestos alternativos ha sido la de prever escenarios excluyentes entre sí para que, en cualquiera de ellos, pueda entenderse justificado el cumplimiento de ambos principios.

A pesar de tratarse de dos principios que se abordan de manera diferenciada en el artículo, la doctrina suele analizarlos de manera conjunta, fundamentalmente porque el uno implica recíprocamente al otro. Por ese motivo los incluimos también aquí de manera conjunta. Toda medida de averiguación digital debe ser, en este sentido, la medida menos gravosa para los derechos fundamentales del investigado y, simultáneamente, la única que permita satisfacer con un resultado óptimo la finalidad de la actividad instructora. El principio de necesidad, por su parte, viene regulado en el artículo 8.2 CEDH, que prevé que la medida ha de ser necesaria en una sociedad democrática. También se prevé en el

artículo 52.1 CDFUE, que señala que solamente pueden limitarse los derechos fundamentales cuando sea estrictamente necesario.

La regulación conjunta que el legislador dispensa a ambos principios revela el vínculo que existe entre ellos, poniendo de manifiesto la íntima relación que guardan entre sí, en la que el principio de excepcionalidad hace las veces de criterio general, que es complementado por el principio de necesidad en la ponderación concreta de las medidas aplicables a cada caso particular[379].

De acuerdo con el Tribunal Constitucional, los principios de necesidad y excepcionalidad integran, junto con el de idoneidad, el test de proporcionalidad en sentido genérico, interactuando a modo "de esclusa del siguiente, de manera que la ausencia de cualquiera de ellos relevaría de la necesidad de examinar los restantes", según la STC 973/2013 de 21 de julio, STC 173/2011 de 7 de noviembre y 115/2013 de 9 de mayo. De este modo, primero hay que determinar que la medida es idónea para la obtención de resultados relevantes para la investigación, para después valorar si puede adoptarse otra medida menos gravosa de forma que se entienda como necesaria en el caso concreto. No está claro cuál sería el nivel que ocuparía en ese sistema de esclusas el principio de especialidad, aunque nosotros, en atención a un criterio sistemático y de gravedad de la injerencia, nos inclinamos por situarlo en primer lugar.

En cualquier caso, una vez superados estos filtros, ha de analizarse la proporcionalidad en sentido estricto. Vinculando esta regulación con la postura del TEDH, el triple juicio favorable supondrá el cumplimiento del requisito relativo a la necesidad de la medida en una sociedad democrática[380].

D. PRINCIPIO DE PROPORCIONALIDAD

El principio de proporcionalidad se prevé en el apartado quinto del artículo 588 *bis* a, al establecer que "las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los

[379] *Ibid.*

[380] Ilustran también el sentido de este principio la STS 104/2011, de 1 de marzo, cuando indica que este tipo de medidas suponen un sacrificio para un derecho fundamental, lo que determina que el recurso a las mismas deba ser excepcional y no rutinario, y la STS 279/2017, de 19 de abril, cuando indica que su adopción se justifica únicamente cuando no se alcanza otra línea de investigación ilícita.

intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho".

Sobre este principio, debemos destacar su importancia en la estructura jurídica sobre la que se asienta un Estado de Derecho, pues si los derechos fundamentales desde una perspectiva objetiva son aquellos "elementos esenciales del ordenamiento de una comunidad que determinan una obligación positiva del Estado de contribuir a su efectividad" (SSTC 25/1981, de 14 de julio, y 53/1985, de 11 de abril) y, desde una perspectiva subjetiva, conforman y garantizan un status jurídico en ámbitos de la existencia (STC 25/1981, de 14 de julio) que obliga a los poderes públicos a no lesionar la esfera individual que protegen, por lo menos la misma importancia tendrán aquellos mecanismos que, como el principio de proporcionalidad, sirven para mantener incólume su esencia jurídica en cuanto a su necesaria coexistencia con el propio ejercicio del poder público y las injerencias que del ejercicio del mismo puedan derivarse para los primeros.[381]

El *ius puniendi* del Estado no puede ejercitarse a cualquier precio, de acuerdo con la condición de valor superior del ordenamiento jurídico que tiene la libertad, según el artículo 1.1 CE. Conforme a lo anterior, hay que tener presente que el respeto a los derechos fundamentales exige que su sacrificio se adopte únicamente cuando resulte necesario para salvaguardar otro interés igualmente legítimo. Esto es el núcleo del principio de proporcionalidad, y es lo que comporta la exigencia de la motivación del auto decisorio[382].

Desde ese punto de vista, el principio de proporcionalidad despliega sus efectos en dos ámbitos diferenciados: frente al legislador, obligándole a ponderar las necesidades del *ius puniendi* frente a la necesidad del pleno respeto a los derechos fundamentales, concretando las injerencias que permitirá y bajo qué presupuestos podrán tener lugar; y frente al órgano jurisdiccional, que debe autorizar la injerencia específica, exigiendo que pondere de manera expresa ambas necesidades, de acuerdo con las circunstancias del caso concreto y atendiendo a que existan indicios de la comisión de un delito, a la idoneidad de la medida, y a su carácter necesario. Esta segunda vertiente es la que se ha dado en llamar "principio de proporcionalidad en sentido estricto", porque, como se ha indicado, "tiene como finalidad la determinación, mediante la utilización de las técnicas del

[381] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 342.
[382] *Ibid.*, p. 344.

contrapeso de los bienes o valores y la ponderación de intereses según las circunstancias del caso concreto, si el sacrificio de los intereses individuales que comporta la injerencia guarda una relación razonable o proporcionada con la importancia del interés estatal que se trata de salvaguardar"[383]. Así, este test de proporcionalidad en sentido estricto conforma, junto con los principios de idoneidad y necesidad, el test de proporcionalidad en sentido genérico, con el que se satisface el requisito de que la medida sea necesaria en un Estado democrático, uno de los tres elementos exigidos por el TEDH, junto con la persecución de un fin legítimo y la existencia de previsión suficiente en el ordenamiento jurídico de que se trate.

Desde un punto de vista sistemático, el precepto se estructura mediante una primera definición del principio de proporcionalidad, que exige valorar, por un lado, los derechos e intereses afectados por la medida –es decir, los de los implicados– y, por otro, el interés público y de terceros. A continuación, la norma establece los criterios sobre los que debe efectuarse la valoración del interés público: gravedad del hecho, trascendencia social o ámbito tecnológico de producción, intensidad de los indicios existentes y relevancia del resultado perseguido. Llama la atención que los dos primeros elementos (gravedad del hecho y trascendencia social o ámbito tecnológico) podrán concurrir a la vez o no, mientras que los otros dos (intensidad de los indicios y relevancia del resultado) es ineludible[384]. La resolución judicial que autorice la medida debería exteriorizar los criterios seguidos y la ponderación de intereses realizada.

En cuanto a la gravedad del hecho, la STC 299/2000, de 11 de diciembre, indica que la gravedad de la infracción punible no puede estar determinada únicamente por la calificación de la pena legalmente prevista (aunque, indudablemente, es un factor que debe ser considerado) sino que también deben tenerse en cuenta otros factores, como los bienes jurídicos protegidos y la relevancia social de aquella. Por otro lado, conforme a la STJUE de 2 de octubre de 2018, asunto C–207/16, la gravedad de la infracción debe valorarse también en relación a la concreta limitación del derecho fundamental que comporte la medida, ya que cuando la injerencia en el derecho no sea especialmente grave, el

[383] GONZÁLEZ–CUÉLLAR SERRANO, N., *Proporcionalidad y derechos fundamentales en el proceso penal*, Constitución y Leyes, COLEX, 1990, fecha de consulta 22 abril 2020, en https://dialnet.unirioja.es/servlet/libro?codigo=101185.

[384] "Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal.".

simple objetivo de prevenir, investigar, descubrir y perseguir infracciones que carezcan de especial gravedad puede ser justificación suficiente de la diligencia de investigación.

La trascendencia social del hecho investigado ya venía siendo considerada por la doctrina jurisprudencial[385]. Este indicador de proporcionalidad ha sido apreciado en delitos como el tráfico de drogas (STS nº 1241/2005, de 27 de octubre), los relativos a la prostitución (STS nº 1305/2004, de 3 de diciembre), contrabando (STS nº 457/1999, de 19 de junio), detención ilegal (STS nº 270/2008, de 13 de mayo), maquinaciones para alterar el precio de las cosas (STS nº 692/1997, de 7 de noviembre), falsedad en documento oficial en la que están involucrados funcionarios públicos (STS nº 529/1996, de 18 de julio), prevaricación (STS nº 308/2009, de 23 de marzo), revelación de secretos (STS nº 1898/2000, de 12 de diciembre), terrorismo (STS nº 985/2009, de 13 de octubre) o cohecho (STS nº 702/1997, de 20 de mayo). La comisión de delitos en el ámbito tecnológico aumenta la trascendencia social del hecho, como indica expresamente la STC 104/2006, de 3 de abril, al referirse a la potencialidad lesiva del uso de instrumentos informáticos para la comisión del delito. En todo caso, parece que la razón esencial de la introducción de este nuevo criterio reside en el hecho de que muchos de los delitos que se cometen en red solamente pueden ser investigados mediante diligencias de investigación informáticas.

La intensidad de los indicios existentes será utilizada para fundamentar la proporcionalidad de la medida, pues en función de la consistencia de dichos indicios podrá calibrarse el nivel de desarrollo de la conducta delictiva y la participación del investigado en la misma. La Fiscalía General del Estado señala la pertinencia de velar en estos supuestos por que los indicios de mayor intensidad permitan un análisis más ponderado sobre el grado de injerencia en el derecho fundamental de que se trate, sin caer en una suerte de condena prematura[386].

La relevancia del resultado perseguido con la restricción del derecho fundamental tiene que relacionarse con los principios de idoneidad y necesidad, conformando la proporcionalidad en sentido estricto. Englobará tanto la incidencia del descubrimiento en la integración y prueba de la correspondiente figura delictiva como el efecto de la medida

[385] SSTS nº 1241/2005, de 27 de octubre, 1078/2001, de 8 de junio y 900/2000, de 28 de julio, entre otras
[386] "Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal.".

en el restablecimiento de la paz social, perturbada por el delito. En todo, caso, como indica la STC 123/2002, de 20 de mayo "nuestra Constitución exige que toda limitación de un derecho fundamental esté prevista en la ley (art. 53.1 CE) y que dicha limitación sea adecuada a las exigencias derivadas del principio de proporcionalidad, esto es, necesaria para alcanzar un fin legítimo, proporcionada al efecto y, en todo caso, respetuosa del contenido esencial del derecho (por todas, SSTC 181/1995, de 11 de diciembre, FJ 5)".

Como indicaba la STC 115/2013, "el acceso policial limitado a los datos recogidos en el archivo electrónico o agenda de contactos telefónicos de un terminal móvil —sin afectar al registro de llamadas entrantes y salientes, ni a ningún otro archivo o enlace que pudiera contener el terminal móvil— constituye una injerencia en el derecho a la intimidad personal (artículo 18.1 CE), al igual que lo es la apertura de una agenda en soporte de papel y la lectura de los papeles encontrados en ella (STC 70/2002, FJ 9), pues la agenda de contactos telefónicos contenida en un teléfono móvil (entendiendo por tal el archivo elaborado por el titular de dicho teléfono que, como también ya hemos dicho, recoge una relación de números telefónicos identificados habitualmente mediante un nombre) ofrece información que pertenece al ámbito privado de su titular, siendo aplicable nuestra doctrina según la cual el artículo 18.1 CE garantiza al individuo un ámbito reservado de su vida "vedando que terceros, sean particulares o poderes públicos, decidan cuales sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio" (SSTC 127/2003, de 30 de junio, FJ 7 y 89/2006, de 27 de marzo, FJ 5, entre otras). La protección de ese ámbito reservado confiere a la persona, así, el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido (SSTC 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 5; 70/2009, de 23 de marzo, FJ 2; y 241/2012, FJ 3, entre otras muchas)."

2. POSIBILIDADES DE INVESTIGACIÓN TECNOLÓGICA AUTÓNOMA

En este apartado nos referiremos a los poderes de investigación autónomos –en tanto que no precisan de autorización judicial– que han sido conferidos por el legislador a la Policía Judicial con ocasión de la reforma operada por la LO 13/2015, y que se encuentran recogidos en los ya mencionados artículos 588 *ter* k), 588 *ter* l) y 588 *ter* m) LECrim.

En el estudio de estas facultades de investigación autónomas, debemos comenzar recordando que la investigación de los hechos delictivos en el medio virtual, tengan la consideración de ciberdelincuencia o no, exige un elevado nivel de conocimientos técnicos de quienes la ejerciten. Por ello, en la mayoría de las ocasiones, son los grupos especializados de los poderes de investigación los que deben asumir la averiguación material de los hechos, determinando la autoría y circunstancias de los delitos, y procediendo a la recogida de los efectos, instrumentos y pruebas de los mismos.

Del mismo modo, ha de tenerse presente que la restricción de los derechos fundamentales a la inviolabilidad del domicilio y el secreto de las comunicaciones precisa, en todo caso, de control judicial[387]. Igualmente, hemos de partir de la obligación que tienen los órganos investigadores de trasladar al juez instructor los avances de su investigación.

Sin embargo, habida cuenta de la singularidad del delito informático, se han elevado voces desde la doctrina[388] que reclaman la conveniencia de que se concedan mayores facultades a los investigadores policiales, en aras de dotarles de la agilidad suficiente en sus labores de investigación, lo que además supondría otorgar refrendo legal a lo que, en realidad, parece constituir la auténtica práctica judicial[389]. Ello pasaría por una ampliación de sus habilitaciones legales, incluyéndose aquellos supuestos en los que el derecho fundamental quedara afectado sólo tangencialmente. De este modo, parece que la figura del juez de instrucción quedaría asimilada a un juez de garantías, si bien falta por concretar el modo en que ello se articularía. En este aspecto, podría resultar especialmente interesante la estructura orgánica prevista en el anteproyecto de LECrim de 2020, con la figura de un juez de garantías y de una audiencia preliminar previa a la fase de enjuiciamiento que depure el procedimiento de cualquier vulneración de derechos fundamentales que haya podido tener lugar.

Por último, conviene también recordar que estas capacidades de investigación tecnológica que ahora vamos a estudiar deben acordarse en el marco de un proceso penal debidamente incoado.

---

[387] No sucede lo mismo con el derecho a la intimidad, que puede ser restringido policialmente en determinar circunstancias (SSTC 98/2000, de 10 de abril, FJ 5; 156/2001, de 2 de julio, FJ 4; 70/2009, de 23 de marzo, FJ 3).

[388] CALVO LÓPEZ, D., "Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (apartados K) a M) del art. 588 ter de la LECrim)", cit., p. 11.

[389] MORENO CATENA, V. M., "El mito de la instrucción dirigida por el juez", cit, p. 4.

A. IDENTIFICACIÓN DE TITULARES MEDIANTE NÚMERO IP

El artículo 588 *ter* k LECrim dispone que *"*cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo utilizada para la comisión algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el artículo 588 *ter* e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso.*"*

Como se puede apreciar, la propia redacción del artículo no se refiere en sentido expreso a la actividad de obtención de direcciones IP asociadas a una conexión cibernética, sino que, dando ello por sentado, regula la necesidad de que la Policía Judicial deba solicitar a la autoridad judicial que requiera a las entidades obligadas a colaborar los datos necesarios para identificar y localizar al terminal y su usuario[390].

Esta medida de investigación en particular será estudiada con ocasión del deber de colaboración que nos ocupa en el capítulo IV de esta tesis, pero lo que sí está claro es que el artículo se desenvuelve sobre la base lógica de que la Policía Judicial haya obtenido, sin necesidad de autorización judicial, la dirección IP objeto de investigación.[391] Como recuerda la Fiscalía General del Estado[392], En realidad, lo que prescribe el precepto es que la Policía Judicial no necesita autorización judicial para determinar la dirección IP si puede hacerlo sin recurrir al operador de comunicaciones electrónicas obligado por la Ley 25/2007 (obteniéndola directamente de Internet, si fuere posible); para lo que sí la necesitará será para relacionar esa dirección IP con un equipo o dispositivo concreto y, en último término, con la persona usuaria del mismo. El fundamento de esta previsión se encuentra en que la dirección IP, por sí sola, no identifica a persona alguna. Su operatividad se pone de manifiesto, únicamente, cuando se interrelaciona esa dirección IP con

---

[390] BARRIO ANDRÉS, M., *Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 264.
[391] CALVO LÓPEZ, D., "Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (apartados K) a M) del art. 588 ter de la LECrim)", cit., p. 12.
[392] "Circular 2/2019, de 6 de marzo, de la Fiscal General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas.", p. 2.

ciertos datos de identidad conservados por las operadoras de comunicaciones. Es decir, la dirección IP no identifica, pero permite identificar; por lo tanto, su obtención no resultaría extraña a las labores policiales que regula el art. 22.2 de la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (vigente conforme a la disposición transitoria de la Ley Orgánica 3/2018, de 5 de diciembre), que permite la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas, pero la identificación final del usuario mediante el cruce de ese dato con los conservados por imposición de la Ley 25/2007, sí precisará de esa autorización judicial.

El precepto, por tanto, incorpora a la LECrim la doctrina jurisprudencial elaborada por el Tribunal Supremo en los últimos años según la cual la dirección IP no está protegida por el artículo 18.1CE ni por el artículo 18.3 CE[393].

En todo caso, merece la pena mantener en consideración que en los casos en que para acceder a una IP sea necesario oficiar a una operadora será necesario obtener autorización judicial.

B. IDENTIFICACIÓN DE TERMINALES MEDIANTE CAPTACIÓN DE CÓDIGOS

a) Concepto de IMSI, IMEI y MAC

En primer lugar, quisiéramos destacar que los números IMSI o IMEI se incluyen en el conjunto de códigos de identificación aptos para identificar al equipo de comunicación utilizado (como puede ser el PIN de acceso a un teléfono Blackberry, de conformidad con las STS 967/2016, de 21 de diciembre, y 551/2016, de 22 de junio[394]). No obstante, dada su amplia utilización, resulta necesario comenzar por su definición.

De esta manera, el IMEI, o *International Mobile Equipement Identity*, es un código único utilizado para identificar terminales móviles incluidos en el estándar 3GPP[395] (redes GSM, UMTS, LTE y 5G), de manera que permite reconocerlos y, en caso de necesidad, bloquearlos en la red correspondiente. Es un código que generalmente se

[393] SSTS 292/2008, de 28 de mayo; y 776/2008, de 18 de noviembre.
[394] CALVO LÓPEZ, D., "Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (apartados K) a M) del art. 588 ter de la LECrim)", cit., p. 21.
[395] "About 3GPP Home", fecha de consulta 15 abril 2020, en https://www.3gpp.org/about–3gpp/about–3gpp.

encuentra dentro de los componentes del equipo, como el número de bastidor de un vehículo, y no depende de la tarjeta SIM que tenga introducida. Su estructura viene establecida por el estándar 3GPP[396]. Interesa destacar, sin embargo, que es perfectamente posible modificar el IMEI de un teléfono, por lo que el efecto bloqueador del dispositivo queda difuminado en la práctica[397].

El IMSI, o *International Mobile Subscriber Identity*, por su parte, siendo también un código único, en vez de identificar al terminal móvil, lo que señala es el abonado de una línea de comunicación móvil determinada, al estar integrado en el módulo de identificación del usuario, o *Subscriber Identity Module*[398]. No debe confundirse con el ICCID, que es el número de serie de la propia tarjeta SIM o e–SIM, en su caso.

Por su parte, la dirección MAC es un identificador de 48 bits que corresponde de forma única e individualizada a una tarjeta o dispositivo de red incluida dentro del terminal, cuya identidad es única para cada dispositivo a nivel mundial y constituyen una huella digital que permite determinar desde qué interfaz de red se ha emitido un determinado paquete de datos.

La averiguación de esos códigos utilizando medios tecnológicos posibilita la identificación del número de teléfono que emplea el sujeto investigado e, incluso, su geolocalización en un punto geográfico relativamente preciso, desde el que esté efectuando la llamada[399].

No obstante, como señala RODRÍGUEZ LAÍNZ, "la técnica policial ha derivado esencialmente al empleo de apartados diseñados no para captar el número IMSI al hilo del transcurso de una comunicación, sino como auténticos señuelos que generan un diálogo automático con el terminal, al ser identificado el aparato como una nueva célula radio con la que interconectar a los efectos de la siguiente llamada entrante o saliente. No se capta una comunicación en curso, pero se genera un diálogo entre artefactos

---

[396] "Specification # 23.003", fecha de consulta 15 abril 2020, en https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729.
[397] CALVO LÓPEZ, D., "Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (apartados K) a M) del art. 588 ter de la LECrim)", cit., p. 21.
[398] "E.212 : The international identification plan for public networks and subscriptions", fecha de consulta 15 abril 2020, en https://www.itu.int/rec/T–REC–E.212.
[399] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 452.

electrónicos que en sí mismo es una comunicación *"*[400]. Son los llamados *IMSI–catchers*, que simulan una antena que opera de puente entre la antena del operador y el dispositivo a investigar.

Desde el punto de vista de su funcionamiento, consiste en un dispositivo que simula ser una torre de radio del ISP de turno frente al terminal que se conecta, cuando en realidad actúa como intermediario entre el dispositivo que sirve de objetivo y las torres de radio verdaderas del proveedor de servicios. Es considerado, por tanto, un tipo de actuación *man–in–the–middle*[401].

Uno de los modelos más conocidos de este tipo de dispositivos son los llamados *StingRay*, que son *IMSI–catchers* creados por *Harris Corporation*, inicialmente desarrollados para uso militar y posteriormente extendidos en el uso policial local en Estados Unidos y Reino Unido.

Esta operativa se realiza en diversas ubicaciones relacionadas con el investigado, y luego se entrecruzan para descartar lo que corresponda a otros terminales que, accidentalmente, se hubieran acercado al escáner.[402] A ese respecto, debe recordarse que, aunque el artículo 588 *ter* l no exige autorización judicial para averiguar el IMSI o IMEI de un terminal móvil, no por ello quiere decir que deje de estar sometida a los principios generales previstos en el artículo 588 *bis* a. No en vano, el artículo se refiere hasta en dos ocasiones a una investigación concreta que se esté llevando a cabo. Desde luego, la ausencia de validación judicial *a posteriori* plantea dudas sobre el efectivo control de la actuación policial en estos casos.

Debe tenerse en cuenta, no obstante, que la falta de exigencia de autorización judicial deriva del extendido conocimiento de que los dispositivos utilizados para averiguar estos identificadores no acceden al contenido de las comunicaciones. Sin embargo, resulta de gran importancia destacar que ocurre más bien lo contrario, pues los *IMSI catchers* pueden acceder al contenido de dichas comunicaciones, afectar a la cobertura del aparato,

---

[400] RODRÍGUEZ LAINZ, J. L., "Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas", cit.

[401] SHAIK, A.; BORGAONKAR, R.; ASOKAN, N.; NIEMI, V.; SEIFERT, J.–P., "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems", *arXiv:1510.07563 [cs]*, 2015, fecha de consulta 19 enero 2021, en http://arxiv.org/abs/1510.07563.

[402] CALVO LÓPEZ, D., "Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (apartados K) a M) del art. 588 ter de la LECrim)", cit., p. 23.

así como a los metadatos, claves de cifrados, datos de geolocalización e, incluso, escribir y acceder datos sobre la memoria del terminal móvil interceptado[403]. Una vez más, se pone de manifiesto la gran problemática intrínseca a esta materia: la inmensa capacidad de actuación policial frente al desconocimiento por parte del investigado de las actuaciones de que está siendo objeto[404]. En este sentido, adelantamos aquí una de nuestras conclusiones, como es la necesidad de que el ordenamiento jurídico dispense a los ciudadanos de a pie las garantías que estos no pueden procurarse por sí mismos, a través de la imposición de obligaciones de acreditación de procedimientos y legalidad a la Policía Judicial.

En todo caso, lo que está claro es que ambos códigos resultan fundamentales para identificar al usuario del dispositivo móvil, en la medida en que aparecen en toda conexión que tenga lugar entre el terminal y la red de telefonía móvil. Su utilidad es reconocida por la doctrina sin reservas[405], pues permite avanzar no sólo en la investigación de los *ciberdelito*s, sino también en la de los delitos tradicionales

b) Práctica de la diligencia

Esta medida de investigación se prevé en el artículo 588 *ter* l LECrim, que dispone que "1. Siempre que en el marco de una investigación no hubiera sido posible obtener un determinado número de abonado y este resulte indispensable a los fines de la investigación, los agentes de Policía Judicial podrán valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, tales como la numeración IMSI o IMEI y, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones. 2. Una vez obtenidos los códigos que permiten la identificación del aparato o de alguno de sus componentes, los agentes de la Policía Judicial podrán solicitar del juez competente la intervención de las comunicaciones en los términos establecidos en el artículo 588 *ter* d. La solicitud habrá de poner en conocimiento del órgano jurisdiccional la utilización de los artificios a que se refiere el

[403] BARRIO ANDRÉS, M., *Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 265.
[404] Dejando a salvo las excepciones en que un individuo disponga de un alto grado de conocimientos técnicos, muy superior a la media.
[405] CALVO LÓPEZ, D., "Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (apartados K) a M) del art. 588 ter de la LECrim)", cit., p. 22.

apartado anterior. El tribunal dictará resolución motivada concediendo o denegando la solicitud de intervención en el plazo establecido en el artículo 588 *bis* c."

Al contrario de lo que sucedía en el caso de la obtención de direcciones IP, esta medida de investigación queda expresamente prevista en la dicción del artículo, que plasma la doctrina del Tribunal Supremo contenida, entre otras, en la STS 249/2008, de 20 de mayo de 2008.

Como es sabido, la sentencia referida analizaba la naturaleza del IMSI y se planteaba si debía ser encuadrado dentro de la esfera de especial protección del artículo 18.3 CE cuando era captado por agentes policiales sin la preceptiva autorización judicial. Concluía, a este respecto, que la autorización judicial sería necesaria, pero exclusivamente para la cesión del IMSI por las operadoras, mientras que su obtención autónoma por la policía no afectaría al secreto de las comunicaciones, considerando que, además, estaba suficientemente prevista en el ordenamiento jurídico. En concreto, disponía que "La primera idea que sugiere la lectura de la Ley 25/2007 es que sus preceptos se centran en ofrecer un casuístico régimen jurídico de la conservación y cesión por las operadoras de los datos relativos a las comunicaciones electrónicas –en nuestro caso, del IMSI–, pero no aborda la regulación de su recogida por las Fuerzas y Cuerpos de Seguridad del Estado, no desde los ficheros automatizados que obran en poder de los prestadores de servicio, sino desde el propio teléfono celular. Cobra todo su significado el régimen jurídico del acceso a los ficheros contemplado por la LO 15/1999, 13 de diciembre, de protección de datos.

Frente al silencio de la nueva regulación, esta ley dispone que "la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad (artículo 22.2). Además, «la recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las

pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales" (artículo 22.3).”

El argumento esgrimido principalmente era que el IMSI, por sí solo, no proporciona una información que permita averiguar la identidad de los comunicantes, la titularidad del teléfono móvil o cualquier otra circunstancia que pudiera quedar protegida por el artículo 18.3 CE. En particular, concluía que “para que la numeración IMSI brinde a los investigadores toda la información que alberga, es preciso que esa serie numérica se ponga en relación con otros datos que obran en poder del operador. Y es entonces cuando las garantías propias del derecho a la autodeterminación informativa o, lo que es lo mismo, del derecho a controlar la información que sobre cada uno de nosotros obra en poder de terceros, adquieren pleno significado. Los mismos agentes de Policía que hayan logrado la captación del IMSI en el marco de la investigación criminal, habrán de solicitar autorización judicial para que la operadora correspondiente ceda en su favor otros datos que, debidamente tratados, permitirán obtener información singularmente valiosa para la investigación. En definitiva, así como la recogida o captación técnica del IMSI no necesita autorización judicial, sin embargo, la obtención de su plena funcionalidad, mediante la cesión de los datos que obran en los ficheros de la operadora, sí impondrá el control jurisdiccional de su procedencia.”

c) Derechos fundamentales afectados

No es pacífica la cuestión acerca de si el código IMSI o el código IMEI deben tener la consideración de datos externos a la comunicación, en la medida en que no permiten conocer, por sí mismos, ninguno de los aspectos externos de la comunicación a que se refiere la doctrina del TEDH[406]. Si se entendiera generado cuando esta se produce, su averiguación afectaría al derecho fundamental al secreto de las comunicaciones[407].

La jurisprudencia emanada del TS en los últimos años consolida la tesis de que el empleo policial de una herramienta de escaneado o barrido electrónico en un radio de acción determinado para identificar los números de IMSI o IMEI utilizados no afecta al secreto de las comunicaciones, por lo que no sería precisa la autorización judicial (SSTS

[406] VEGAS TORRES, J., “Obtención de pruebas en ordenadores personales y derechos fundamentales en el ámbito de la empresa”, 2011, Cátedra de Investigación Financiera y Forense KPMG–URJC, p. 47, fecha de consulta 24 marzo 2020, en https://eciencia.urjc.es/handle/10115/5881.
[407] SÁNCHEZ SISCART, J. M., “A vueltas con el secreto de las comunicaciones: Algunos supuestos críticos en la jurisprudencia de la Sala 2.ª del Tribunal Supremo”, *Diario La Ley*, 7338, 2010, Wolters Kluwer.

de 8 de junio de 2016, de 18 de diciembre de 2008, de 18 de noviembre de 2008, de 8 de octubre de 2008 y de 20 de mayo de 2008)[408].

A ese respecto, la STS 185/2011, de 1 de marzo, afirmaba que *"*no constituye una irregularidad pues ese número al que la policía pudiera acceder a través de sistemas de detección no implica Guna afectación al contenido de las comunicaciones, ni la identificación de las personas que estaban en la comunicación, ni tan siquiera el número de los terminales móviles empleados en la comunicación". En el mismo sentido, la STS 492/2016, de 8 de junio, concluye que "en modo alguno afecta al derecho al secreto de las comunicaciones eventualmente realizadas o de futura realización a través de dicho equipo. Y ni siquiera puede decirse que la intimidad de la persona en cuyo poder es habido el equipo, cuyo IMEI se desvela, tiene más afectación que la de poner de manifiesto la posesión del aparato." A tal efecto, la STS 249/2008, de 20 de mayo, afirmaba que el carácter de datos externos de la comunicación protegidos por el secreto de comunicaciones "habría de predicarse, actualizando la pauta interpretativa ofrecida por el TEDH, de los datos indicativos del origen y del destino de la comunicación, del momento y duración de la misma y, por último, los referentes al volumen de la información transmitida y el tipo de comunicación entablada. Y la información albergada en la serie IMSI, desde luego, no participa de ninguna de estas características".

En definitiva, la jurisprudencia viene entendiendo que determinar el IMEI o IMSI de un dispositivo o de una tarjeta SIM no afecta al derecho fundamental al secreto de las comunicaciones porque esa información, por sí sola, no permite obtener la identidad de los sujetos que intervinieren en la comunicación.[409] Ahora bien, para lo que sí viene exigiendo la jurisprudencia autorización judicial es para identificar los números comerciales de teléfono que corresponda a un determinado IMEI o IMSI, así como sus titulares. A tal efecto, se ha reflexionado que el acceso al IMEI o IMSI se trata "de un dato electrónico que, en la medida en que permite, mediante su interrelación con otros datos tratados por las operadoras, la identificación de quien hasta ese momento sólo aparece como identificable, ha de ajustarse al régimen general de tutela dispensado por la legislación en materia de protección de datos"[410]. En tal sentido, la precitada STS 249/2008, de 20 de mayo,

---

[408] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 452.
[409] *Ibid.*
[410] MARCHENA GÓMEZ, M., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Ediciones Jurídicas Castillo de Luna, Madrid, 2015, p. 325.

también reconocía que "para que la numeración IMSI brinde a los investigadores toda la información que alberga, es preciso que esa serie numérica se ponga en relación con otros datos que obran en poder del operador. Y es entonces cuando las garantías propias del derecho a la autodeterminación informativa, o lo que es lo mismo, del derecho a controlar la información que sobre cada uno de nosotros obra en poder de terceros, adquieren pleno significado."

d) Modalidades de actuación

Los artículos 588 *ter* l) y siguientes LECrim regulan varios supuestos en la materia; la doctrina[411] los ha venido sistematizando en tres categorías diferenciadas.

Por un lado, se distingue la utilización de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación de etiquetas técnicas del apartado de telecomunicación o de alguno de sus componentes, tales como la numeración IMSI o IMEI y, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones. Estas medidas pueden ser dispuestas por la policía judicial sin necesidad de previa autorización judicial. Están previstas en el artículo 588 *ter* l) LECrim que, por tanto, desjudicializa la obtención de los datos identificativos del equipo de comunicación siempre que se efectúe por los propios medios policiales (como el *IMSI–Catcher*) y sin acudir a los datos conservados por las operadoras[412]. Como ejemplo de lo expuesto, puede estarse a lo dispuesto en la STS 342/2013, de 17 de abril.

Por otro lado, y en relación con la importancia de los códigos referidos, se distingue también la intervención de las comunicaciones, que tiene lugar una vez obtenidos los datos que permiten la identificación del apartado o de alguno de sus componentes. Esta medida solamente puede realizarse previa autorización judicial en los términos establecidos en el artículo 588 *ter* d), teniendo que indicarse en la solicitud cursada al órgano jurisdiccional qué artificios se hayan utilizado para obtener los números IMEI o IMSI. El tribunal deberá dictar resolución motivada concediendo o denegando la autorización del

---

[411] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 454.
[412] GUDIN RODRÍGUEZ–MAGARIÑOS, F., "Obtención de los códigos de identidad del teléfono móvil y del abonado (IMEI/IMSI): crónica de un caos normativo", fecha de consulta 25 marzo 2020, en https://www.sepin.es/nuevas–tecnologias/verDoc.asp?referencia=SP%2FDOCT%2F19788&imprimir=1&cod=01–08f17U0Gz05u1eq0%2650Hu1vk0G–0GA1dG00–0HF1%3DO29H0H517U1Cl09P1AZ1iI08U1Mq0H90JP1Jn0ml0I01LI01c#24076548.

a medida conforme al artículo 588 *bis* c. De esta manera, la medida de intervención de las comunicaciones queda sometida al régimen general de los artículos 588 *bis* a) y siguientes LECrim, pero añadiéndose la especialidad de que la solicitud policial deba "poner en conocimiento del órgano jurisdiccional la utilización de los artificios" que se haya utilizado para obtener los datos identificativos del equipo de comunicación. Sobre esta exigencia, contenida en el artículo 588 *ter* l) 2 LECrim, se ha dicho que no es suficiente con que simplemente la Policía Judicial ponga en conocimiento del Juzgado la utilización de dichos medios técnicos, sino que "habrá de extenderse a la exposición de las razones por las que se ha acudido a la utilización de los artificios técnicos", todo ello para "motivar las razones que hayan podido justificar la invasión del derecho a la protección de datos del artículo 18.4 CE".[413]

Por último, se distingue el acceso a la titularidad de un número de teléfono o de cualquier otro medio de comunicación, y el acceso al número de teléfono o los datos identificativos de cualquier medio de comunicación. En estos supuestos el Ministerio Fiscal y la Policía Judicial pueden dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, y estos estarán obligados a cumplir dicho requerimiento bajo apercibimiento de incurrir en delito de desobediencia. A esto último se refiere el artículo 588 *ter* m) LECrim cuando indica que "cuando, en el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia".

Respecto de esta última modalidad, a pesar de que el régimen general exige autorización judicial para acceder a los datos conservados por las operadoras en cumplimiento de las funciones establecidas en la Ley 25/2007, el Ministerio Fiscal o la Policía Judicial puede solicitar la cesión de los datos concernientes a la titularidad o identificación de un

[413] MARCHENA GÓMEZ, M., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, cit., p. 312.

dispositivo sin necesidad de previa autorización, al no afectar al secreto de comunicaciones por no ser datos vinculados a un proceso de comunicación[414].

C. IDENTIFICACIÓN DE TITULARES O TERMINALES O DISPOSITIVOS DE CONECTIVIDAD

La última de las posibilidades de investigación autónoma previstas en nuestro ordenamiento jurídico es la diligencia de identificación de titulares, terminales o dispositivos de conectividad, prevista en el artículo 588 *ter* m LECrim, que a tal efecto establece que "Cuando, en el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia."

Se trata, en realidad, de un supuesto de cesión de datos concernientes a la titularidad o identificación de un dispositivo electrónico –desvinculados de los procesos de comunicación– a favor del Ministerio Fiscal o de la Policía, sin necesidad de autorización judicial, tal y como expone la LO 13/2015 en su exposición de motivos[415].

Esta diligencia de investigación es la que dota de verdadero contenido a las otras dos estudiadas. Si las otras dos medidas permiten identificar a terminales móviles de conexión, la que ahora estudiamos es la que permite convertir dicho conocimiento en una información útil en la investigación del proceso penal. Ello es así porque, en muchas ocasiones, y con independencia del delito cometido, el punto de partida de la investigación suele ser un teléfono móvil, y a través de esta diligencia es posible averiguar su verdadero titular y, así, por ejemplo, conocer el resto de las líneas de teléfono que tuviera contratadas[416].

En el marco de esta diligencia de investigación se ha venido planteando cierta problemática entre la Policía Judicial y el Ministerio Fiscal, por un lado, y los prestadores

---

[414] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 456.
[415] CALVO LÓPEZ, D., "Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (apartados K) a M) del art. 588 ter de la LECrim)", cit., p. 25.
[416] *Ibid.*

de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, por otro. Esta controversia tiene su origen en el artículo 3 LDCE, que los incluye entre los datos objeto de conservación. A su vez, el artículo 6 LDCE establece que dichos datos "sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial". Este precepto, en vigor con anterioridad a la reforma de la LECrim de 2015, determinó que nuestros tribunales entendieran ya en 2010 que era "necesaria la autorización judicial para que los operadores que prestan servicios de comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo"[417].

La problemática surge cuando los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, al recibir las solicitudes de la Policía o del Ministerio Fiscal con base en el artículo 588 *ter* m LECrim, se niegan a facilitarlos aduciendo que, con base en los artículos 3 y 6 LDCE, es necesaria autorización judicial para ello. Generalmente, se considera que la aparente contradicción entre el artículo 588 *ter* m LECrim y el artículo 6 LDCE debe resolverse, en este particular caso, a favor de la primera, por aplicación del criterio *lex posterior derogat anterior*[418].

Otros autores, alcanzando la misma conclusión, consideran que el supuesto del artículo 588 *ter* debe equipararse a aquellos casos en los que para obtener un número de teléfono o identificar a su titular, un particular acudía a las guías telefónicas o la Policía se dirigía a las compañías para que le facilitara esa información, limitada siempre al conocimiento de la titularidad del número de teléfono o del medio de comunicación en concreto, pero sin referirse en ningún momento a los datos de tráfico de un determinado proceso de comunicación[419]. Por último, hay quien apunta que el artículo 588 *ter* m LECrim, aunque no se refiere a datos vinculados a un proceso de comunicación, sí se refiere a datos de carácter personal, por lo que afecta el derecho fundamental del artículo 18.4 CE aunque no afecte al derecho al secreto de las comunicaciones y, en consecuencia, la

---

[417] "Acuerdo del 23 de febrero de 2010, sobre la necesidad de autorización judicial para la cesión de datos de las operadoras de comunicaciones", fecha de consulta 16 enero 2021, en https://www.poderjudicial.es/cgpj/es/Poder–Judicial/Tribunal–Supremo/Jurisprudencia–/Acuerdos–de–Sala/Acuerdo–del–23–de–febrero–de–2010—sobre–la–necesidad–de–autorizacion–judicial–para–la–cesion–de–datos–de–las–operadoras–de–comunicaciones.

[418] BARRIO ANDRÉS, M., *Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 268.

[419] QUEVEDO GONZÁLEZ, J., *Investigación y prueba del ciberdelito*, cit., p. 140.

falta de necesidad de autorización judicial constituye una auténtica excepción al régimen general[420].

A este respecto, la Fiscalía de Criminalidad Informática emitió un informe en el que analizaba si dicha postura era sostenible o si, por el contrario, rayaba en la comisión de un delito de desobediencia. En él, concluyó que tanto el IMEI como el IMSI deben catalogarse como "datos de abonados" cuando se obtengan de forma desvinculada de un proceso comunicativo y que, por tanto, deben entregarse obligatoriamente por las operadoras de internet a la fuerza instructora, pues "la forma en que los operadores de comunicaciones decidan controlar/almacenar es datos no podría suponer, en ningún caso, una modificación del régimen jurídico aplicable a los mismos y en consecuencia de las condiciones para su obtención hasta el punto de que esa circunstancia determine la necesidad de la previa autorización judicial"[421].

La Circular 2/2019, de 6 de marzo, de la Fiscal General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas, contiene interesantes pronunciamientos al respecto de esta modalidad de diligencia de investigación que tampoco debemos pasar por alto.

Para empezar, la propia Circular declara que los datos a los que se refiere el artículo 588 *ter* m LECrim no afectan al derecho fundamental al secreto de las comunicaciones, pero no se pronuncia en relación el derecho fundamental del artículo 18.4 CE.

Asimismo, reconoce que la justificación de esta medida subyace en dotar al Ministerio Fiscal y a la Policía Judicial de una mayor operatividad y agilidad en las investigaciones.

En cuanto a la utilidad de esta medida de investigación, la Circular declara que la obtención de los datos resulta completamente extraña a la interceptación de comunicaciones. Es más, la gran mayoría de los casos en los que el Ministerio Fiscal o la Policía Judicial pudieran hacer uso de esta facultad podrían no tener relación, ni siquiera, con la preparación de una ulterior intervención de comunicaciones. En consecuencia, entiende que esa facultad no debe entenderse circunscrita a los supuestos de interceptación de

---

[420] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 456.
[421] CALVO LÓPEZ, D., "Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (apartados K) a M) del art. 588 ter de la LECrim)", cit., p. 28.

comunicaciones que contempla el art. 588 *ter* a LECrim. Asimismo, recuerda que la STJUE de 2 de octubre de 2018 (asunto C–207/16) ha proclamado que, si bien la obtención de estos datos constituye una injerencia en los derechos fundamentales de los ciudadanos, no reviste la gravedad suficiente como para limitarla a la lucha contra la delincuencia grave, estando justificada "por el objetivo de prevenir, investigar, descubrir y perseguir delitos en general".

En cuanto a los concretos datos que pueden ser recabados directamente por el Ministerio Fiscal o por la Policía Judicial, la Circular afirma que la previsión no se agota en la obtención de la titularidad de un número de teléfono o, en sentido inverso, en la obtención del concreto número telefónico que utilice una persona, sino que debe entenderse incluida cualquier petición de datos encaminada a esa identificación del titular o del dispositivo de comunicación, siempre que no se trate de datos vinculados a procesos de comunicación, como puede ser el IMSI, apuntando que no puede ser considerado como un dato de tráfico y, por lo tanto, vinculado a un proceso de comunicación, pues no se genera como consecuencia de una comunicación concreta, sino que se trata, en palabras de la STS n.º 249/2008, de 20 de mayo, de un código de identificación de cada dispositivo de telefonía móvil que sirve para posibilitar esa identificación a través de las redes GSM y UMTS.

En cuanto a la delimitación subjetiva, la Circular destaca que el precepto no limita el posible destinatario de la solicitud a los operadores obligados por la Ley 25/2007, sino que, por el contrario, se refiere de manera genérica a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información

Al margen de lo anterior, existen otros supuestos en los que se plantean controversias en relación con este tipo de medidas de investigación, como el acceso a las claves PIN de las tarjetas SIM, la obtención de listados de llamadas, el acceso a los mensajes de un teléfono móvil y el acceso a la agenda de contactos de un teléfono móvil.

En cuanto al PIN del teléfono móvil, los tribunales vienen entendiendo que acceder al mismo no exige autorización judicial, por tratarse de un elemento similar al IMSI o IMEI[422]. En tal sentido, las SSTS, Sala 2ª, de 4 de abril de 2017 y de 22 de junio de

[422] BARRIO ANDRÉS, M., *Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 268.

2016, recordaban que "el número de PIN es un dato de acceso a la terminal telefónica citada, cuyo conocimiento no requiere autorización judicial, por no tratarse de dato alguno relativo a las comunicaciones. En cierta manera, aunque no sea exactamente lo mismo, se parece a la obtención de los números correspondientes al chasis del terminal (IMEI) o al número internacional de la tarjeta telefónica (IMSI)".

En cuanto a la obtención de listados de llamadas, viene entendiéndose que afecta al secreto de las comunicaciones, por lo que resulta precisa autorización judicial para obtener los listados de llamadas efectuados desde una línea telefónica[423]. En tal sentido, las SSTC 230/2007, de 5 de noviembre, 123/2002, de 20 de mayo, y la STS, Sala 2ª, de 22 de enero de 2014, entendían que "el acceso policial al registro de llamadas del terminal móvil intervenido al recurrente sin su consentimiento ni autorización judicial, dicho acceso no resulta conforme a la doctrina constitucional reiteradamente expuesta sobre que la identificación de los intervinientes en la comunicación queda cubierta por el secreto de las comunicaciones garantizado por el art. 18.3 CE y, por tanto, que resulta necesario para acceder a dicha información, en defecto de consentimiento del titular del terminal telefónico móvil intervenido, que se recabe la debida autorización judicial".

Recientemente, esta postura ha sido confirmada por la STS 87/2020, de 3 de marzo, que declara "En el presente caso no se lleva a cabo por los agentes un simple acceso a la agenda de los móviles encontrados en poder de los detenidos, sino que también se accede por la Guardia Civil a otra función de los teléfonos móviles que sí desvelaban procesos comunicativos, en concreto se analizan las llamadas entrantes y salientes, lo que si requiere autorización judicial o consentimiento del titular"[424].

Esta postura se mantiene también en el caso de que resulte necesario acceder a los mensajes contenidos en un móvil, por formar parte de procesos comunicativos.[425] En tal sentido, la STS, Sala 2ª, de 5 de febrero de 2010, sobre el acceso por la policía a mensajes

---

[423] *Ibid.*, p. 269.

[424] En este caso concreto, la autorización judicial se produjo, concluyendo además el Tribunal Supremo que *«El estudio policial en relación al móvil del Sr. Cayetano, solo fue realizado sobre el flujo de llamadas entrantes y salientes, día y hora de las mismas, por lo que en este caso, la injerencia se encuentra justificada dada la gravedad de los hechos, la urgencia y necesidad de investigación de los participantes en la operación, por lo que, ponderando los intereses en juego, puesto en relación con la motivación del auto autorizante de la medida que se remite al atestado policial, la injerencia en la intimidad se encontraba justificada y era proporcional a las circunstancias del caso concreto.»*

[425] BARRIO ANDRÉS, M., *Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 269.

archivados en el móvil sin autorización judicial, concluía que los datos registrados durante un proceso de comunicación, como propios del mismo, permanecen protegidos por el derecho al secreto de las comunicaciones incluso una vez finalizado el proceso comunicativo.[426]

Por último, en cuanto al acceso policial a la agenda de contactos del teléfono móvil, se ha concluido que no es necesaria autorización judicial. Con carácter general señala la STS 493/2010, de 25 de abril, que "La doctrina de esta Sala de Casación, según las reiteradas sentencias que ha dictado sobre casos similares relativos al conocimiento por los agentes policiales de los listados telefónicos de las agendas de teléfonos móviles (SSTS 316/2000, de 3–3; 1235/2002, de 27–6; 1086/2003, de 25–7; 1231/2003, de 25–9; 449/2006, de 17–4; y 1315/2009, de 18–12), afirma que la agenda de un teléfono móvil, entendiendo por agenda, en este caso, el archivo de dicho aparato en el que consta un listado de números identificados normalmente por un nombre, es equiparable a una agenda en soporte de papel o electrónica con el mismo contenido de direcciones y números de teléfono. Por ello su registro u observación no supone la inmisión o injerencia en el derecho al secreto de las comunicaciones sino en el derecho a la intimidad, con las importantes consecuencias que de ello se derivan. Pues así como la injerencia en el primero de tales derechos requeriría, sin duda ni excepción, la previa autorización judicial, por venir así expresamente dispuesto en el artículo 18.3 de nuestra Constitución, la diligencia que afecta a la intimidad del investigado se encuentra, en cambio, legalmente autorizada a las fuerzas del orden, siempre por supuesto que la misma resulte justificada con arreglo a los criterios de urgencia y necesidad y que se cumpla el requisito de proporcionalidad al ponderar los intereses en juego en el caso concreto".

Confirmando lo anterior, se pronunciaba la STS 489/2018[427], de 23 de octubre, citando a título de ejemplo, la STS 444/2014, de 9 de junio, la cual recuerda que "conviene hacer referencia a la STC (Pleno) 115/2013, de 9 de mayo, que se refiere al acceso por parte de los agentes de la Policía Nacional, sin consentimiento del afectado y sin autorización judicial, a la relación de números telefónicos contenidos en la agenda de contactos telefónicos de un teléfono móvil (entendiendo exclusivamente por agenda el archivo del teléfono móvil en el que consta un listado de números identificados mediante un nombre)

[426] En similar sentido, la STC 123/2002, de 20 de mayo, y la STEDH de 3 de abril de 2007, *copland c. Reino Unido*.
[427] Citada en la STS 87/2020, de 3 de marzo de 2020.

que fue encontrado por los agentes en el lugar de comisión de un delito, y considera que esta actuación no afecta al derecho al secreto de las comunicaciones (art. 18.3 CE) del usuario de dicho aparato de telefonía, sino exclusivamente al derecho a la intimidad (art. 18.1 CE). Recuerda el Tribunal Constitucional que la intervención de las comunicaciones requiere siempre de autorización judicial, pero el art. 18.1 CE no prevé esa misma garantía respecto del derecho a la intimidad, por lo que se admite la legitimidad constitucional de que la policía realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas sin previa autorización judicial (y sin consentimiento del afectado), siempre que exista la suficiente y precisa habilitación legal y se hayan respetado las exigencias dimanantes del principio de proporcionalidad. Estima el Tribunal Constitucional que con el acceso a la agenda de contactos del teléfono móvil del recurrente los agentes de policía no obtienen dato alguno concerniente a un proceso de comunicación emitida o recibida mediante dicho aparato, sino únicamente un listado de números de teléfono introducidos voluntariamente por el usuario del terminal, equiparable a los recogidos en una agenda de teléfonos en soporte de papel, por lo que debe descartarse que el derecho al secreto de las comunicaciones quede afectado por esta actuación policial. Distinto sería el caso si se hubiese producido el acceso policial a cualquier otra función del teléfono móvil que pudiera desvelar procesos comunicativos, como por ejemplo el acceso al registro de llamadas entrantes y salientes".

En la actualidad, tal vez podría señalarse, en cierto modo, que dicha perspectiva habría dejado de estar en consonancia con las circunstancias vigentes. El pensamiento lógico que llevaba a considerar una agenda telefónica como un elemento diferenciador dentro de un teléfono móvil deja de ser aplicable cuando estos terminales constituyen auténticas unidades personales móviles de procesamiento (prácticamente ordenadores en miniatura que sirven a sus usuarios a multitud de fines) y sin que sea posible diferenciar o garantizar que el acceso policial anticipado se ha limitado al alcance de dicha agenda telefónica. Por otro lado, la circunstancia de que, hoy en día, las agendas telefónicas no se encuentren guardadas en los teléfonos móviles, sino en las cuentas de usuario ubicadas en la nube, que incluyen muchos más servicios que la simple agenda de contactos, redunda en la dificultad de entender limitada la actuación policial a ese respecto.

3. POSIBILIDADES DE INVESTIGACIÓN TECNOLÓGICA EN SUPUESTOS DE URGENCIA

A. CONSIDERACIONES PREVIAS

Como ya hemos tenido ocasión de exponer, la adopción de medidas de investigación tecnológica exige autorización judicial con carácter previo a su práctica, dado que con ellas se afectan generalmente los derechos fundamentales a la intimidad[428], propia imagen, inviolabilidad domiciliaria, secreto de comunicaciones y privacidad informática, entre otros. Sin embargo, no es menos cierto que es posible que la policía adopte dichas medidas de manera anticipada, prescindiendo de autorización judicial habilitante, siempre que exista una situación de urgencia justificada[429].

En el registro de dispositivos electrónicos la información que puede hallarse tiene múltiples y variados soportes: emails, SMS, imágenes, documentos de texto, que pueden tener gran trascendencia para el buen fin de la instrucción penal y posterior acreditación de los hechos y autoría del delito[430].

La STS 342/2013 exponía la lesividad que para los derechos fundamentales podían tener las medidas de investigación del referido entorno digital, cuando indicaba que: "El ordenador y, con carácter general, los dispositivos de almacenamiento masivo son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (artículo 18.4 de la CE). Pero su contenido también puede albergar –de hecho, normalmente albergará– información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones.

El correo electrónico y los programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato telemático, el derecho a la libre comunicación entre dos o más personas. Es opinión generalizada que los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por su destinatario y

---

[428] En todas sus vertientes, incluido el derecho al propio entorno virtual.
[429] VELASCO NÚÑEZ, E., "La investigación de delitos cometidos a través de Internet y otras nuevas tecnología", cit., p. 273.
[430] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 387.

almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito que sería propio de la inviolabilidad de las comunicaciones. La comunicación ha visto ya culminado su ciclo y la información contenida en el mensaje es, a partir de entonces, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad, cuya tutela constitucional es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad de las comunicaciones."

La consecuencia de lo anterior es el surgimiento de "necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital." En definitiva, conforme a la STS 786/2015, "más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de *nomen iuris* propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital".

A ese respecto, el Tribunal Constitucional alemán, en su sentencia de 27 de febrero de 2008, se refería al libre desarrollo de la personalidad, al secreto de las comunicaciones y a la inviolabilidad del domicilio, tras comprobar la insuficiencia de la protección que se dispensaban frente a investigaciones tecnológicas, reconoció la existencia de un nuevo derecho, que entendió como "el derecho fundamental a la garantía de confidencialidad e integridad de los grupos informáticos", cuyo objeto era "proteger la vida privada y personal de los sujetos de los derechos fundamentales contra el acceso por parte del Estado en el ámbito de las tecnologías de la información, en la medida en que el Estado posea acceso al sistema de tecnologías de la información en su conjunto y no sólo a los acontecimientos de comunicación individuales o a los datos almacenados"[431].

De esa posición misma ha partido la jurisprudencia del Tribunal Supremo de los últimos años, especialmente en sus sentencias SSTS 204/2016, de 10 de marzo, 786/2015,

[431] CABEZUDO RODRÍGUEZ, N., "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal", cit., p. 42.

de 4 de diciembre, y 342/2013, de 17 de abril, en las que reconoce la existencia de un derecho a la protección del propio entorno virtual, que entiende como un derecho constitucional de nueva generación[432].

Con la reforma de 2015 de la LECrim, el legislador ha configurado un tratamiento unitario respecto de las medidas de investigación que supongan alguna injerencia en dicho derecho fundamental. Ello es así porque, como ha indicado la STS 204/2016, de 10 de marzo, "La razón de ser de la necesidad de esta autorización con carácter generalizado es la consideración de estos instrumentos como lugar de almacenamiento de una serie compleja de datos que afectan de modo muy variado a la intimidad del investigado (comunicaciones a través de sistemas de mensajería, por ejemplo, tuteladas por el art 18 3º CE , contactos o fotografías, por ejemplo, tuteladas por el art 18 1º CE que garantiza el derecho a la intimidad, datos personales y de geolocalización, que pueden estar tutelados por el derecho a la protección de datos, art 18 4º CE). La consideración de cada uno de estos datos de forma separada y con un régimen de protección diferenciado es insuficiente para garantizar una protección eficaz, pues resulta muy difícil asegurar que una vez permitido, por ejemplo, el acceso directo de los agentes policiales a estos instrumentos para investigar datos únicamente protegidos por el derecho a la intimidad (por ejemplo, los contactos incluidos en la agenda), no se pueda acceder o consultar también otros datos tutelados por el derecho a la inviolabilidad de las comunicaciones albergados en el mismo dispositivo. Es por ello por lo que el Legislador otorga un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando un derecho constitucional de nueva generación que es el derecho a la protección del propio entorno virtual.

A lo anterior hay que añadir que, conforme a la doctrina del TEDH, el poder público podrá tener acceso al entorno virtual de una persona siempre que i) la injerencia esté prevista por la ley; ii) su finalidad sea legítima; y iii) sea necesaria en una sociedad democrática para la consecución de ese fin legítimo. A la vista de la alarmante anomia de que adolecía el ordenamiento jurídico español al respecto de las diligencias de investigación tecnológica, era fundamental que el legislador español estableciera el régimen jurídico expreso de las mismas, a fin de eliminar la incertidumbre en la investigación y prueba

[432] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 387.

del delito y proteger las garantías del proceso y los derechos fundamentales de los ciudadanos[433].

Tampoco está de más recordar que la Constitución establece una reserva absoluta de resolución judicial en las medidas que, adoptándose en un proceso penal, puedan afectar a la inviolabilidad del domicilio o al secreto de las comunicaciones. Sin embargo, dicha reserva no está establecida respecto de las actuaciones que afecten al derecho a la intimidad[434], ni tampoco al derecho al propio entorno virtual[435], que ni siquiera aparece expresamente contemplado[436]. En ese sentido, la STS 691/2009, de 5 de junio, recordaba que de la doctrina del Tribunal Constitucional "se puede concluir que no existe en la Constitución reserva absoluta de previa resolución judicial respecto a derecho a la intimidad personal y excepcionalmente se admite la legitimidad constitucional de que en determinados casos, con precisa habilitación legal, pueda la Policía judicial realizar determinadas prácticas que constituyen una leve injerencia en la intimidad de las personas siempre que se respeten las sugerencias derivadas del principio de proporcionalidad".

El artículo 588 *sexies* c), en ese sentido, prevé que en los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida, la Policia Judicial pueda llevar a cabo el examen directo e inmediato de los datos que contenga el dispositivo de almacenamiento masivo incautado, siempre que lo comunique inmediatamente y en todo caso en el plazo máximo de 24 horas al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. Por tanto, los presupuestos para la adopción de la medida son tres: urgencia en el acceso a los datos, existencia de un interés constitucional legítimo, y proporcionalidad de la actuación.

B. ACCESO A DATOS CONTENIDOS EN DISPOSITIVOS APREHENDIDOS

Con carácter ordinario, el registro de dispositivos electrónicos precisa de una autorización judicial previa que efectúe una ponderación de los bienes afectados por la

---

[433] *Ibid.*, p. 388.
[434] *Ibid.*, p. 394.
[435] MARTÍN RÍOS, P., "El alcance del derecho al propio entorno virtual en la valoración de la evidencia digital", cit., p. 6.
[436] CALAZA LÓPEZ, S., "Protección judicial del derecho a la intimidad informática en su doble dimensión de derecho a la autodeterminación informativa y derecho al entorno virtual", en *Nuevos postulados de la cooperación judicial en la Unión Europea: libro homenaje a la Prof.ª Isabel González Cano, 2021, pp. 1111–1146*, Tirant lo Blanch, 2021, p. 5, fecha de consulta 26 noviembre 2021, en https://dialnet.unirioja.es/servlet/articulo?codigo=7892073.

medida a adoptar, controlando la aplicación de los principios que han de inspirar este tipo de diligencias de investigación y realizando un juicio de proporcionalidad. No obstante, existen dos supuestos en los que dicha autorización judicial deja de ser necesaria: los supuestos de urgencia y los de consentimiento del afectado.

a) Presupuestos

De conformidad con el artículo 588 *sexies* c 4 LECrim, "en los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida prevista en los apartados anteriores de este artículo, la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida."

En consecuencia, se prevé que la Policía Judicial pueda llevar a cabo un examen directo de los datos contenidos en un dispositivo incautado siempre que concurra i) situación de urgencia; ii) necesidad insoslayable de acceder a dichos datos para no comprometer el buen fin de la investigación; y iii) un interés constitucional legítimo perseguido por dicha medida.

b) La urgencia en el acceso a los datos

En cuanto al primero de dichos elementos, la urgencia en el acceso a los datos es un concepto indeterminado que obliga a estar a las circunstancias concretas de cada caso. Por ejemplo, la STC 115/2013, de 9 de mayo, entendió que la urgencia de la actuación quedaba justificada por la necesidad de averiguar la identidad de las personas que intervinieron en el delito y huyeron cuando fueron sorprendidas *in fraganti* custodiando un alijo de droga, permitiendo así que su detención fuera posible y evitando que se sustrajeran a la acción de la justicia o destruyeran ulteriores pruebas.

Ejemplo de esta circunstancia puede encontrarse en la STS 786/2015, de 4 de diciembre, cuando indica que "la simple posibilidad de que esas imágenes pudieran llegar a convertirse, de una u otra forma en contenidos difundibles en la red, intensificando de

forma irreparable el daño ocasionado a las dos menores, era un riesgo que había que ser ponderado en el momento del juicio de necesidad y proporcionalidad".

c) Necesidad de acceder a la información

En cuanto al segundo de los requisitos, la necesidad de acceder a la información, en la STC 115/2013 concluye que "no existía otra medida más moderada para la ejecución de tal propósito –la identificación de las personas que huyeron tras ser sorprendidas por la policía en el invernadero donde fue aprehendido el alijo de droga– con igual eficacia, toda vez que gracias a la identificación inmediata del recurrente como usuario de uno de los teléfonos móviles encontrados por los agentes de policía se pudo corroborar su presencia en el lugar de los hechos, así como obtener otras pruebas incriminatorias para fundamentar la convicción judicial sobre su participación en el delito contra la salud pública por el que ha sido condenado". Dicho en otros términos, debe concurrir la circunstancia de que el fin perseguido no pueda alcanzarse por ningún otro medio que sea igual en eficacia pero de menor intensidad respecto del derecho fundamental que se vea afectado. Esto es, debe ser el medio suficientemente eficiente y menos gravoso para el investigado[437].

d) La existencia de un fin constitucional legítimo

Mayoritariamente. la doctrina[438] existente hasta la fecha identifica este requisito con el del principio de idoneidad y necesidad, entendiendo que se exige que el registro sea necesario para la finalidad de la investigación, de manera que no exista un medio menos gravoso para el investigado que produzca la misma utilidad. Es decir, debe tratarse de la diligencia de investigación que menos restrinja el derecho fundamental afectado del investigado sin comprometer la eficacia y resultado necesario.

e) La proporcionalidad de la actuación

En los términos de la STC 115/2013, "se trató de una medida ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto, dada la naturaleza y gravedad del delito

[437] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 391.
[438] *Ibid.*, p. 395.

investigado y la leve injerencia que comporta en el derecho a la intimidad del recurrente el examen de la agenda de contactos de su teléfono móvil".

En relación con dichos requisitos, la STS 786/2015, de 4 de diciembre, razona que "la simple posibilidad de que esas imágenes pudieran llegar a convertirse, de una u otra forma, en contenidos difundibles en la red, intensificando de forma irreparable el daño ocasionado a las dos menores, era un riesgo que había de ser ponderado en el momento del juicio de necesidad y proporcionalidad".

La STS 204/2016, de 10 de marzo, casó una sentencia condenatoria al considerar que no concurrió una efectiva urgencia en la intervención policial en el acceso a datos de la agenda de contactos. Indica que "estas injerencias policiales directas deben ser examinadas con especial atención, dado que la multifuncionalidad de los datos que se albergan en estos dispositivos provoca una extrema debilidad de la tutela jurisdiccional del derecho del investigado a la reserva de su propio entorno virtual, pues una vez realizado el acceso al dispositivo, superando la barrera de la contraseña, todos los datos, incluidos los relacionados con el secreto de las comunicaciones, están al libre alcance del investigador".

Y continúa afirmando que en el caso concreto no se encontraba justificada la actuación policial con arreglo a los criterios de urgencia y necesidad. "La detención de Pedro Enrique se produjo, según la sentencia, el 25 de junio de 2014, siendo ese el momento en el que se aprehendió policialmente su teléfono móvil. El 9 de julio se produjo la inspección y registro en la discoteca que regentaba el recurrente. Hubo tiempo más que suficiente para interesar del Juzgado que autorizase el acceso al contenido del móvil de Pedro Enrique, si se consideraba necesario para la investigación en lugar de realizar la injerencia directamente. Y añade indicando que "los teléfonos de Eusebio fueron ocupados durante el registro policial practicado en la Discoteca. Se trata de una diligencia cuyo resultado debe entregarse en el Juzgado. No concurría razón alguna de urgencia y necesidad en ese momento para proceder al acceso policial de los móviles intervenidos, cuando podían ser entregados al Juez y solicitar la autorización pertinente para salvaguardar el derecho constitucional a la intimidad".

Por último, en cuanto al tercer y último requisito, relativo a la proporcionalidad de la actuación, podemos citar la STC 115/2013, cuando indica que "se trató de una medida ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto, dada la naturaleza

y gravedad del delito investigado y la leve injerencia que comporta en el derecho a la intimidad del recurrente el examen de la agenda de contactos de su teléfono móvil".

En tal sentido, la STS 204/2016, en un supuesto de intervención policial de la agenda de contactos de un investigado, resaltaba que siempre había que tener en consideración que "estas injerencias policiales directas deben ser examinadas con especial atención, dado que la multifuncionalidad de los datos que se albergan en estos dispositivos provoca una extrema debilidad de la tutela jurisdiccional del derecho del investigado a la reserva de su propio entorno virtual, pues una vez realizado el acceso al dispositivo, superando la barrera de la contraseña, todos los datos, incluidos los relacionados con el secreto de las comunicaciones están al libre alcance del investigador."

Con base en ese razonamiento, la sentencia concluye que "La detención de Pedro Enrique se produjo, según la sentencia, el 25 de junio de 2014, siendo ese el momento en el que se aprehendió policialmente su teléfono móvil. El 9 de julio se produjo la inspección y registro en la discoteca que regentaba el recurrente. Hubo tiempo más que suficiente para interesar del Juzgado que autorizase el acceso al contenido del móvil de Pedro Enrique, si se consideraba necesario para la investigación, en lugar de realizar la injerencia directamente. Asimismo, los teléfonos de Eusebio fueron ocupados durante el registro policial practicado en la Discoteca. Se trata de una diligencia cuyo resultado debe entregarse en el Juzgado. No concurría razón alguna de urgencia y necesidad en ese momento para proceder al acceso policial de los móviles intervenidos, cuando podían ser entregados al Juez y solicitar la autorización pertinente para salvaguardar el derecho constitucional a la intimidad. No ha de olvidarse tampoco que los datos de la agenda no eran neutros, ni escasamente relevantes porque lo que pretendían era confirmar una comunicación telefónica entre ambos acusados, a partir de una información obrante en el terminal telefónico que genera el propio usuario, dejando un rastro susceptible de seguimiento por los poderes públicos, y que en consecuencia forma parte de su perfil personal, reservado e íntimo, que no puede ser sacrificado sin las oportunas garantías constitucionales".

f) Revocación judicial

La propia LECrim prevé que se revoque o confirme la actuación en un plazo máximo de 72 horas. En la doctrina del Tribunal Constitucional se mantiene que la valoración de la urgencia y necesidad de la intervención policial ha de realizarse *ex ante*, al igual que del principio de proporcionalidad.

La constatación *a posteriori* de la falta del presupuesto de urgencia implica la vulneración del derecho fundamental y podría determinar la ilicitud de la prueba obtenida, según las SSTC 206/2007 y 70/2002. Al menos antes de la STC 97/2019, de 16 de julio. también surge problemática cuando lo hallado se disfraza como hallazgo casual o cuando siendo nulo adquirido se utiliza el conocimiento adquirido para poder practicar otras diligencias.

Aunque la actuación policial basada en la urgencia y persecución de un fin constitucional legítimo no precise de autorización judicial, sí deberá trasladar al juez competente dicha noticia en el plazo máximo de 24 horas. Este, a su vez, en el plazo de 72 horas desde que fue ordenada la medida, deberá revocarla o confirmarla de forma motivada.

Como es lógico, la valoración de la urgencia y necesidad de la intervención policial ha de realizarse *ex ante* aunque el control judicial se realice *ex post*, del mismo modo que sucede con el principio de proporcionalidad. En su caso, la constatación *ex post* de la falta del presupuesto habilitante determinaría que las diligencias de investigación se hubieran efectuado con vulneración de los derechos fundamentales que hubieran resultado afectados por ella (SSTC 206/2007 y 70/2002).

No obstante lo anterior, no puede dejar de señalarse lo que podría entenderse un principio de cambio de criterio en la STC 97/2019 [439]. Como ya hemos comentado, dicha sentencia declara que la garantía de ilicitud de las pruebas obtenidas con vulneración de derechos fundamentales no está contenida por sí misma, y de forma autónoma, en el resto de las garantías del artículo 24.2 CE, como debería suceder a consecuencia de la supremacía de los derechos fundamentales en el ordenamiento jurídico sino que, en realidad, está integrada dentro del concepto de un proceso justo y equitativo. De este modo, la obtención de pruebas con vulneración de derechos fundamentales ha pasado a ser meramente instrumental y únicamente atendible si, además, se entiende vulnerada dicha idea de un proceso justo y equitativo.

[439] ASENCIO MELLADO, J. M., "La STC 97/2019, de 16 de julio. Descanse en paz la prueba ilícita", cit.

C. ACTUACIONES DE SEGUIMIENTO Y LOCALIZACIÓN

a) Concepto

En este apartado, nuestro propósito es analizar la regulación de los mecanismos técnicos destinados a localizar y seguir un objetivo de la investigación, sea una persona o una cosa, de manera que sea posible determinar su posición en el espacio mediante técnicas de geolocalización. Es lo que se ha venido en denominar como *positioning*[440], haciendo referencia al conjunto de herramientas de investigación que permiten identificar la posición geográfica de una persona o dispositivo.

En general, se reconocen varias técnicas: desde la geolocalización de dispositivos electrónicos de comunicación y la utilización de balizas o dispositivos RFID[441], hasta el el empleo de los determinados *finders*, teléfonos celulares que los investigadores pueden colocar en lugares estratégicos pero que, por pertenecer a las propias fuerzas policiales, no precisan de autorización judicial ni de la colaboración del proveedor de servicios de internet[442].

b) Geolocalización de dispositivos electrónicos de comunicación

En la categoría de dispositivos hay que entender todo tipo de *smartphones*, teléfonos móviles, ordenadores portátiles con capacidad para conectarse a la red GSM, *smarwatches* con capacidad para tarjeta e–SIM, *routers* de internet radio, etc. Al estar encendidos, con independencia de que estén siendo utilizados para un proceso de comunicación o no, quedan registrados en antenas BTS cuya posición geográfica les puede ofrecer la cobertura del servicio, permitiendo así localizar en el espacio su ubicación aproximada.

Esta determinación de su ubicación, además, cuenta con el valor añadido de que puede efectuarse en tiempo real, partiendo de datos de SITEL (previa autorización judicial) y utilizando técnicas complementarias de triangulación. Esta modalidad está prevista en el artículo 588 *ter* b.2 LECrim, que dispone que "2. La intervención judicialmente acordada podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se

---

[440] MERKEL, L., *Derechos humanos e investigaciones policiales*, Marcial Pons, Madrid, 2022, p. 251.
[441] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 505.
[442] MERKEL, L., *Derechos humanos e investigaciones policiales*, cit., p. 253.

produzcan con independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario."

También puede efectuarse con carácter retrospectivo, utilizando para ello los datos conservados por operadoras, según el régimen de la Ley 25/2007 y aplicando técnicas de localización, para lo que será necesario autorización judicial, de conformidad con el artículo 588 *ter* j LECrim.

c) Balizas de seguimiento

La otra modalidad apuntada consiste en la geolocalización mediante instrumentos distintos de los dispositivos electrónicos de comunicación del investigado. A estos supuestos se refiere el artículo 588 *quinquies* b.1 LECrim al indicar que "Cuando concurran acreditadas razones de necesidad y la medida resulte proporcionada, el juez competente podrá autorizar la utilización de dispositivos o medios técnicos de seguimiento y localización."

En general, son todo tipo de instrumentos que, al emitir de manera continuada una señal, permiten el seguimiento activo de cualquier persona o cosa que, de otro modo, no sería posible geolocalizar[443].

d) Derechos fundamentales afectados

Lo primero que hay que tener en cuenta es que en la utilización de mecanismos de geolocalización no se compromete el derecho al secreto de las comunicaciones. En ese sentido, se ha concluido que "el concepto genuino de baliza policial atendería a la idea de un dispositivo electrónico oculto que genera información sobre localización; y que, a través de las señales que emite por radiofrecuencia, sea o no a través de canales cerrados, permite realizar un seguimiento remoto de determinado objeto a través de un dispositivo receptor. Este tipo de dispositivos no generan una especie de comunicación en las que participara de manera forzada la persona que conduce o transporta el objeto de la vigilancia. La emisión de tales señales, en cualquier caso, se produce de forma ajena a la

[443] URIARTE VALIENTE, L. M., "Nuevas técnicas de investigación restrictivas de derechos fundamentales", fecha de consulta 8 abril 2020, en https://docplayer.es/56647100–Nuevas–tecnicas–de–investigacion–restrictivas–de–derechos–fundamentales–luis–m–uriarte–valiente–fiscal.html.

participación de personas, tiene lugar de máquina a máquina; y el hecho de que en cierto modo dicha persona participe de la generación de la información que emite la baliza, o sea detentador de una posesión sobre el objeto de la vigilancia, no le convierten en titular de esa forma peculiar de comunicación"[444].

Ahora bien, aunque no afecte al derecho al secreto de las comunicaciones, el conocimiento de la situación en el espacio de una persona sí puede afectar a su derecho a la intimidad, afectación que aumentará en intensidad cuanto mayor sea la extensión en el tiempo de la medida[445]. A ese respecto, la STEDH de 2 de septiembre de 2010 (Uzun c. Alemania), refiriéndose a un supuesto de vigilancia por la persona vía GPS que se extendió durante tres meses y supuso la recolección sistemática de datos relativos a donde se encontraba y los desplazamientos utilizado, concluía "que la vigilancia mediante GPS, así como el tratamiento y la utilización de los datos resultantes, supuso una injerencia en la vida privada del demandante, aun cuando el dispositivo se hubiera instalado en un objeto –un vehículo–, de un tercero –su cómplice– y sólo revelara la ubicación del receptor y no si la persona se encontraba en su interior, pues no en vano, señala el Tribunal de Estrasburgo, la pretensión de las autoridades alemanas era conocer la ubicación y los desplazamientos del demandante y su cómplice"[446].

En atención a lo anterior se ha apreciado una relación directamente proporcional entre el tiempo durante el que se extiende la medida de videovigilancia y la intensidad de la injerencia en el derecho a la vida privada del afectado[447].

Precisamente esa distinción ha permitido que nuestra jurisprudencia acepte que la injerencia se efectúe por la policía sin previa autorización judicial, siempre que existan razones de urgencia y sin perjuicio del juicio de proporcionalidad efectuado *a posteriori*, que es lo que prevé el apartado cuarto del artículo 588 *quinquies* b LECrim cuando indica que "4. Cuando concurran razones de urgencia que hagan razonable temer que de no colocarse inmediatamente el dispositivo o medio técnico de seguimiento y localización se frustrará la investigación, la Policía Judicial podrá proceder a su colocación, dando cuenta

---

[444] RODRÍGUEZ LAINZ, J. L., "GPS y balizas policiales", *Diario La Ley*, 8416, 2014, Wolters Kluwer, p. 4.
[445] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 507.
[446] SERVICIO DE ESTUDIOS DEL PARLAMENTO EUROPEO, *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado – Consejo de Europa – Think Tank*, fecha de consulta 8 abril 2020, en https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2018)628261.
[447] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 508.

a la mayor brevedad posible, y en todo caso en el plazo máximo de veinticuatro horas, a la autoridad judicial, quien podrá ratificar la medida adoptada o acordar su inmediato cese en el mismo plazo. En este último supuesto, la información obtenida a partir del dispositivo colocado carecerá de efectos en el proceso."

Es una postura que, como decimos, ya venía siendo admitida por nuestra jurisprudencia. Así, por ejemplo en la STC 115/2013 se concluía que "si bien los agentes de policía accedieron a los datos recogidos en la agenda de contactos telefónicos del terminal móvil del recurrente sin autorización judicial (ni tampoco consentimiento del afectado), ya hemos adelantado que tal exigencia se excepciona en los supuestos en que existan razones de necesidad de intervención policial inmediata para la averiguación del delito, el descubrimiento de los delincuentes o la obtención de pruebas incriminatorias, siempre que se respete el principio de proporcionalidad (SSTC 70/2010, FJ 10, y 173/2011, FJ 2, entre otras), como acontece en el presente caso".

También se considera que el uso indiscriminado y persistente de balizas para el control de personas investigadas puede llegar a afectar a sus derechos fundamentales, teniendo en cuenta que proporciona información exacta y en tiempo real de la situación de una persona durante las 24 horas del día, por lo que su utilización durante un período continuado de tiempo proporcionará información precisa acerca de los hábitos, comportamientos, relaciones y actividades de esa persona. Entre otros ejemplos, se señala que si se comprueba la posición de una persona todos los días a una determinada hora en un templo religioso, obtendremos información sobre sus creencias religiosas; si comprobamos que visita habitualmente un centro médico de una determinada especialidad, podremos obtener información acerca de su salud; en definitiva, la simple constatación de sus visitas a un determinado local de ocio nos puede proporcionar información acerca de sus hábitos o preferencias sexuales"[448].

Esta posibilidad de descubrir con profundidad todos los datos relativos a la persona del investigado aumenta conforme se mantiene en el tiempo la geolocalización, de ahí que se haya apreciado dicha relación de proporcionalidad directa entre la duración de la medida y la intensidad de la injerencia, y que el artículo 588 *quinquies* c LECrim exija

[448] URIARTE VALIENTE, L. M., "Nuevas técnicas de investigación restrictivas de derechos fundamentales", cit.

que la resolución judicial establezca el periodo de duración inicial y la posible prórroga de la medida.

Por otro lado, este celo se flexibiliza en los supuestos de seguimiento y localización de objetos desligados de personas. La STS 798/2013, de 5 de noviembre, concluía a ese respecto que el uso de radiotransmisores (balizas de seguimiento GPS) para la localización de embarcaciones en alta mar por la policía no vulnera el derecho fundamental al secreto de las comunicaciones ni supone una inferencia excesiva sobre el derecho fundamental a la intimidad a los efectos de exigir un control jurisdiccional previo y una ponderación sobre dicha afectación constitucional. A juicio del tribunal, se trata de diligencias de investigación legítimas desde la función constitucional que tiene la policía, previstas entre otras en las SSTS 22/6/2007, 11/7/2008, 19/12/2008, e incluso la sentencia TEDH caso *UZUN c. Alemania* de 02/09/2010[449]. Del mismo modo, la STS 610/2016, de 7 de julio, recuerda que se hace una distinción significativa cuando la injerencia recae sobre cosas y no sobre personas, distinguiendo si el dispositivo GPS es aplicado directamente sobre objetos, para su localización, o para la localización de personas, ya que solo respecto a estas últimas puede verse afectado el derecho a la intimidad.

e) Regulación

En el artículo 588 *quinquies* b LECrim, relativo a la utilización de dispositivos o medios técnicos de seguimiento y localización, se regulan a todos los instrumentos que permiten localizar en el espacio a una persona o cosa, sea a través de dispositivos específicos o mediante el rastreo de aparatos conectados. A tal efecto, la doctrina se ha referido al "sometimiento mediante dispositivos técnicos a control de las actividades de una persona, lugar u objeto preciso en una investigación penal, tanto para poder probar una actividad delictiva pasada (observar a quien accede al cuadro robado, al depósito de armas descubierto, por ejemplo), como actual o futura (observar las actividades de sospechosos de un delito para ver si lo reiteran)[450]".

[449] En un caso de intervención de una cabina telefónica habitualmente usada por un supuesto terrorista, consideró que la vigilancia a través del sistema GPS, y procesamiento de los datos obtenidos constituía una injerencia en la vida privada, pero también precisó que la vigilancia GPS, por su propia naturaleza, debe distinguirse de otros métodos de seguimiento acústico o visual que, por regla general, son más susceptibles de interferir en el derecho de la persona al respeto de su vida privada, porque revelan unas informaciones sobre la conducta de una persona, sus operaciones o sus sentimientos.

[450] VELASCO NÚÑEZ, E., "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías – El Derecho – Fiscal, Penal, Sector Jurídico", *El Derecho*, fecha de consulta 19 marzo 2020, en https://elderecho.com/novedades–tecnicas–de–investigacion–penal–vinculadas–a–las–nuevas–tecnologias.

Dentro de las diferentes modalidades, se han señalado las siguientes[451]:

- Sistemas de señal por radio, que incluyen aquellos sistemas que permiten apoyar al dispositivo de seguimiento y que se fundamentan en analizar la intensidad y dirección de la señal, así como un despliegue de antenas y la triangulación de la posición de manera aproximada.

- Sistemas GPS, que recogen la señal emitida por varios satélites y así permite ubicar el instrumento que integra el GPS.

- Sistema satelital especial, que utiliza satélites independientes para el control de un espacio determinado y concreto, lo que posibilita, por ejemplo, la localización de embarcaciones en largas travesías por alta mar.

- Tecnología GSM, que utiliza el sistema de repetidores de la telefonía móvil mediante recepción de la señal en el repetidor junto con técnicas de trilateración, triangulación y multilateración.

- Descarga de archivos log, en los que se acumulan las ubicaciones del dispositivo de localización GPC y, posteriormente, se descargan de manera acumulada.

Conviene destacar que la LECrim no contiene una limitación de los delitos que pueden ser objeto de investigación utilizando este tipo de medidas, sin perjuicio del correspondiente control judicial y el necesario respeto del principio de proporcionalidad.

Ha de llamarse la atención, igualmente, sobre la necesidad de que en la autorización judicial se especifique el medio técnico que va a ser utilizado en la concreta investigación, incluyendo el tipo de datos que graba y transmite, aunque no pueda exigirse una descripción detallada de los detalles técnicos[452]. Conviene igualmente destacar que, al contrario de lo que sucede con la grabación de comunicaciones orales, en este caso no se exige que se identifiquen los agentes que realizarán la instalación de los dispositivos o medios técnicos de seguimiento y localización.

Es de destacar que, conforme al artículo 588 *quinquies* b.4 LECrim, la Policía Judicial puede colocar los dispositivos sin necesidad de autorización judicial, siempre que

---

[451] DE LA TORRE OLID, F.; GARCÍA RUIZ, F., "Tecnología de geolocalización y seguimiento al servicio de la investigación policial. Incidencias sobre el Derecho a la intimidad", *Revista Derecho y Criminología*, vol. Anales, 2, 2011.
[452] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 511.

"concurran razones de urgencia que hagan razonablemente temer que de no colocarse inmediatamente el dispositivo o medio técnico de seguimiento y localización se frustrará la investigación", con la obligación de trasladar la actuación a la autoridad judicial a la mayor brevedad posible y, en todo caso, en el plazo máximo de 24 horas, para que aquella ratifique la medida o acuerde su cese en función de la proporcionalidad de la actuación, careciendo de efectos en el proceso la información obtenida vulnerando tales previsiones. Ahora bien, no puede negarse la posibilidad de solicitar nuevas medidas de investigación por el cauce ordinario, una vez se haya adquirido el conocimiento de tal información previa.

4. ACTUACIONES DE INVESTIGACIÓN TECNOLÓGICA QUE EXIGEN, EN TODO CASO, AUTORIZACIÓN JUDICIAL PREVIA

Además de las dos categorías estudiadas, no queremos cerrar este capítulo sin hacer referencia al resto de actuaciones de investigación que, aun no siendo autónomas ni estando prevista la autonomía en caso de urgencia, presentan peculiaridades de cierto interés.

A. CAPTACIÓN DE IMAGEN

En el presente trabajo no se aborda el examen de los supuestos de captación de sonidos o conversaciones por la Policía Judicial, puesto que, al contrario de lo que sucede con las imágenes, en los supuestos de captación de sonido siempre es necesaria la autorización judicial previa.

En la captación de la imagen se ven afectados los derechos fundamentales a la propia imagen, pero también el derecho fundamental a la intimidad cuando la misma se refiere a aspectos de la vida privada del sujeto, a la inviolabilidad del domicilio, si la captación se efectúa dentro del propio domicilio del titular, así como al derecho a la protección de datos personales[453].

Resulta fundamental el análisis[454] que realiza del derecho a la propia imagen la STEDH de 27 de mayo de 2014 (*De la Flor Cabrera c. España*), cuando indica que la imagen de un individuo es uno de los atributos principales de su personalidad, por el hecho de revelar su originalidad y permitirle diferenciarse de sus congéneres. En

[453] VELASCO NÚÑEZ, E., "Derecho a la imagen: tratamiento procesal penal", *Diario La Ley*, 8596, 2015, Wolters Kluwer.
[454] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 492.

consecuencia, el derecho de la persona a la protección de su propia imagen constituye uno de los componentes esenciales para alcanzar la plenitud personal y presupone, principalmente, el control del individuo sobre su propia imagen. Tal control implica la posibilidad para el individuo de rechazar la difusión de su imagen, así como el derecho de este de oponerse a la captura, la conservación y la reproducción de la misma por un tercero, pues, siendo la imagen una de las características ligadas a la personalidad de cada uno, su protección efectiva exige el consentimiento del individuo desde el momento de su captura, y no solamente en el momento de su posible difusión al público, pues, en caso contrario, un atributo esencial de la personalidad podría ser detentado por otro sin que el interesado tuviera el control sobre su eventual uso posterior (ver, *mutatis mutandis*, *Reklos y Davourlis c. Grecia*, no1234/05, § 40, 15 de enero de 2009).

Por su parte, el Tribunal Constitucional lo define en su STC de 26 de marzo de 2001 como aquel derecho que atribuye a su titular la potestad de determinar la información gráfica generada por sus rasgos físicos personales que pueden tener difusión pública. La facultad otorgada por este derecho, en tanto que derecho fundamental, consistiría en impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad –informativa, comercial, científica, cultural, etc.– perseguida por quien la capta o difunde.

En todo caso, conviene tener presente que el derecho a la propia imagen puede ser limitado en diferentes supuestos. En primer lugar, por la propia actuación de su titular, sea a través de un consentimiento expresado de manera inequívoca, libre e informada, o por realizar actos que permitan entender que mantiene una inferior expectativa razonable de privacidad, esto es, cuando realiza de manera intencional o consciente actividades o actuaciones en las que se expone al conocimiento ajeno. Son los casos, por ejemplo, de los espacios públicos y las fuentes abiertas en internet, como salas de *streaming*, páginas web, redes sociales, etc. Paralelamente, también puede limitarse el derecho a la propia imagen en defensa del interés público, para la investigación y persecución de delitos.

B. Obtención de imágenes por la Policía en funciones de investigación y prueba del delito

a) En espacios públicos

La teoría de la expectativa razonable de privacidad determina que la obtención de imágenes en espacios públicos no afecte a la intimidad ni a la propia imagen. En este

sentido, el artículo 588 *quinquies* a) LECrim establece que "la Policía Judicial podrá obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos.

Igualmente, la STS 200/2017, de 27 de marzo, ya concluía que no existe obstáculo para que las labores de investigación practicada por los agentes de la policía en cumplimiento del mandato contenido en el artículo 282 LECrim, se extiendan a la captación de imágenes de personas de manera subjetiva en los momentos en que se está fundadamente cometiendo un hecho ilícito, ya que ningún derecho queda vulnerado si la filmación se realiza en vías públicas o espacios abiertos al público, y que dicha labor de captación de imágenes por medios de reproducción mecánica, no precisa autorización judicial. Todo ello, en contraposición a los supuestos en que se trate de domicilios o lugares considerados como tales, en los que sí es preceptiva autorización judicial y debe concederse por el órgano judicial en resolución motivada y proporcional al hecho a investigar.

Como ya se adelantó, conviene recordar que dicho precepto únicamente habilita la captación de imágenes, y no puede entenderse que se extiende también a la captación o grabación de sonidos, para los que en todo caso la Policía Judicial precisa de autorización judicial, conforme al artículo 588 *quater* a LECrim.

A este respecto, quizás lo más destacable sea el concepto de lugar o espacio público. En ese sentido, se ha concluido que sería todo aquel ajeno a la protección constitucional dispensada por el artículo 18.2 LECrim a la inviolabilidad del domicilio o por el artículo 18.1 a la intimidad[455].

Por su parte, la STS 272/2017, de 18 de abril, concluye que lo relevante es discernir cuando se trata de un espacio reservado a la autorización judicial, domicilio o lugar cerrado, o cuando por propia iniciativa los agentes pueden captar las imágenes cuestionadas por tratarse de "lugares o espacios públicos". En estos últimos, incluyendo con carácter general todos aquellos ajenos a la protección constitucional dispensada por el artículo 18.2 CE a la inviolabilidad domiciliaria o por el artículo 18.1 a la intimidad, podrá ser

[455] MARCHENA GÓMEZ, M., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, cit., p. 495.

decidida por propia iniciativa por los agentes de policía[456] . También debe tenerse en cuenta cuándo la utilización de cámaras en espacios públicos tiene un fin puramente preventivo pues el precepto citado, 588 *quinquies* a), está dirigido una utilización concreta en función de la investigación de un hecho delictivo ya cometido y respecto del que la captación de imágenes resulta necesaria para identificar a los responsables.

Por su parte, el artículo 588 *quinquies* a LECrim prevé también la posibilidad de dirigir la medida de investigación contra terceros, cuando indica en su apartado segundo que "La medida podrá ser llevada a cabo aun cuando afecte a personas diferentes del investigado, siempre que de otro modo se reduzca de forma relevante la utilidad de la vigilancia o existan indicios fundados de la relación de dichas personas con el investigado y los hechos objeto de la investigación." Precisamente la afectación a terceros ha provocado que la doctrina recuerde la necesidad de que la Policía Judicial opere con un criterio restrictivo en este punto, aunque las consecuencias de incumplir dicha máxima no están en absoluto claras[457]

b) En espacios no públicos

La grabación en espacios no públicos está prevista en el apartado tercero del artículo 588 *quater* a LECrim exclusivamente como complemento de la grabación de comunicaciones orales directas, al disponer que la escucha y grabación de las conversaciones privadas se podrá complementar con la obtención de imágenes cuando expresamente lo autorice la resolución judicial que la acuerde.

De lo anterior resulta cierta confusión acerca de si es posible obtener imágenes de espacios no públicos cuando no va a acompañada de una captación y grabación de sonidos. De lo que no cabe duda es de que, si fuera posible, el régimen jurídico aplicable sería el de las conversaciones orales, por lo que el juez debería indicar en su resolución judicial, con la motivación suficiente, los espacios privados en los que se podría proceder a la captación de la imagen, a la vista de que no todos tendrán, a buen seguro, igual significación en relación a los derechos fundamentales de los afectados por la medida de investigación[458].

---

[456] Lo que ha dado lugar a no pocas sentencias, como las SSTS 124 o 129/2014, 485/2013, 433/2012 o 793/2013, entre otras muchas

[457] MARCHENA GÓMEZ, M., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, cit., p. 680.

[458] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 497.

c) Incorporación de las imágenes al proceso

De conformidad con la referida STS 272/2017, de 18 de abril, la incorporación del resultado de las videograbaciones al plenario por medio de las actas levantadas por la policía judicial derivadas de aquellas, como parte del atestado, tienen el valor de una denuncia que debe ser ratificada ante el Tribunal por los agentes que han intervenido en tales videograbaciones, que efectivamente han sido incorporadas mediante los "foto–printers" extraídos de las mismas, ratificados por los agentes en el plenario, lo que en principio valida su autenticidad mientras no se contradiga la misma con datos o pruebas que lo justifiquen.

C. REGISTRO DE DATOS ALMACENADOS EN LA NUBE

En los casos de registros de dispositivos de almacenamiento masivo de la información digital, pueden distinguirse dos modalidades, si atendemos al soporte que contiene la información. Así, por un lado, pueden distinguirse los registros tradicionales, cuando se accede a los datos contenidos en el sistema informático o equipo de almacenamiento del propio usuario, y los registros en la nube, cuando se accede a datos que, aunque están disponibles para el sistema informático o equipo de almacenamiento del propio usuario, en realidad están almacenados en otro dispositivo.[459] A mi juicio, concurren suficientes especialidades en el registro de datos almacenados en la nube desde el punto de vista de la actuación policial como para incluirlos en este apartado.

Las denominadas técnicas de computación en la nube o *cloud computing*, consisten en que la información se almacene de manera permanente en uno o varios servidores alojados en cualquier parte del mundo y se ponga a disposición del usuario a través de Internet en las cachés temporales de su equipo informático[460]. De esa manera, la doctrina identifica cinco características fundamentales del *cloud computing*: autoservicio, en el sentido de que es el usuario el que decide en qué momento acceder al servicio y se sitúa a sí mismo en condiciones de recibirlo; ubicuidad de la información, en el sentido de que la información confiada por los usuarios se encuentra disponible desde cualquier parte del globo que permita acceder, vía internet, a los servidores del prestador de servicios;

---

[459] *Ibid.*, p. 403.

[460] ORTIZ PRADILLO, J. C., "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica", en *El proceso penal en la sociedad de la información: las nuevas tecnologías para investigar probar el delito, 2012, pp. 267–310*, La Ley (España), 2012, p. 276, fecha de consulta 4 abril 2020, en https://dialnet.unirioja.es/servlet/articulo?codigo=4079500.

agrupación de recursos, en el sentido de la decisión que adoptan las compañías prestadoras de dichos servicios de concentrar sus herramientas de computación en espacios concretos; elasticidad, pues el servicio puede adaptarse a las condiciones y necesidades de cada usuario; y servicio medido, pues las compañías prestadoras del servicio mantienen un estricto control tanto de la capacidad de almacenamiento utilizada como del contenido de los archivos confiados, para asegurarse de que no son contrarios a los términos del servicio.[461]

Las técnicas de computación en la nube, o *cloud computing*, surgen en el marco de la deslocalización de la información, y permiten que esta se almacene permanentemente en servidores alojados en cualquier parte del mundo, generalmente incluso en varios servidores de manera simultánea. Desde ellos, se envía a través de internet a cachés temporales del equipo informático del usuario, que pueden ser varios y simultáneos, como un portátil, un ordenador de sobremesa, un *smartphone*, un *smartwatch*, una *Smart tv* y, en general, cualquier aparato informático que disponga de conexión a internet.

De todas esas características, debe destacarse la nota de la ubicuidad, entendida como la posibilidad del acceso a la nube del proveedor desde cualquier ubicación mediante la conexión a internet, en cualquier momento y a través de múltiples dispositivos[462], con independencia de la localización física de los datos, que generalmente estarán repartidos entre varios servidores de la compañía que preste el servicio. Al margen de la facilidad de uso que supone para los usuarios, lo cierto es que para la investigación de los delitos puede implicar una dificultad considerable, pues, frecuentemente, los datos a investigar se encontrarán en servidores situados en distintas jurisdicciones que, a su vez, serán diferentes respecto de aquella cuya autoridad judicial haya autorizado la medida de investigación. Todo ello exige a los Estados que mantengan una estrecha colaboración entre ellos.

Se ha generalizado entre los usuarios de internet la práctica de almacenar información en depósitos o sitios ajenos al propio dispositivo electrónico. Lo que inicialmente comenzó como un servicio de categoría empresarial que requería complejos artificios técnicos y de preparación en cada uno de los sistemas a utilizar para acceder a la información

---

[461] MERCHÁN MURILLO, A., "Cloud computing: soluciones ante un posible conflicto de leyes", *La Ley mercantil*, 48 (junio), 2018, Wolters Kluwer, fecha de consulta 4 abril 2020.
[462] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 404.

de manera telemática, en la actualidad se ha convertido en un servicio de masas, ofrecido a prácticamente cualquier usuario de internet. En estos supuestos, como decimos, no se archiva la información en el dispositivo electrónico, sino en otro dispositivo, generalmente, un servidor, al que se accede a través de una red, que puede ser de comunicación interna al propio sistema informático (utilizando VPN si fuera necesario) o de comunicación externa, a través de internet.

Se hace necesario matizar que, al referirnos al concepto de *red de comunicación externa*, en realidad nos estamos refiriendo al supuesto más comúnmente conocido, en el que el repositorio se encuentra en servidores ajenos al propio sistema informático y están siendo mantenidos y gestionados por una empresa distinta a la del titular de la información. Son los casos tradicionales supuestos de *cloud computing* que, como decimos, son cada vez más frecuentes no sólo entre las empresas, sino entre los propios particulares. Por otro lado, al referirnos al concepto de *red de comunicación interna*, nos referirnos a supuestos en los que el repositorio se encuentra en servidores vinculados al propio sistema informático, siendo mantenidos y gestionados por el propio titular de la información. Nótese que no es necesario que la conexión respecto de estos últimos sea de red de área local en el sentido físico, gracias a las *virtual private network* o, más concretamente, *wide area network*.

Con independencia de lo anterior, en los supuestos de registros de dispositivos de almacenamientos de datos diferentes respecto del propio dispositivo registrado, la doctrina diferencia tres hipótesis: el acceso al repositorio telemático de datos dentro del registro de dispositivos de almacenamiento masivo de información, regulado en el artículo 588 *sexies* a y b, el registro de información accesible regulado en el artículo 588 *sexies* c, y el registro remoto sobre equipos informáticos, regulado en el artículo 588 *septies* a.

De dichos preceptos resultan los siguientes supuestos[463]:

1. Acceso a datos contenidos en servidores externos de almacenamiento de datos a través del concreto dispositivo cuyo registro ha sido autorizado. En estos casos, a su vez, la doctrina distingue varias modalidades:

[463] *Ibid.*, p. 405.

a. Que el dispositivo electrónico esté abierto o el acceso a su contenido sea posible sin el uso de claves o contraseñas, supuesto en el que es posible su acceso de conformidad con el artículo 588 *sexies* 3 LECrim.

b. Que el dispositivo electrónico se encuentre cerrado pero la autoridad pública conozca las claves de forma legítima, habiendo sido suministrada por el titular, o siendo el resultado de un análisis forense del dispositivo, lo que también queda permitido por el artículo 588 *sexies* 3 LECrim.

c. Cuando el dispositivo se encuentre cerrado y no se conozcan las claves y contraseñas, no será de aplicación el régimen del artículo 588 *sexies* 3 LECrim, y solamente podrá accederse a su contenido almacenado en servidores fuera de España mediante instrumentos de cooperación internacional.

2. Acceso a datos contenidos en servidores externos de almacenamiento de datos, pero no a través del concreto dispositivo cuyo registro haya sido judicialmente autorizado, sino mediante otra técnica de registro remoto. Será aplicable el régimen de los artículos 588 *septies* a y siguientes LECrim.

3. Acceso a datos a través de una red de ordenadores que están interconectados con servidores internos de la propia red, sea una red de área local *strictu sensu* o sea a través de otros sistemas como VPN. Será aplicable el régimen de los artículos 588 *sexies* a, b y c LECrim.

En los dos primeros supuestos, además, hay que destacar que nuestro ordenamiento jurídico atiende exclusivamente al lugar en que se encuentre el dispositivo de almacenamiento a través del cual se acceda al repositorio telemático, de manera que lo único que exige es que aquel se encuentre siempre en territorio español, y con independencia del lugar en que se encuentre el servidor que contenga la información accedida[464].

Respecto de lo anterior, es necesario destacar la situación en la que se encuentran aquellas jurisdicciones en las que se encuentren domiciliadas las matrices de empresas internacionales que presten servicios de computación en la nube. En particular, tenemos que citar el caso *Microsoft Corp. v. United States*, en el que en 2013, Microsoft impugnó

[464] MARTÍN DE LA ESCALERA, A. M., "El registro de dispositivos de almacenamiento masivo de la información", *Revista del Ministerio Fiscal*.

una orden del Gobierno federal emitida al amparo de la *Stored Communications Act (SCA)* de 1986 para entregar el correo electrónico de una cuenta objetivo que estaba almacenada en Irlanda, argumentando que la orden emitida no podía obligar a las empresas estadounidenses a facilitar datos almacenados en servidores fuera de los Estados Unidos. Microsoft perdió inicialmente en el Distrito Sur de Nueva York, afirmando el tribunal que la naturaleza de la orden no estaba sujeta a limitaciones territoriales. Microsoft apeló ante el Tribunal de Apelaciones del Segundo Circuito de los Estados Unidos, que llegó a favor de Microsoft en 2016 e invalidó la orden. En respuesta, el Departamento de Justicia de los Estados Unidos apeló ante el Tribunal Supremo de los Estados Unidos, que decidió examinar la apelación.[465]

Mientras el caso estaba pendiente, El Congreso de los Estados Unidos aprobó la *Clarifying Lawful Overseas Use of Data Act* o *CLOUD Act*, que modificaba la *Stored Communications Act (SCA)* de 1986 para incluir la previsión de que fuera posible obligar a las empresas estadounidenses a facilitar datos almacenados en servidores fuera de los Estados Unidos. El Tribunal Supremo, tras el acuerdo tanto del gobierno como de Microsoft, determinó que la aprobación de la Ley CLOUD y una nueva orden para los datos presentados en virtud de ella hizo que el caso fuera discutible y dejó sin efecto la decisión del Segundo Circuito[466].

Por otro lado, en cuanto al régimen jurídico previsto en el apartado 3 del artículo 588 *sexies* c LECrim, la doctrina recuerda también que la autorización judicial inicial debe contemplar el registro de dicho repositorio telemático de datos, siendo necesario que lo incluya desde el principio o que, en caso de no hacerlo, se solicite su ampliación, sin perjuicio de que, en caso de concurrir urgencia, el Ministerio Fiscal o la Policía Judicial pueda adelantar el registro por sus propios medios[467]. En todo caso, tal y como establece el artículo 19.2 del Convenio de Budapest, el ordenamiento ha de contemplar la posibilidad de que las autoridades competentes amplíen el registro o forma de acceso similar al otro sistema[468].

---

[465]"Microsoft Corp. v. United States", *Wikipedia*, 2020, fecha de consulta 4 abril 2020, en https://en.wikipedia.org/w/index.php?title=Microsoft_Corp._v._United_States&oldid=948795680.
[466]"U.S. top court rules that Microsoft email privacy dispute is moot", *Reuters*, 2018, fecha de consulta 5 abril 2020, en https://www.reuters.com/article/us–usa–court–microsoft–idUSKBN1HO23S.
[467] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 406.
[468] *Ibid.*, p. 407.

5. AGENTE ENCUBIERTO INFORMÁTICO

A. CONCEPTO

El agente encubierto *online* constituye una especialización de la figura tradicional del agente encubierto, que ha sido definido como aquel funcionario policial que se introduce de manera inadvertida en un grupo de delincuencia organizada, presentándose como un miembro natural de ella y participando tanto en su estructura como en sus actividades, con la finalidad de conseguir información sobre las actividades de dicha organización. Decimos que es una especialización porque la medida original ya se encontraba prevista en el artículo 282 *bis* LECrim, pero solamente desde la reforma de 2015 se regula en dicho artículo que la figura del agente encubierto se desarrolle a través de los medios informáticos.

La utilidad del agente encubierto informático se manifiesta, especialmente, en la investigación de los ciberdelitos cometidos por grupos de delincuencia organizada, pues los autores suelen utilizar mecanismos de anonimato y protección frente a la actuación policial.[469]

En esta diligencia es trascendental también la labor de los colaboradores del agente encubierto informático, como informáticos, traductores, personal administrativo, etc. Algunos autores consideran conveniente que la actuación del resto de integrantes del equipo también recibiera regulación específica, teniendo en cuenta que es posible que alguno de los miembros del equipo deba actuar con la organización criminal bajo las pautas del agente encubierto virtual[470]. Todo ello motivaría la necesidad de que la propia autorización judicial previera lo anterior.

La figura del agente encubierto informático surge para responder a las necesidades que aparecen cuando los ciberrastreos, concebidos para investigar el intercambio ilícito de archivos en redes P2P, pierden efectividad cuando los delincuentes mudan su base virtual de operaciones a foros de acceso restringido. En estos casos, la única vía para

[469] *Ibid.*, p. 475.
[470] *Ibid.*, p. 480.

alcanzar los sujetos creadores u originadores del material ilícito o de las redes de distribución es infiltrarse en dichos foros como usuario.[471]

Por último, hay que hacer referencia también a que, en ocasiones, el propio curso de la investigación determina que el agente encubierto informático deba mantener contacto físico con los investigados. Este cambio de ámbito debe quedar previsto en la autorización judicial o ser incluido con posterioridad.

B. RÉGIMEN JURÍDICO

El régimen jurídico de la medida viene establecido en los apartados 6 y 7 del artículo 282 *bis* LECrim: "6. El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 *ter* a. El agente encubierto informático, con autorización específica para ello, podrá 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. 7. En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio."

Como prevé el apartado 6 del artículo 282 *bis* LECrim, el agente encubierto informático puede actuar en el marco de comunicaciones mantenidas en canales cerrados de comunicación, en los que la información se transmite dentro de una vía predefinida y cerrada, ya sea de uno a otro de uno a muchos. Son ejemplos tradicionales de canales cerrados el correo, las llamadas telefónicas, el SMS y el correo electrónico, pero también se incluyen dentro de dicho concepto, conforme a una interpretación funcional del mismo, los sitios web o grupos de conversaciones que tienen el acceso restringido a un grupo cerrado de personas que han de ser específicamente admitidas en el grupo. No obstante, es necesario tener en cuenta que el acceso por un agente encubierto a dichos canales restringidos puede afectar al derecho al secreto de comunicaciones –porque interviene en un

[471] BUENO DE MATA, F., "El agente encubierto en internet: mentiras virtuales para alcanzar la justicia", en *Los retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso Gallego de Derecho Procesal (I Internacional), A Coruña, 2 y 3 de junio de 2011, 2012, pp. 295–306*, 2012, fecha de consulta 14 febrero 2021, en https://dialnet.unirioja.es/servlet/articulo?codigo=4036206.

intercambio de información entre personas determinadas o determinables– y al derecho a la intimidad, pues el consentimiento de acceso al grupo cerrado se presta sobre el engaño efectuado por el poder público. Todo ello determina que la medida deba ser objeto de autorización judicial previa.[472]

De igual modo, en cuanto al ámbito objetivo de la medida, el apartado 6 del artículo 282 *bis* LECrim remite al ámbito previsto en el artículo 588 *ter* a LECrim, que a su vez se refiere a los delitos del artículo 579.1 LECrim (delitos dolosos castigados con pena límite máximo de al menos tres años de prisión, delitos cometidos en el seno de un grupo o autorización criminal o delitos de terrorismo) y a los delitos cometidos a través de instrumentos informáticos o de cualquier tecnología de la información o la comunicación servicio de comunicación. La adición relativa a los ciberdelitos persiguió resolver la posibilidad de utilizar esta medida en supuestos de pornografía o corrupción de menores cuando era difícil acreditar la existencia de organización criminal.

C. UTILIZACIÓN DE ARCHIVOS ILÍCITOS

La posibilidad de que el agente encubierto informático intercambie o envíe por sí mismo archivos ilícitos por razón de su contenido viene prevista en el apartado 7 del artículo 282 *bis* LECrim.

Esta previsión legislativa permite resolver el programa de la utilización de material pornográfico infantil por el agente encubierto, pero también permite un mayor margen de actuación en la investigación de algunas formas de terrorismo.

En todos estos supuestos los miembros del grupo cibernético en el que se quiere infiltrar el policía exigen la aportación de material sensible (como archivos pornográficos) para permitirle el acceso a la red o grupo criminal, y resultaba difícil aceptar que la propia policía pusiera en circulación archivos de contenido ilícito[473]. Es más, para alcanzar el nivel más alto en la organización criminal suele ser necesario entablar contacto personal y directo con miembros del grupo[474].

En cuanto a las posibilidades de utilización de dichos archivos, es posible utilizar imágenes o vídeos obtenidos con ocasión de operaciones anteriores o material creado *ad*

---

[472] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 476.
[473] BUENO DE MATA, F., "El agente encubierto en internet", cit.
[474] VALIÑO CES, A., "Una lectura crítica en relación al agente encubierto informático tras la Ley Orgánica 13/2015", *Diario La Ley*, 8731, 2016, Wolters Kluwer.

hoc utilizando, en el caso de la pornografía infantil, actores mayores de edad caracterizados como menores de edad. La doctrina aprecia una menor victimización en esta segunda posibilidad[475], lo que podría considerarse contradictorio si se compara con aquellos supuestos en los que, utilizando *bots* o señuelos para descubrir a posibles delincuentes en relación con la pornografía infantil, se considera que han delinquido a pesar de que ni siquiera han afectado a titular de bien jurídico alguno.

Por último, merece la pena destacar que el apartado 6 del artículo 282 *bis* LECrim permite analizar el *hash* de los archivos compartidos para identificarlos en la red y detectar quienes han podido acceder al mismo.[476]

D. MODALIDADES DE ACTUACIÓN

Existen distintos niveles de infiltración policial. Cada una de esas ellas merece una respuesta individualizada y concreta que atienda a sus circunstancias particulares.[477] En ese sentido parece distinguirse entre exploraciones o indagaciones realizadas por la policía en canales abiertos de comunicación y por tanto sin autorización judicial previa, conocidas como "*ciberpatrullaje*" y, por otro lado, la estricta infiltración del agente en cubierto online que opera en canales cerrados y que, por tanto, requiere la autorización del artículo 282 *bis* LECrim.

Tal distinción, sin embargo, choca con supuestos de la realidad en los que no está clara la naturaleza de la actuación policial, pues entra a la vez en ambas modalidades. En estos casos, el tratamiento jurídico será directamente dependiente del mayor o menor grado de engaño por parte de la autoridad policial y de la duración que haya tenido dicha infiltración. Así, pueden distinguirse varios supuestos:

Conocimiento por usuario no policía: son los supuestos en los que un particular adquiere conocimiento de una posible conducta delictiva, ya sea un delito que tenga lugar o una oferta de bien o servicio ilícito, que entonces tiene la obligación de transmitir dicha noticia a la autoridad pública para que proceda a la averiguación del hecho.

Navegación del agente policial por la web: observando una oferta de bien o servicio ilícito realizada por un internauta (drogas, sustancias dopantes prohibidas,

---

[475] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 479.
[476] VELASCO NÚÑEZ, E., "Crimen organizado, internet y nuevas tecnologías", cit., p. 264.
[477] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 469.

reclutamiento de terroristas…), o incluso por comentarios ilícitos en redes sociales. Esta actuación no afecta a derecho fundamental alguno porque es sobre fuentes abiertas, ni tampoco supone provocación del delito.

Establecimiento de un contacto puntual con el investigado, ocultando la condición de agente policial, tras la denuncia de un particular o conocer el posible delito por navegación policial: Este contacto puede ocurrir a instancia del propio investigado, que erróneamente intenta ofrecer sus servicios al que desconoce que tiene la condición de agente policial, y por tanto no existe provocación del delito ni es necesaria autorización judicial, y también a instancia del agente policial, en cuyo caso parece entenderse necesario que exista autorización de agente encubierto por el Ministerio Fiscal o por el Juez de Instrucción al amparo del o establecido en el artículo 282 *bis* LECrim.[478] La línea parece quedar marcada cuando se indica que "a diferencia de lo que ocurre en el mundo convencional, en el virtual, la actuación por agente encubierto, salvo que suponga la simple "aceptación" de las típicas ofertas delictivas que realiza el infractor en ese escaparate público que es Internet, generalmente a través de Webs (entrando el agente a manifestar su falsa voluntad de adquirir lo previamente ofertado por el investigado: droga, enrolamiento en organización terrorista, adquisición o intercambio de pornografía infantil) y aflorando el autor inmediatamente, sin otras actividades más complejas ulteriores, lo normal es que la infiltración sólo pueda realizarse con autorización judicial. En efecto, las infiltraciones sencillas (espontáneas, momentáneas y pasivas), que tan sólo afloran la previamente exteriorizada voluntad delictiva de quien ofrece el objeto prohibido (la pornografía, la droga, etc.), ni se pueden confundir con la provocación delictiva, ni precisan de más exteriorizaciones oficiales de la "simulación" del agente encubierto que las justifique que las que autoriza el artículo 282–bis LECrim –EDL 1882/1–, a través de la oportuna autorización del Ministerio Fiscal, "dando cuenta inmediata al Juez", o las que otorgue el propio Juez de Instrucción competente."[479]

Ocultación de la condición de policía, teniendo un contacto con el investigado que se extiende en el tiempo, utilizando una identidad falsa para establecer una relación de confianza con el investigado. Supuestos en los que es necesaria la autorización judicial

[478] *Ibid.*, p. 470.
[479] VELASCO NÚÑEZ, E., "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías – El Derecho – Fiscal, Penal, Sector Jurídico", cit.

prevista por el artículo 282 *bis* LECrim para los supuestos de agente encubierto. Son los supuestos de las STS 767/2007, de 3 de octubre, y de 173/2018, de 11 de abril.[480]

En este sentido, debe tenerse muy presente el peligro de provocación delictiva, que está prohibida, como veremos seguidamente. En tal sentido, se hace fundamental determinar la regularidad de la actuación. No ha de existir ninguna duda respecto del contacto efectuado en la red a través de la identidad encubierta, ni de la inexistencia de inducción al delito. Sentencias como las SSTS 752/2010 y 173/2018 concluyen que no hay provocación cuando el agente interviene en un chat o en una red de descargas P2P u otra de tipo abierto, ni cuando, únicamente, no cierra un contacto iniciado por el que, posteriormente, es investigado[481].

En esta medida de investigación se destaca la importancia de determinar de manera exacta el canal cerrado de comunicación al que ha accedido el agente y la forma de acceso al mismo, así como el tipo de archivo ilícito intercambiado, en su caso, y la información relativa al hash del mismo[482].

E. PROVOCACIÓN DELICTIVA

Finalmente, es necesario hacer referencia a que la actuación del agente encubierto determina el nacimiento de un peligro de provocación delictiva que, en su caso, puede dar lugar a que las pruebas obtenidas se excluyan del proceso.

El concepto de "provocación al delito" o provocación delictiva es incorporado por el artículo 282 *bis* LECrim recogiendo en su apartado 5º) que el agente encubierto estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de esta y no constituyan una provocación al delito.

Conforme a la doctrina establecida por el TEDH en su sentencia de 14 de febrero de 2017 (*Patrascu c. Rumanía*), son dos los criterios o test que debe superar la actuación policial para entender que no concurre provocación a la conducta delictiva.

---

[480] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 473.
[481] DELGADO MARTÍN, J., "La prueba digital. Concepto, clases, aportación al proceso y valoración", cit., p. 469.
[482] QUEVEDO GONZÁLEZ, J., *Investigación y prueba del ciberdelito*, cit., p. 254.

Por un lado, se trata de un test sustantivo, en el que se comprueba si se dan los elementos previstos en la normativa y jurisprudencia para entender que existe provocación delictiva. Se trata, por tanto, de verificar si las autoridades no se limitan a investigar la actividad delictiva de una manera esencialmente pasiva, sino ejerciendo influencia sobre el asunto como para incitar a la comisión de un delito que de otro modo no se habría cometido. En este criterio, resulta relevante el estado en que se encontrase la conducta delictiva cuando se produjo el contacto o colaboración policial, atendiendo especialmente a si el acto delictivo se encontraba ya en curso.

Por otro lado, se atiende al denominado test procesal, en el que se examina si la alegación sobre la existencia de provocación delictiva se efectuó con todas las garantías de un proceso justo, conforme a los principios de contradicción, igualdad de armas y presunción de inocencia, debiendo la acusación demostrar la inexistencia de incitación delictiva. A tal efecto, es posible interrogar al agente encubierto en su calidad de testigo, adoptando las medidas necesarias para garantizar su seguridad.

En nuestra práctica nacional, la STS 204/2013, de 14 de marzo, señalaba que se considera que ha tenido lugar una provocación por parte de la policía cuando los agentes implicados –ya sean miembros de las fuerzas de seguridad o personas que actúen según sus instrucciones– no se limitan a investigar actividades delictivas de una manera pasiva, sino que ejercen una influencia tal sobre el sujeto que le incitan a cometer un delito que, sin esa influencia, no hubiera cometido, con el objeto de averiguar el delito, esto es, aportar pruebas y poder iniciar un proceso.

Finalmente, en cuanto al concepto de delito provocado, la STS 395/2014, de 13 de mayo, señala que el delito provocado se integra por una actuación engañosa del agente policial que supone una apariencia de delito.

La STS 289/2015, de 28 de septiembre, apuntaba que 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 teleológico 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

Finalmente, la STS 863/2011 decía que el delito provocado aparece cuando la voluntad de delinquir surge en el sujeto no por su propia y libre decisión, sino como

consecuencia de la actividad de otra persona, generalmente un agente o un colaborador de los Cuerpos o Fuerzas de Seguridad, que, guiado por la intención de detener a los sospechosos o de facilitar su detención, provoca a través de su propia y personal actuación engañosa la ejecución de una conducta delictiva que no había sido planeada ni decidida por aquel, y que de otra forma no hubiera realizado, adoptando al propio tiempo las medidas de precaución necesarias para evitar la efectiva lesión o puesta en peligro del bien jurídico protegido.

6. BREVE REFERENCIA A LOS REGISTROS REMOTOS

Aunque tampoco existe posibilidad de realizar esta práctica policial sin autorización judicial previa, consideramos de interés incluir en este capítulo una breve referencia a la diligencia de investigación tecnológica de registro remoto, dada la especial injerencia que supone en los derechos fundamentales del investigado y a la vista de las especialidades que puede presentar su práctica.

Los registros remotos (*remote search* o registros *on line*), son aquellos en los que se accede a los datos contenidos en un sistema informático sin necesidad de acceder físicamente al mismo[483]. Hacen uso de una técnica[484] que por la que se accede de manera telemática al sistema registrado, ya sea mediante la instalación de un *software* o empleando los códigos que identifican al terminal.

Debe tenerse en cuenta que los registros remotos suponen un elemento de trascendental importancia en las investigaciones criminales. Generalmente, permiten obtener sustanciosas fuentes de prueba del hecho delictivo, especialmente en los supuestos en que se hace precisa una actuación ágil y rápida que permita salvaguardar las evidencias necesarias o evitar que el daño producido se expanda.

A pesar de ello, también es ampliamente conocido que suponen una afectación de elevada intensidad en los derechos fundamentales a la intimidad, al secreto de las comunicaciones y a la protección de datos personales de la persona investigada, en comparación con los registros tradicionales, articulados sobre el elemento de aprehensión física o material.

---

[483] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 408.
[484] ORTIZ PRADILLO, J. C., "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica", cit., p. 289.

Esto explica que no exista posibilidad de que la Policía Judicial ni el Ministerio Fiscal lleven a cabo registros remotos sin autorización judicial previa, ni siquiera en los casos de urgencia[485], así como que solamente se permita dicha modalidad de investigación en supuestos de delitos concretos[486], además del resto de notas del régimen específico de los artículos 588 *septies* a), b) y c) LECrim respecto de la autorización judicial, ampliación, duración y deber de colaboración.

A pesar de ello, atendiendo precisamente a la intensidad de la injerencia que provoca este tipo de diligencia, se elevan voces desde la doctrina[487] denunciando, en general, el fenómeno del incremento de la intervención pública en la investigación del delito, del que se entiende esta diligencia como máximo exponente, y el riesgo que asumimos de establecer un procedimiento penal con diligencias opacas, con incidencias de alta intensidad en derechos fundamentales y, en fin, de configurar un Estado policial.

Apartándonos del tradicional reproche a la falta de actualización legislativa, debe también reconocerse a España que es uno de los últimos países de su entorno en adoptar este tipo de medidas.

Así, en Estados Unidos, la *Patriot Act* de 2001 ya autorizaba medidas similares, a veces incluso sin autorización judicial necesaria. En Italia, el Código Procesal Penal fue modificado en 2017, introduciendo, entre otras diligencias, el llamado *captatore informatico*. En Francia, desde 2011 se prevé la posibilidad de llevar a cabo registros remotos.

A. CONCEPTO Y ELEMENTO DEFINIDOR

De conformidad con el apartado 1 del artículo 588 *septies* a) LECrim, la medida consiste en "la utilización de datos de identificación y códigos, así como en la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos

---

[485] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 409.
[486] los cometidos en el seno de organizaciones criminales, delitos de terrorismo, delitos cometidos contra menores o personas con capacidad modificada judicialmente, delitos contra la Constitución, de traición y relativos a la defensa nacional, y delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación
[487] GÓMEZ COLOMER, J. L., "El aumento del intervencionismo público en la investigación del delito: Una reflexión al hilo del acto de investigación criminal de registro remoto de equipos informáticos (coloquialmente llamado «del gusano informático»)", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, pp. 817–852*, Ediciones Jurídicas Castillo de Luna, 2020, p. 830, fecha de consulta 25 noviembre 2021, en https://dialnet.unirioja.es/servlet/articulo?codigo=7870306.

o base de datos". El elemento definidor es, por tanto, el acceso al contenido de un dispositivo o sistema informático sin necesidad de proceder a su posesión física.

En particular, la doctrina[488] distingue entre aquellos registros remotos realizados mediante la utilización de datos de identificación y códigos para acceder al dispositivo a registrar de los registros remotos llevados a efectos gracias a la instalación de *software* especializado.

Generalmente, los troyanos son utilizados para robar información, en casos extremos, obtener el control remoto de la computadora, de forma que el atacante consiga acceso de lectura y escritura a los archivos y datos privados almacenados, visualizaciones de las pantallas abiertas, activación y desactivación de procesos, control de los dispositivos y la conexión a determinados sitios de Internet desde la computadora afectada como las páginas pornográficas. Los troyanos están compuestos principalmente por dos programas: un programa de administración, que envía las órdenes que se deben ejecutar en la computadora infectada y el programa residente situado en la computadora infectada, que recibe las órdenes del administrador, las ejecuta y le devuelve un resultado. Generalmente también se cuenta con un editor del programa residente, el cual sirve para modificarlo, protegerlo mediante contraseñas, unirlo a otros programas para disfrazarlo, configurar en que puerto deseamos instalar el servidor, etc. Atendiendo a la forma en la que se realiza la conexión entre el programa de administración y el residente se pueden clasificar en:

- Conexión directa: El atacante se conecta directamente al PC infectado mediante su dirección IP. En este caso, el equipo atacante es el cliente y la víctima es el servidor.
- Conexión indirecta (o inversa): El equipo *host* o víctima se conecta al atacante mediante un proceso automático en el malware instalado en su equipo, por lo que no es necesario para el atacante disponer de la dirección IP de la víctima. Para que la conexión esté asegurada, el atacante puede utilizar una IP fija o un nombre de dominio. La mayoría de los troyanos modernos utilizan este sistema de conexión, donde el atacante es el servidor a la espera de la conexión y el equipo *host* es el cliente que envía peticiones de conexión para recibir órdenes de ejecución remotas bajo su propia demanda.

[488] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 410.

Los troyanos y otros tipos de *malware*, así como muchas utilidades *software* han evolucionado hacia el modelo de conexión inversa debido a la extensión de *routers* que aplican en su mayoría por defecto una capa de seguridad en la red inicial (como el propio NAT) actuando como *firewall* que impide bajo condiciones, conexiones entrantes hacia los clientes de la red salvo que este mecanismo se deshabilite o configure expresamente. De esta manera, es más sencillo crear herramientas que se salten esta protección ocasionando que sean los clientes los que soliciten sus órdenes remotas en lugar de permitir recibirlas.

A pesar de que los troyanos de conexión directa han caído en desuso casi totalmente frente a los de conexión inversa, dentro de los círculos de piratas informáticos se sigue utilizando la denominación de cliente para el equipo atacante y servidor para el equipo víctima, aunque sea incorrecto desde un punto de vista estricto.

La conexión inversa tiene claras ventajas sobre la conexión directa. Esta traspasa algunos firewalls (la mayoría de los *firewalls* no analizan los paquetes que salen de la computadora, pero que sí analizan los que entran), pueden ser usados en redes situadas detrás de un *router* sin problemas (no es necesario redirigir los puertos) y no es necesario conocer la dirección IP del servidor.

Cabe destacar que existen otro tipo de conexiones, que no son de equipo víctima a equipo atacante, sino que utilizan un servidor intermedio, normalmente ajeno a ambos, para realizar el proceso de control. Se suelen utilizar para este propósito los protocolos IRC y el FTP, HTTP, aunque también pueden usarse otros.

B. INSTALACIÓN DE TROYANOS

En esta modalidad de acceso se procede a instalar un *software* que permite acceder al contenido del dispositivo electrónico infectado, haciendo posible que las autoridades escaneen los discos duros y demás unidades de almacenamiento conectadas y remita, de forma remota y automatizada, el contenido a la autoridad responsable de la investigación.[489] Una de las principales ventajas de los troyanos es que permite evitar la intervención de los proveedores de servicios de internet o ISP, por lo que la investigación puede avanzar con independencia de la colaboración de instituciones privadas (frecuentemente

[489] ORTIZ PRADILLO, J. C., "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica", cit., p. 289.

extranjeras) que, por motivos insondables, pueden no tener interés en que la investigación llegue a buen puerto[490].

Por lo general, se emplean troyanos, que son programas que, camuflados con una apariencia de programa útil, en realidad explotan los derechos del usuario del programa de una forma que el usuario no pretende[491]. Los troyanos están diseñados para permitir a un individuo el acceso remoto a un sistema. Una vez en ejecución, el atacante puede acceder al sistema de forma remota y realizar diferentes acciones sin necesitar permiso[492].

Generalmente, se reconoce[493] que la instalación de troyanos resulta útil en supuestos variados, como cuando el dispositivo electrónico se encuentra en movimiento constante –caso de los *smartphones* y demás dispositivos portátiles, cuando acceder al lugar donde se halle suponga un peligro para la vida de los agentes o para la integridad de la información o del propio equipo informático, o cuando es necesario acceder al equipo informático en directo para capturar las claves utilizadas[494]. En tal sentido, se ha afirmado que los troyanos proporcionan "a las autoridades la posibilidad de acceder de forma rápida a una valiosa fuente de prueba (la información almacenada en el equipo informático), pero deben establecerse legalmente las circunstancias, requisitos y límites bajo los cuales estos registros remotos (transfronterizos o no) resultarán admisibles"[495].

La doctrina tampoco desatiende las múltiples ventajas que los troyanos pueden tener en esas circunstancias. Así, se destaca que tal modalidad de investigación, captando mucha más información, exige menos efectivos investigadores que cualquier otra. Además, es fácilmente expandible, en la medida en que se instala a través de internet, lo que le aporta un elemento de ubicuidad muy necesario en la *ciberinvestigación*. Permite, igualmente, enfocar la actividad investigadora, en la medida en que también puede programarse para buscar y seleccionar la información más relevante a través del uso de

---

490 "Van den Eynde | Prueba Electrónica (III): Cloud, Troyanos, Herramientas forenses, etc.", fecha de consulta 6 abril 2020, en https://eynde.es/es/prueba–electronica–cloud–troyanos/.
491 LANDWEHR, C.; BULL, A.; MCDERMOTT, J.; CHOI, W., "A Taxonomy of Computer Program Security Flaws", *ACM Computing Surveys – CSUR*, vol. 26, 1993.
492 "SANS Institute: Reading Room – Malicious Code", fecha de consulta 5 abril 2020, en https://www.sans.org/reading–room/whitepapers/malicious/paper/953.
493 DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 411.
494 ORTIZ PRADILLO, J. C., "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica", cit., p. 290.
495 ORTIZ PRADILLO, J. C., "Propuestas para la lucha contra el cibercrimen: la obtención transfronteriza de prueba electrónica en la Unión Europea", *Revista General de Derecho Procesal*, 20, 2010, p. 9.

búsquedas automatizadas[496]. Sobre esto último, tal vez hay que destacar que supondría un tratamiento adicional de la información que, por un lado, puede permitir búsquedas y rastreos más respetuosos con los derechos fundamentales del investigado (al recabar solamente la información que contenga determinadas etiquetas), pero, por otro, implica una serie de atribuciones a la autoridad investigadora que quizás harían exigible que dicho extremo se incluyera en el auto que dictara el juez de instrucción autorizando la medida.

C. TIPOS Y UTILIDADES DE TROYANOS

Existen multitud de troyanos diferentes en función de la finalidad a la que sirven. Nosotros vamos a destacar aquellos que, por sus características, reúnen más probabilidades de ser empleados por la policía.

Backdoors: un troyano de estas características permite al atacante conectarse remotamente al equipo infectado. Las conexiones remotas son comúnmente utilizadas en informática y la única diferencia entre estas y un *backdoor* es que, en el segundo caso, la herramienta es instalada sin el consentimiento del usuario. La tecnología aplicada para acceder remotamente al equipo no posee ninguna innovación en particular ni diferente a los usos inofensivos con que son utilizadas estas mismas aplicaciones. Una vez que el atacante accede al ordenador del usuario, los usos que puede hacer del mismo son variados, según las herramientas que utilice: enviar correos masivos, eliminar o modificar archivos, ejecución de archivos, reiniciar el equipo o usos más complejos como instalar aplicaciones para uso malicioso (por ejemplo: alojamiento de sitios web de violencia o pornografía de menores).

***Keyloggers*: s**e ha entendido como un complemento técnico que se emplea ante la necesidad de captar actuaciones interactivas no monitorizables en el investigado, especialmente su clave y contraseña, y previa autorización judicial[497]. Los *keyloggers*[498] son uno de los tipos más utilizados para obtener información sensible de los usuarios. Los troyanos de esta clase instalan una herramienta para detectar y registrar las pulsaciones del teclado en un sistema. Pueden capturar información relativa contraseñas de correos, cuentas bancarias o sitios web, entre otras, y abrir la puerta para atentar contra

[496] VELASCO NÚÑEZ, E., "ADSL y troyanos: intervención de sus datos y telecomunicaciones en la investigación penal", *La ley penal: revista de derecho penal, procesal y penitenciario*, 82, 2011, Wolters Kluwer.
[497] VELASCO NÚÑEZ, E., "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías – El Derecho – Fiscal, Penal, Sector Jurídico", cit.
[498] del inglés Key = Tecla y Log = Registro

información sensible del usuario. La información capturada es enviada al atacante generalmente, en archivos de texto con la información. Estos troyanos no son una amenaza para el sistema sino para el usuario y su privacidad. Los datos recolectados pueden ser utilizados para realizar todo tipo de ataques, con fines económicos o, simplemente, malignos[499]. Una de las más destacadas utilidades de los *keyloggers* es que permiten a la autoridad averiguar las contraseñas de cifrado utilizadas por los investigados para proteger la información. Ello es especialmente útil en un ordenamiento jurídico como el nuestro, en el que de momento no se sanciona la negativa del investigado a facilitar las contraseñas de su cifrado, al contrario de lo que sucede, por ejemplo, en Reino Unido, en el que la *Regulation of Investigatory Powers Act*, en su apartado 39, ya permitía en el año 2000 establecer sanciones por dicha negativa.[500]

***Botnets*:** Los troyanos botnets son utilizados para crear redes de equipos zombis (*botnets*). El atacante utiliza el troyano (generalmente combinado con herramientas de *backdoors*) para controlar una cantidad importante de ordenadores y así poder utilizarlos para cualquier fin maligno. Pueden ser utilizados para enviar spam o para realizar ataques de denegación de servicio (DoS); estos consisten en saturar un sitio web generando más accesos y requerimientos de los que puede soportar y provocando la baja del servicio.

***Proxy*:** este tipo de troyanos instalan herramientas en el ordenador que le permiten al atacante utilizar el ordenador infectado como un servidor *proxy*. Un *proxy* es un servidor que da acceso a otros ordenadores a Internet a través de él. En este caso, el atacante utiliza el ordenador infectado para acceder a la web a través de él, enmascarando su identidad.

***Password Stealer*:** se encargan de robar información introducida en los formularios en las páginas web. Pueden robar información de todo tipo, como direcciones de correo electrónico, *logins*, *passwords*, PINs, números de cuentas bancarias y de tarjetas de crédito. Estos datos pueden ser enviados por correo electrónico o almacenados en un servidor al que el delincuente accede para recoger la información robada. En la mayoría de sus versiones, utilizan técnicas *keyloggers* para su ejecución y son similares a estos.

---

[499] como modificar las contraseñas de las cuentas de acceso a algún servicio

[500] "Van den Eynde | Retos relacionados con la prueba electrónica (parte I)", fecha de consulta 6 abril 2020, en https://eynde.es/es/prueba–electronica–1/.

***Dialer*:** crean conexiones telefónicas en el ordenador del usuario, utilizando las funcionalidades del módem. Estas conexiones son creadas y ejecutadas de forma transparente a la víctima. Generalmente, se trata de llamados de alto costo a sitios relacionados con contenido adulto en Internet. Este tipo de troyanos crean un daño económico al usuario, el ordenador no se ve afectado por hacer una llamada telefónica.

***Cementery*:** novedad en este tipo de *malware*, apareciendo por primera vez en 2018. Su principal propósito es el robo de información multimedia y documentos. Trabaja exclusivamente en la papelera de reciclaje, ya que es el área más vulnerable de cualquier ordenador. Cambia las propiedades de los archivos infectados, alterando su fecha de creación, tipo de archivo o fecha de eliminación del mismo, comúnmente con fechas recientes o incluso semanas próximas, provocando que un antivirus no pueda detectarlo ya que el archivo todavía "no fue creado".

Algunas de las operaciones más comunes a las que sirven los troyanos son: utilización la máquina como parte de una *botnet* (por ejemplo, para realizar ataques de denegación de servicio o envío de *spam*), instalación de otros programas (incluyendo aplicaciones maliciosas), robo de información personal: información bancaria, contraseñas, códigos de seguridad, robo de archivos varios, etcétera, borrado, modificación o transferencia de archivos (descarga o subida), borrado completo del disco, ejecución o finalización de procesos, apagado o reiniciado del equipo, captura de las pulsaciones del teclado, capturas de pantalla, llenado del disco duro con archivos inútiles, monitorización del sistema y seguimiento de las acciones del usuario, captura de imágenes o videos a través de la webcam, si tiene, expulsar la unidad de CD, cambiar la apariencia del sistema, etc.

Por último, hay que dejar constancia de que los troyanos no solamente pueden ser empleados en ordenadores, sino también en dispositivos móviles y tabletas. Dado el uso personal de estos dispositivos, las acciones que un atacante puede realizar en estos dispositivos comprende las ya descritas, más otras específicas derivadas de la naturaleza privada de la información que se almacena en estas plataformas, como captura de los mensajes entrantes y salientes de aplicaciones de mensajería, captura del registro de llamadas, acceso y modificación de contactos en la agenda, habilidad para efectuar llamadas y enviar mensajes de texto, adquirir conocimiento de la posición geográfica del dispositivo mediante GPS.

7. LOS HALLAZGOS CASUALES

La figura del hallazgo casual ha sido regulada de manera expresa con ocasión de la reforma de la LECrim operada 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. Se trata de la primera ocasión en que es abordada de un modo claro por el legislador. Hasta entonces, solamente la doctrina y la jurisprudencia se habían ocupado de esta cuestión[501].

A. CONCEPTO DE HALLAZGO OCASIONAL

Originariamente, se ha venido entendiendo que hallazgo casual sería todo aquel descubrimiento fortuito de cualquier elemento de la realidad que no estuviera siendo inicialmente buscado[502], sin importar si dicho descubrimiento se producía en el seno de una diligencia de investigación restrictiva de derechos fundamentales o en cualquier otro momento, incluso previo a la apertura de la fase de instrucción. Con "hallazgo casual" se refería la jurisprudencia, por tanto, a todo descubrimiento no expresamente perseguido[503].

Posteriormente, dichas concepciones generalistas se han superado por la doctrina[504], que ha establecido definiciones no sólo más concretas, sino que sitúan al concepto de "hallazgo casual" en una situación jurídica muy específica, que exige para su apreciación la existencia de una investigación previa en la que se haya autorizado una injerencia de derechos fundamentales de la que derive dicho hallazgo. Queda, por tanto, descartado que sean hallazgos casuales los supuestos en que el descubrimiento no tenga lugar en el marco descrito.[505]

La STS 377/2018, de 23 de julio, recordaba, respecto de los hallazgos casuales, que estos se producen cuando, habiéndose obtenido la correspondiente habilitación

---

[501] NADAL GÓMEZ, I., "El Régimen de los hallazgos casuales en la Ley 13/2015, de modificación de la ley de Enjuiciamiento criminal", cit., p. 3.
[502] DÍAZ CABIALE, J. A.; MARTÍN MORALES, R., *La garantía constitucional de la inadmisión de la prueba ilícitamente obtenida*, 2001, p. 190.
[503] NADAL GÓMEZ, I., "El Régimen de los hallazgos casuales en la Ley 13/2015, de modificación de la ley de Enjuiciamiento criminal", cit., p. 5.
[504] ECHARRI CASI, F. J., "Prueba ilícita: conexión de antijuridicidad y hallazgos casuales", *Revista del poder judicial*, 69, 2003, Consejo General del Poder Judicial; KAPPLER, S. I. Á. DE N., "Los descubrimientos casuales en el marco de una investigación penal: (Con especial referencia a las diligencias de entrada y registro en domicilio).", *Riedpa: Revista Internacional de Estudios de Derecho Procesal y Arbitraje*, 2, 2011, Del Blanco Editores.
[505] NADAL GÓMEZ, I., "El Régimen de los hallazgos casuales en la Ley 13/2015, de modificación de la ley de Enjuiciamiento criminal", cit., p. 7.

judicial para la práctica de una diligencia que afecta a los derechos fundamentales del sujeto investigado, con motivo de la persecución de una serie de conductas delictivas concretas y determinadas, aparecen fuentes de prueba relativas a otro u otros delitos distintos de los cuales no se tenían noticias con anterioridad.

B. RÉGIMEN JURÍDICO

El precepto nuclear, que contiene la regulación de dicho instituto, es el artículo 579 *bis* LECrim que, en tres apartados diferenciados, dispone que "1. El resultado de la detención y apertura de la correspondencia escrita y telegráfica podrá ser utilizado como medio de investigación o prueba en otro proceso penal. 2. A tal efecto, se procederá a la deducción de testimonio de los particulares necesarios para acreditar la legitimidad de la injerencia. Se incluirán entre los antecedentes indispensables, en todo caso, la solicitud inicial para la adopción, la resolución judicial que la acuerda y todas las peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen. 3. La continuación de esta medida para la investigación del delito casualmente descubierto requiere autorización del juez competente, para la cual, este comprobará la diligencia de la actuación, evaluando el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento. Asimismo, se informará si las diligencias continúan declaradas secretas, a los efectos de que tal declaración sea respetada en el otro proceso penal, comunicando el momento en el que dicho secreto se alce." A dicho contenido remitirá posteriormente el artículo 588 *bis* i) LECrim, cuando indica que "el uso de las informaciones obtenidas en un procedimiento distinto y los descubrimientos casuales se regularan con arreglo a lo dispuesto en el artículo 579 bis."

Al estudiar el contenido del artículo 579 *bis* LECrim, la doctrina ha concluido[506] que contiene una doble perspectiva respecto del hallazgo casual, la de su utilidad investigadora como punto de partida de una instrucción o *notitia criminis*, y la de su validez probatoria como fundamento de la posterior sentencia. Esta doble perspectiva coincide con la mantenida por la jurisprudencia, que recuerda que en los hallazgos casuales hay

[506] *Ibid.*, p. 3.

que distinguir dos funciones, la probatoria y la investigadora, como indica la STS 377/2018, de 23 de julio[507].

La referida STS 377/2018 también se refiere a los supuestos en que se le podrá atribuir una u otra eficacia, cuando recuerda que "1) Si los hechos descubiertos tienen conexión (artículo 17 LECrim) con los que son objeto del procedimiento instructorio, los hallazgos surtirán efectos tanto de investigación como de prueba.2) Si los hechos ocasionalmente conocidos no guardasen esa conexión con los causantes del acuerdo de la medida y aparentan una gravedad penal suficiente como para tolerar proporcionalmente su adopción, se estimarán como mera "notitia criminis" y se deducirá testimonio para que, siguiendo las normas de competencia territorial y en su caso las de reparto, se inicie el correspondiente proceso. Todo ello determina que la jurisprudencia se pronuncie favorablemente con que un descubrimiento causal sea lícito y no afecte a la presunción de inocencia, considerándose una nueva fuente de prueba de cargo, enervante y motivadora de una sentencia condenatoria."

Como se puede comprobar, se exigen una serie de requisitos que han de cumplirse para que dicha eficacia sea posible. Esos requisitos apuntan directamente a la legitimidad de la injerencia que dio lugar al hallazgo casual y de las actuaciones posteriores que se realicen tras dicho hallazgo. Esto es, "el precepto consagra la necesidad de constatar la legalidad precedente y subsecuente en la obtención del hallazgo casual, como requisito ineludible para otorgarle cualquier valor en el mismo o en otro proceso"[508]. En ese sentido, hay que recordar que será necesario "llevar a cabo una comprobación acerca de si la Policía Judicial o el Fiscal que solicitaron la medida tendrían que haber previsto la posibilidad de la aparición de tal hallazgo, que no sería entonces casual, y por consiguiente denegarle tal carácter o, por el contrario, entender que vistas las circunstancias era imposible su previsión anticipada, y ha de otorgarse naturaleza de hallazgo casual" [509].

---

[507] Cuando concluye que "para clarificar el problema de los hallazgos casuales es necesario distinguir entre función probatoria y función investigadora. En el primer caso, los descubrimientos casuales no podrán utilizarse como fuente de prueba en un proceso distinto de aquel en que se obtienen, quedando limitada su eficacia a los supuestos de conexión del artículo 17 LECrim. Respecto de los efectos investigadores, los descubrimientos casuales podrán actuar como *notitia criminis* , que daría lugar al inicio de una instrucción independiente para averiguación y comprobación del nuevo hecho delictivo."

[508] NADAL GÓMEZ, I., "El Régimen de los hallazgos casuales en la Ley 13/2015, de modificación de la ley de Enjuiciamiento criminal", cit., p. 4.

[509] SÁNCHEZ MELGAR, J., "La nueva regulación de las medidas de investigación tecnológica. Estudio de su Parte General", *Práctica penal: cuaderno jurídico*, 82, 2016, Sepin Editorial Jurídica.

Tal postura era mantenida por la doctrina[510] incluso con anterioridad a la entrada en vigor de la LO 13/2015, al entender que la LECrim, al no prohibir el hallazgo casual, lo admitía siempre que se apreciara flagrancia, pues, como señala la STS de 3 de septiembre de 2003, los hallazgos casuales "se instalan en la nota de la flagrancia, por lo que, producida tal situación, la inmediata recogida de los mismos no es sino consecuencia de la norma general contenida en el artículo 286 de la ley procesal". En cualquier caso, tampoco puede obviarse la elevada dificultad que planteará acreditar la flagrancia[511].

Se ha entendido que el juez competente para decidir la continuación de la medida de investigación[512] es el que ha dictado la resolución judicial autorizando la medida de investigación en la que se produce el hallazgo casual, independientemente de que resulte competente para conocer el nuevo procedimiento que se incoe con ocasión del hallazgo casual o de que dicho conocimiento corresponda a otro órgano judicial.[513]

En todo caso, tras el hallazgo casual y la ulterior autorización judicial, lo actuado habrá de ser remitido al Juzgado competente de conformidad con las normas de competencia territorial y reparto. En tal sentido, hay que estar lo dispuesto en el artículo 579 *bis* 3.

C. EL CONTEXTO NECESARIO PARA QUE SUCEDA EL HALLAZGO CASUAL

Las diligencias de investigación –como conjunto de actuaciones que se realizan sobre la parte de la realidad, personas o cosas que interesa investigar en el marco de un proceso penal– constituyen el principal vehículo para la introducción de hechos en el proceso. Como tales, provocan la aparición de los llamados hallazgos casuales cuando los hechos hallados son distintos de aquellos que se pretendía investigar.[514]

Hay que tener presente que el nuevo artículo 579 *bis* LECrim sitúa la aparición y problemática de los hallazgos no en cualquier diligencia, sino en el seno de algunas de las que afectan a los derechos fundamentales. En este contexto, el precepto de referencia

---

[510] VELASCO NÚÑEZ, E., "La investigación de delitos cometidos a través de Internet y otras nuevas tecnología", cit., p. 85.
[511] CASTILLEJO MANZANARES, R., "Alguna de las cuestiones que plantean las diligencias de investigación tecnológica", *Revista de derecho y proceso penal*, 45, 2017, Aranzadi Thomson Reuters.
[512] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 379.
[513] *Ibid.*
[514] NADAL GÓMEZ, I., "El Régimen de los hallazgos casuales en la Ley 13/2015, de modificación de la ley de Enjuiciamiento criminal", cit., p. 21.

permite que los hallazgos puedan ser utilizados como medios de investigación y de prueba, pero siempre que pueda acreditarse la legitimidad de la medida.

Ahora bien, para que pueda otorgarse valor probatorio a lo obtenido en los actos de investigación es necesario que, entre otros requisitos, se haya seguido con el régimen legal previsto para cada uno de ellos. Dicho régimen legal vendrá dado por la normativa específica establecida en la LECrim para cada diligencia y por el necesario respeto a los derechos fundamentales. La alternativa será la imposibilidad de su valoración conforme al artículo 11. 1 LOPJ[515].

Por lo tanto, la posible utilización de tales hallazgos está supeditada a que la medida en la que se originó fuera legítima. Debe hacerse especial referencia al escrito de solicitud, a la resolución por la que se autoriza y se prorroga la medida en su origen. Más allá del propio descubrimiento, una vez producido este, se requiere que su investigación sea también autorizada por el juez competente. A ello deberán sumarse las cuestiones ya vistas acerca de la competencia del juez que acuerde la continuación de la medida en relación con la configuración del objeto del proceso y la posible alteración de las reglas de la competencia a consecuencia de la acumulación de los objetos conexos, según las reglas del artículo 17 LECrim. Solo cuando se haya cumplido con todas estas exigencias de legalidad ordinaria y constitucional, los hallazgos casuales podrán desplegar toda la eficacia que la nueva normativa les reconoce.

Cuando se analiza su contenido desde la perspectiva de la posible aparición de descubrimientos ocasionales, se aprecia como estos suponen una quiebra de varios de los elementos que han servido para dotar de legalidad constitucional a la medida[516].

Precisamente, para aclarar tal situación se manifestó el pleno de la Sala Segunda del Tribunal Supremo en su acuerdo de 26 de junio de 2009. En este acuerdo se trataba precisamente de la valoración de escuchas telefónicas, procedentes de otras diligencias distintas. Básicamente se establecía la posibilidad de discutir de forma contradictoria la legitimidad en la obtención de la fuente de prueba en otro procedimiento y la posibilidad que tiene quien pretende la utilización de tal medio de prueba de acreditar la legitimidad, cuando la misma haya sido impugnada por la otra parte. En definitiva, se establecía que el medio de prueba que tenía su origen en una fuente de prueba originada en un proceso

[515] *Ibid.*, p. 23.
[516] *Ibid.*, p. 27.

distinto podría tener valor si estaba claro su origen y si surgía de una investigación inicial lícita.

Las dudas aparecían cuando se distinguía entre aquellos supuestos en los que el inicio o el traspaso a un segundo proceso se realizaban de oficio por el órgano que estaba conociendo de la primera investigación y aquel en que tal traspaso se hacía de oficio por la policía que acude a otro órgano judicial, sin el respaldo de ningún otro juzgado. En estos últimos casos, esto es, cuando se ocultaba la fuente de origen o cuando el juez inicial tenía competencia para conocer de ese nuevo descubrimiento, bien por la identidad o por la conexión con el objeto inicial, es cuando nos encontrábamos con supuestos claros de ilicitud de la actuación policial, que conllevarían la ilegalidad del medio probatorio. El elemento decisivo de la ilegalidad en estos casos se encuentra fundamentalmente en la ocultación de la información al nuevo juez del que se pretende autorice o que debería autorizar la medida en cuestión. En este sentido, pueden consultarse repetidas sentencias del Tribunal Supremo, desde la núm.6/2007, de 10 de enero, la 864/2012 de 16 de octubre, o la más reciente de la Audiencia Provincial de Barcelona núm. 134/2015, de 24 de febrero, que aplica al caso concreto la doctrina conforme a la cual lo esencial es que "exista conocimiento temporáneo por parte del juez del nuevo delito, y ya en las mismas diligencias o en otras, autorice la investigación con base en lo hallado en la investigación inicial"[517].

Por lo tanto, puede decirse que los requisitos para otorgar valor a los descubrimientos causales son[518]:

a) Que la diligencia sea válida. Para su constatación se debe proceder a la expedición de los testimonios previstos en el apartado 2 del artículo 579 *bis* LECrim.

b) Que todas las actuaciones que se hayan seguido a partir del conocimiento del descubrimiento ocasional tengan su propio marco de legalidad, enjuiciado de forma autónoma.

c) Que todas las autorizaciones y actuaciones necesarias para cumplir con dicho régimen de legalidad hayan sido acordadas por el juzgado competente.

---

[517] *Ibid.*, p. 41.
[518] *Ibid.*, p. 45.

d) Necesaria evaluación positiva por parte del juez que decide continuar con la medida, de las circunstancias en las que se produjo el hallazgo y en especial, de la imposibilidad de haber solicitado su inclusión en la diligencia de investigación.

Cabe también plantearse si el procedimiento previsto en la segunda parte del apartado 3 del artículo 588 *sexies* c) y en el apartado 4 del mismo precepto que permite por razones de urgencia a la policía o al Ministerio Fiscal ampliar el registro o acceder inmediatamente al examen directo de los datos contenidos en el dispositivo incautado sería también aplicable a los supuestos en los que afecta a ese delito nuevo. A mi juicio, no debe haber obstáculo en que ello sea así, pero siempre sujeto al régimen especial previsto para estos casos y que obliga a la inmediata comunicación al juez y en todo caso dentro del plazo máximo de 24 horas y la posterior resolución motivada de aquel en el plazo de 72, en la que confirme o revoque dicha actuación[519].

Por su parte, la STS 377/2018, de 23 de julio afirma que los hallazgos causales, para que sean válidos desde el punto de vista de la licitud probatoria (art 11.1 LOPJ), deben reunir los siguientes requisitos:

a) Principio de buena fe según STS de 26 de mayo de 2011: encontrar una prueba incriminatoria se ha de deber a la consecuencia lógica de que la previa medida judicial restrictiva del derecho (por ejemplo, a la inviolabilidad del domicilio) se ajusta a ley.

b) Igualmente tiene que haber flagrancia delictiva, que sea tan evidente que, pese a no ser lo esperado por el instructor, puede servir como posterior prueba de cargo.

En ese sentido, se puede concluir que se encontrará el hallazgo durante el curso de una previa medida jurisdiccional restrictiva de derechos fundamentales y libertades públicas. A su vez, esa medida restrictiva previa tiene que ser legítima: es decir, naturaleza jurisdiccional, adoptada por un juez competente, proporcional al delito grave con pena de libertad grave con trascendencia social.

Así, la STS 18–2–1994 afirma que si las pruebas casualmente halladas hubieran podido ser obtenidas mediante el procedimiento en el que se encontró, nada impide que tales pruebas puedan ser valoradas. Por su parte, la STS 465/1998 declara la existencia

[519] *Ibid.*, p. 54.

de una posición favorable a la licitud de la investigación de aquellas otras conductas delictivas que nacen de los hallazgos acaecidos en un registro judicialmente autorizado.

Finalmente, en la jurisprudencia del Tribunal Constitucional se recoge un idéntico tratamiento con relación al hallazgo casual. Así, la STC 41/1998 afirma que el que se estén investigando unos hechos delictivos no impide la persecución de cualesquiera otros distintos que sean descubiertos por casualidad al investigar los primeros, pues los funcionarios de policía tienen el deber de poner en conocimiento de la autoridad penal competente los delitos de que tuviera conocimiento, practicando incluso las diligencias de prevención.

En fin, es indubitado que el hallazgo casual de efectos que pudieran ser constitutivos de un objeto delictivo obliga a los funcionarios de la policía judicial que realizan la investigación y, en su caso, a los funcionarios de la Administración de Justicia, a su intervención y a la realización de aquellas diligencias necesarias para la investigación del delito para su persecución.

D. SUPUESTOS PROBLEMÁTICOS

En este apartado hemos podido estudiar el cauce debido que han de seguir los descubrimientos fortuitos, pero no quedan respondidos así todos los interrogantes que pueden formularse –o plantearse en la práctica– al respecto. Así, por ejemplo, ¿qué debería suceder en el caso de que el "hallazgo" tuviera lugar antes de comenzar alguna diligencia de investigación autorizada judicialmente? En la práctica de nuestros tribunales no siempre la solución que se alcanza coincide con el "deber ser" que reclama la doctrina.

En ese sentido, traemos a colación la sentencia del Tribunal Superior de Justicia de Navarra, Sala de lo Civil y Penal, núm. 14/2019, de 2 de julio, que desestima un recurso de apelación planteado contra la sentencia de la Audiencia Provincial de Navarra núm. 9/2019, de 15 de enero. A nuestro juicio, se trata de una sentencia fundamental en el marco de la regulación actual de las diligencias de investigación tecnológicas y la protección de los derechos fundamentales que puedan verse afectados por ellas, y se encuentra íntimamente vinculada con el estado de la figura de la prueba ilícita, cuyo régimen recibió

una contundente modificación con ocasión de la sentencia del Tribunal Constitucional núm. 97/2019, de 16 de julio[520].

La sentencia en cuestión resuelve un recurso de apelación presentado por la acusación particular y el Ministerio Fiscal contra la sentencia de la Audiencia Provincial de Navarra núm. 9/2019, de 15 de enero, en un procedimiento ordinario seguido por delitos de abusos sexuales sobre menores y tenencia de pornografía infantil.

En lo que aquí interesa, los hechos fueron los siguientes: el día 14 de junio de 2016, una mujer, entregó en el Servicio de Atención al Ciudadano del Puesto de la Guardia Civil un bolso de hombre y una carterita que, según indicó, se había encontrado en uno de los paseos de la localidad. En el interior del bolso había documentación suficiente para entender que pertenecía a un hombre, denominado Luis Ángel en la sentencia. En el interior de la carterita había una memoria USB y dos tarjetas de memoria SD. El agente de la Guardia Civil, entendemos que para intentar encontrar algún archivo que diera alguna pista sobre el titular de dichos efectos (y, por tanto, de la carterita, si es que fue entregada separadamente del bolso), procedió a abrir los archivos que contenían. Entre muchos con nombres evidentes, como "DNI", "*curriculum vitae*", etc., encontró y revisó una carpeta denominada "Trance", que resultó contener archivos de pornografía infantil. Al día siguiente, 15 de junio de 2016, el agente de la Guardia Civil hizo entrega a su propietario tanto del bolso como de la cartera con la memoria USB y las tarjetas SD. Por la Policía Judicial no se remite notificación alguna al Juzgado hasta el 21 de junio de 2016, fecha en la que, habiendo revisado el contenido de la carpeta "Trance", se presentó oficio solicitando mandamiento para la entrada y registro en el domicilio del propietario e intervención de sus ordenadores personales, discos duros, memorias digitales, CD, DVD u otros objetos susceptibles de haber sido usados para la ocultación de los ilícitos penales y documentación relacionada con cualquiera de tales efectos, en cualquier soporte en que se hallaran, documental o telemático, como ordenadores personales, teléfonos, agendas personales, etc, así como para la extracción y exploración, tanto mecánica como manual, de toda la información contenida en dispositivos de almacenamiento de memoria (ordenadores, tablets, CD, DUD, dispositivos USB, etcétera) que se encontraran en el registro domiciliario. Todo ello fue autorizado hasta en dos ocasiones (fue necesario

[520] Que ha perdido su carácter como garantía ínsita en cada derecho fundamental para ser considerada una garantía procesal, que podrá o no operar en función de si afecta al principio de proceso justo.

repetir el registro). Toda la instrucción posteriormente realizada deriva directamente de las diligencias y actuaciones que se acaban de reseñar.

Se evidencia de esta manera, por tanto, que el acceso por parte del agente de la Guardia Civil a la carpeta "trance" fue el elemento inicial de investigación a partir del cual se tuvo noticia del delito, y que motivó que se presentaran las correspondientes y posteriores solicitudes de acceso ante la autoridad judicial. Debe tenerse en cuenta que dicho primer acceso ocurrió sin autorización del individuo afectado por la medida y tampoco de la autoridad judicial, y no estando justificado que fuera necesario acceder a dichos archivos para averiguar la titularidad del propietario de la cartera, ni que concurriera urgencia alguna, pues su titular no reclamó su devolución, ni consta que tuviera constancia de la pérdida.

Son bien sabidas las consecuencias que corresponden a aquellos supuestos que violentan derechos y libertades fundamentales, conforme al artículo 11.1 LOPJ. Así pues, cuando los hallazgos casuales consistieran en la utilización de medidas restrictivas interpuestas con la finalidad de aparentar un descubrimiento que se sabe que no será casual[521]. En tal sentido, la STS de 3 de julio de 2003 concluía que "si se advirtiera que todo ello pudiera responder, en realidad, a un designio intencionado de los funcionarios solicitantes del registro que fraudulentamente hubieran ocultado al juez autorizante, por las razones que fueren, el verdadero motivo de su investigación, la violación del domicilio habría de ser considerada nula". Esta nulidad pretende disuadir a los poderes públicos de adoptar estrategias espurias completamente incompatibles con la vigencia de un Estado de derecho.

Pues bien, cuando llegó el momento del enjuiciamiento, la Audiencia Provincial concluyó que debía considerar como ilícitas todas las pruebas obtenidas mediante las diligencias de investigación tecnológicas, porque estas se habían obtenido vulnerando los artículos 18.1 y 18.4 CE. Partiendo de que el procedimiento tuvo su origen en el acceso efectuado por el agente de la Guardia Civil el día 14 de junio de 2016 a los soportes informáticos del investigado, examinando las tarjetas SD y el USB y realizando una copia de salvaguarda de las mismas –cuando tal extensión no era necesaria para conocer la identidad de su propietario–, el tribunal recuerda que la Policía Judicial aguardó hasta el

[521] VELASCO NÚÑEZ, E., "La investigación de delitos cometidos a través de Internet y otras nuevas tecnología", cit., p. 85.

día 21 de junio de 2016 para poner a disposición de la autoridad judicial la referida copia de seguridad.

La consecuencia de lo anterior fue que la comunicación en el preceptivo plazo de 24 horas, establecido en el artículo 588 *sexies* c LECrim, cuando indica que "en los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida prevista en los apartados anteriores de este artículo, la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, […]", fue completamente obviada.

En su decisión, el tribunal aportó extractos de diferentes pronunciamientos que, por su relevancia, debemos reproducir aquí.

Así, expone la STS 297/2015, de 8 de mayo, que "el fin nunca justifica los medios" por muy relevante que se considere el delito perseguido; de manera que el ejercicio del "ius puniendi" del Estado no puede prescindir de las limitaciones que el respeto de los derechos fundamentales impone en la persecución de los delitos, entre ellas, las que la repetida LO 13/2015, de 5 de octubre, ha introducido en la Ley de Enjuiciamiento Criminal y la que proviene del artículo 11.1 LOPJ en cuanto dispone que "no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales".

Del mismo modo, alude a la STS 511/2015 de 21 de julio para recordar que actuar de otro modo, desconociendo la vulneración de los derechos fundamentales que se ocasiona en tales conductas, supone utilizar "lo que puede calificarse de maquiavelismo probatorio, incurriendo en dos actuaciones incorrectas. En primer lugar, calificar como confesión, a efectos de eludir la exclusión probatoria de la prueba ilícita refleja, lo que manifiestamente no lo es, al tratarse de una declaración exculpatoria. Y, en segundo lugar, utilizar para cuestionar la verosimilitud de la declaración del acusado, datos procedentes del conocimiento derivado de la prueba que el mismo Tribunal ha calificado como inconstitucional, y por tanto nula, como señalar la dificultad de que el acusado estuviese en la playa y no percibiese las luces y ruidos producidos por la interceptación del desembarco de la droga, cuando dicha interceptación debe excluirse de las actuaciones pues se produjo precisamente gracias a la prueba ilícita. Es claro que el Tribunal no puede valorar la

prueba válida (declaración exculpatoria del acusado en el juicio) en función de los datos conocidos a partir de una diligencia inconstitucional".

Como refuerzo de la idea expuesta, cita igualmente otros pronunciamientos, como el auto del Tribunal Supremo de 18 de junio de 1992, que se expresa en el sentido de recordar que "corresponde a los Jueces penales descubrir la verdad sólo a través de los procedimientos legalmente establecidos […] El procedimiento, la forma, la manera de actuar, el camino seguido, es siempre parte esencial del contenido, del fin alcanzado. […]", y la STS 311/2018, de 27 de junio, cuando indica "se corre el riesgo de tolerar con indiferencia el menoscabo de derechos del máximo rango axiológico y que confieren legitimidad al ejercicio de la función jurisdiccional. El principio de contradicción y los derechos de defensa y a no declararse culpable van más allá de un enunciado constitucional puramente formal. No son ajenos a una genuina dimensión ética, que pone límites a la capacidad de los poderes públicos para restringir derechos fundamentales y que, precisamente por su vigencia, han de operar un efecto disuasorio y excluyente frente a la tentación del Estado de eludir las garantías constitucionales […] que la prueba obtenida con vulneración de un derecho fundamental ha de ser excluida de la apreciación probatoria forma parte de las garantías del sistema constitucional".

Sin embargo, lo llamativo de esta decisión no es tanto la argumentación del tribunal, sino la revisión que realizó de la misma, en sede de apelación, el Tribunal Superior de Justicia. Comenzando con una censura sobre la decisión de no admitir ni siquiera la práctica de la prueba por la Audiencia Provincial, el tribunal de apelación concluye que no queda suficientemente resuelto si el origen de la intervención policial es un hallazgo no intencionado u ocasional, y en qué medida afecta a los derechos fundamentales establecidos en el artículo 18 de la Constitución. Este argumento, relativo a la necesidad de profundizar las circunstancias en las que la Guardia Civil tomó conocimiento de los hechos potencialmente delictivos (cómo fueron perdidos en el parque, posteriormente encontrados y finalmente entregados los objetos del imputado), se repite a lo largo de la sentencia como un motivo suficiente para la estimación de los recursos y la devolución de los autos al tribunal de instancia para que vuelva a dictar sentencia, que determine si el examen del contenido y su copia por los agentes de la Guardia Civil sería en todo caso ilegítimo, o si, en relación a las circunstancias de su entrega y recogida, pudiera existir una duda razonable que justificara el acceso a los archivos.

Se trata de una cuestión fundamental porque, como recuerda el tribunal, para la ponderación de indicios casuales u ocasionales no se aplica, en principio, el plazo perentorio de veinticuatro horas (SSTS 786/2015 de 4 de diciembre y 45/2014 de 7 de febrero) e, incluso, puede determinar la pérdida del nexo de ilicitud, en la medida en que este "no se extiende a pruebas obtenidas de un modo independiente (Sentencia TC 86/1995, de 8 de julio), lo que no se aplica al hallazgo casual, ocasional o inevitable, o a la ilicitud originaria atenuada."

Pero la sentencia del Tribunal Superior de Justicia va mucho más allá y, lejos de apuntar exclusivamente lo anterior, toma los argumentos de la Audiencia Provincial para prácticamente indicar el sentido que debería seguir la nueva sentencia. Así, vuelve a la STEDH del asunto Trabajo Rueda c. España y recuerda que, conforme al epígrafe 26, no puede ser declarada ninguna violación del artículo 8 CEDH cuando el acceso al contenido de ordenador tenga como finalidad que no queden impunes actos criminales que atenten contra menores, y que, conforme al epígrafe 38 de la misma sentencia, "una injerencia sin autorización judicial en el ordenador puede ser legítima "si es proporcionada al fin legítimo que se pretende y si los motivos invocados por las Autoridades nacionales para justificarla se revelan "pertinentes y suficientes", lo que no hace sino apuntar a un juicio de proporcionalidad del que indica la sentencia que "afirma el deber del Estado de garantizar el derecho de las víctimas, particularmente en las agresiones sexuales, que puede justificar medidas atentatorias contra derechos individuales".

Asistimos con este caso, por tanto, a un ejemplo concreto de cuál es el presente de la práctica penal en este tipo de materias, una situación en la que confluyen peligrosamente los poderes investigativos policiales y el cambio de naturaleza de la prueba obtenida con vulneración de derechos fundamentales.

8. OBTENCIÓN POR PARTICULARES DE FUENTES DE PRUEBA

Aunque escapa en cierta medida al objeto de nuestra investigación doctoral, no debemos dejar de hacer referencia a los supuestos en que son los particulares los que obtienen, por sus propios medios, fuentes de prueba de naturaleza tecnológica.

A. GRABACIONES PROPIAS

Vaya por delante que, como se ha indicado, las grabaciones efectuadas por particulares en el ámbito de su vida privada no están expresamente reguladas, por lo que no existe una previsión concreta sobre su admisión y valoración como prueba en el

proceso[522]. Pese a la reforma operada por la LO 13/2015, de 5 de octubre, el legislador no se ocupó de los supuestos en que los particulares obtienen fuentes de prueba tecnológicas, debiendo estarse, por tanto, a lo mantenido en la jurisprudencia de nuestros tribunales.

De conformidad con los pronunciamientos jurisprudenciales al respecto[523], la grabación de la conversación mantenida con otra persona, e incluso de su imagen, puede afectar a los derechos fundamentales del artículo 18 CE, que defienden la vida privada.

En relación con las grabaciones de comunicaciones en las que el sujeto que graba sea uno de los comunicantes, la regla general es que no supone intromisión ilegítima en la esfera privada del otro comunicante.

Así se extrae del artículo 7 de la LO 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, y también de la STC 114/1984, en la que se decía que el deber formal y abstracto del secreto no se extiende al comunicante.[524] Se entiende, así, que con la grabación de una conversación en la que se está participando lo que se produce es incorporar a un registro mecánico la comunicación que estamos manteniendo.

De esta manera, las grabaciones de procesos comunicativos realizadas por los propios comunicantes son válidas, incluso cuando se realizan de manera oculta, sin que pueda entenderse que ello vulnere el secreto de las comunicaciones. Tampoco vulnerarán, por regla general, el derecho a la intimidad, salvo casos excepcionales en los que en la conversación uno de los comunicantes se refiera al núcleo íntimo de su vida personal o familiar y sin ánimo de facilitar el conocimiento público de ello. Ahora bien, sí pueden vulnerar el derecho a no declarar contra sí mismo y a no confesarse culpable cuando se realizan desde una posición de superioridad institucional (agentes de la autoridad que obtienen una confesión extraprocesal mediante engaño[525]), o el derecho a un proceso con todas las

---

[522] MUÑOZ CONDE, F., "Prueba prohibida y valoración de las grabaciones audiovisuales en el proceso penal", *Revista penal*, 14, 2004, Tirant lo Blanch, p. 109.
[523] SSTS de 5 de mayo de 1997, de 17 de junio de 1999 y de 27 de septiembre de 2012, entre otras.
[524] También la STC 56/2003, de 24 de marzo, y las SSTS 652/2016, de 15 de julio; 517/2016, de 14 de junio; 421/2014, de 16 de mayo; 298/2013, de 13 de marzo; 682/2011, de 24 de junio; 1051/2009, de 9 de noviembre; y 2008/2006, de 2 de febrero, entre otras y según se citan en ERREIRO, M. L. N., "Dificultades probatorias en los delitos de violencia de género", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, pp. 1415–1432*, Ediciones Jurídicas Castillo de Luna, 2020, p. 1427, fecha de consulta 17 agosto 2021, en https://dialnet.unirioja.es/servlet/articulo?codigo=7871539.
[525] MARCHENA GÓMEZ, M., "Grabaciones entre particulares y prueba prohibida", *Revista de derecho y proceso penal*, 52, 2018, Aranzadi Thomson Reuters, p. 396.

garantías, cuando la persona grabada es conducida a la conversación o encuentro con argucias, cuando pueda apreciarse provocación al delito.

B. DATOS OBTENIDOS DE DISPOSITIVOS DE ALMACENAMIENTO

Supuestos distintos de lo hasta ahora expuesto son aquellas ocasiones en las que los ciudadanos particulares proporcionan material probatorio al proceso o las autoridades[526], cuando ellos no son los sujetos investigados en el mismo.

Dentro de las variadas posibilidades que engloba esta segunda categoría, los casos con menor dificultad son aquellos en los que se pueda apreciar que el investigado ha renunciado, sea de manera expresa o tácita, a la privacidad del dispositivo accedido por el tercero. Por ejemplo, en los supuestos en los que el dispositivo se entrega para su reparación, o cuando se contratan servicios de copia de recuperación de datos. En estos casos el Tribunal Supremo opta por entender que el titular del dispositivo ha autorizado al tercero para que acceda a los mismos[527]. Este hilo argumental puede llevar, por ejemplo, a entender autorizado el acceso a los prestadores de servicios de alojamiento en la nube para que, al copiar nuestros archivos en sus centros de almacenamiento de datos, revisen el contenido de nuestros archivos. Si en tal operación se descubrieran evidencias de delito, dichos prestadores de servicios tendrían que comunicarlos a la autoridad policial, como de hecho se ha advertido recientemente[528].

A pesar de lo anterior, ni que decir tiene que dicha regla no se aplicará de manera omnímoda, sino que será necesario atender a cuál fue la intención del particular que obtuvo el material probatorio, en el momento de obtenerlo. Así, la STS 508/2017, de 4 de julio, entendía lícito el acceso a las fotografías de una cámara de fotos olvidada, efectuada por un vigilante de seguridad que lo hizo sin intención de preconstituir prueba alguna: " existe la necesidad de dispensar un tratamiento singularizado en aquellos casos en los que la alegada ilicitud probatoria está originada por la actuación de un particular que no persigue –ni es utilizado por los poderes públicos como instrumento para esa finalidad– burlar las garantías de nuestro sistema constitucional en la investigación de los delitos. Y eso es lo que acontece en el presente supuesto. En efecto, se trata de una prueba proporcionada

---

[526] El Tribunal Supremo se ha pronunciado, entre otras, en las SSTS 793/2013, de 28 de octubre; 116/2017, de 23 de febrero; 45/2014, de 7 de febrero; 287/2017, de 19 de abril; y 508/2017, de 4 de julio.
[527] MARTÍN RÍOS, P., "El alcance del derecho al propio entorno virtual en la valoración de la evidencia digital", cit., p. 1263.
[528] "Child Safety", *Apple*, fecha de consulta 17 agosto 2021, en https://www.apple.com/child–safety/.

por un vigilante particular a los agentes de la Guardia Civil, sin que esa entrega haya sido concebida como un mecanismo de elusión de las garantías que el sistema constitucional reconoce para la protección de los derechos a la intimidad y al entorno virtual. De hecho, los agentes interesaron autorización judicial para acceder a su contenido y obtener el volcado de las imágenes de interés para la investigación. Esta Sala ha declarado que "... las reglas de exclusión probatoria se distancian de su verdadero sentido cuando no tienen relación con la finalidad que está en el origen mismo de su formulación. De lo que se trata es de limitar el afán del Estado en la persecución de los ilícitos penales, de apartar a los agentes de la autoridad de la tentación de valerse de medios de prueba que, por su alto grado de injerencia en el círculo de los derechos fundamentales, están sometidos a unas garantías constitucionales concebidas para la salvaguardia de aquellos. Se ha dicho con acierto que la proscripción de la prueba ilícita se explica por el efecto disuasorio que para el aparato oficial del Estado representa tener plena conciencia de que nunca podrá valerse de pruebas obtenidas con vulneración de las reglas constitucionales en juego" (cfr. STSS 287/2017, 19 de abril; 116/2017, 23 de febrero; 793/2013, 28 de octubre; 45/2014, 7 de febrero)."

En idéntico sentido, la reconocida STS 116/2017, de 23 de febrero, caso Falciani, otorgaba valor probatorio a material obtenido por un particular porque cuando lo obtuvo no pretendía prefabricar elementos de cargo utilizables en un proceso penal ulterior. Esta sentencia fue posteriormente confirmada por la STC 97/2019, de 16 de julio, y a la que ya nos hemos referido.

El acceso particular a dispositivos de terceros encuentra una de sus principales líneas definitorias, por tanto, en la necesidad de disuadir a los particulares de obtener elementos probatorios saltándose el régimen establecido para la obtención de los mismos. Si el tribunal, en el juicio de valor que efectúe en el caso concreto, concluye que la obtención de dicho material no estaba viciada por la intención de preconstituir prueba, podrá admitirlo como elemento de cargo en el proceso. Como se ha adelantado, constituirá un problema de prueba en el que no será fácil deslindar cada supuesto[529], y sin que estén claras las competencias revisoras en materia de casación que puedan aplicar en este

[529] MARTÍN RÍOS, P., "El alcance del derecho al propio entorno virtual en la valoración de la evidencia digital", cit., p. 1263.

supuesto, pues el juicio de valor que realice el tribunal estará fuertemente vinculado por la inmediación.

Por último, pero no menos importante, debemos hacer referencia también a aquellos supuestos en los que varios sujetos utilizan un dispositivo que, sin ser público ni de acceso libre (como sí podrían ser un ordenador de una biblioteca o cibercafé), sí es compartido (por ejemplo, entre los miembros de una misma familia, o de un piso de estudiantes, etc.). A nuestro juicio, ni siquiera es necesario acudir a la figura de un dispositivo: basta con la reconocida práctica de compartir cuentas de almacenamiento online, en las que, a fin de compartir gastos, varios usuarios arriendan espacio de almacenamiento a una sociedad prestadora de dichos servicios (OneDrive, Google Drive, Dropbox, iCloud, por citar los más populares, aunque existen muchos otros).

Pues bien, para el Tribunal Supremo parece que el hecho de utilizar un recurso común supone una renuncia por parte del titular de los datos a mantener dichos datos de manera reservada. Como indica la STS 287/2017, de 19 de abril, "quien incorpora fotografías o documentos digitales a un dispositivo de almacenamiento masivo compartido por varios es consciente de que la frontera que define los límites entre lo íntimo y lo susceptible de conocimiento por terceros, se difumina de forma inevitable". A esta postura se han formulado reservas[530], con las que coincidimos plenamente, por entender que desatiende la realidad social en la que dicha interpretación se inserta.

[530] *Ibid.*, p. 1268.

CAPÍTULO V
RETENCIÓN DE DATOS Y DEBER DE COLABORACIÓN CON LA INVESTIGACIÓN POLICIAL

Si hasta ahora nos hemos referido a la actividad de investigación de la policía en el ciberespacio, analizando tanto las herramientas de que dispone como los poderes investigativos autónomos de que puede hacer uso para obtener directamente la información, en este último capítulo de nuestra tesis queremos referirnos a aquellas modalidades en las que la información, en vez de ser recabada por la policía directamente desde la realidad, es o ha sido recabada previamente por un tercero que, al tener alguna relación con los datos objeto de la investigación, puede encontrarse obligado a colaborar con la autoridad judicial y la policía para conservar, captar o ceder datos.

Estos supuestos quedan agrupados, fundamentalmente en dos grandes fenómenos: por un lado, la figura de la retención de datos, regulada por la Ley 25/2007; por otro lado, la figura de los deberes de colaboración incorporados con la entrada en vigor de la LO 13/2015.

Asimismo, debemos señalar también la figura de las *freezing orders*, por un lado, y las *confiscation orders*, por otro. Reguladas en el Reglamento (UE) 2018/1805 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre el reconocimiento mutuo de las resoluciones de embargo y decomiso. De conformidad con el artículo 2 del mismo, una resolución de embargo (*freezing order*) es aquella dictada o validada por una autoridad de emisión con el fin de impedir la destrucción, transformación, traslado, transferencia o enajenación de bienes con vistas a su decomiso; por su parte, una resolución de decomiso (*confiscation order*) es aquella sanción o medida firme impuesta por un órgano jurisdiccional a raíz de un procedimiento relativo a un delito, que tenga como resultado la privación definitiva de bienes de una persona física o jurídica.

1. LA FIGURA DE LA RETENCIÓN DE DATOS

A. ANTECEDENTES HISTÓRICOS Y LEGISLATIVOS

Tras la participación de España y Reino Unido en la guerra de Irak, el 11 de marzo de 2004 y el 7 de julio de 2005 se suceden, respectivamente, atentados contra España y Reino Unido. En la necesidad de combatir y perseguir eficazmente el terrorismo y el crimen organizado, las autoridades nacionales y europeas adoptan diversas iniciativas legislativas, entre las que se encuentra la figura de la retención de datos[531].

Desde el punto de vista normativo, esta figura aparece contemplada incluso con anterioridad a los referidos atentados terroristas, pudiendo señalarse como una de las primeras manifestaciones la contenida en el artículo 16 del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, cuando prevé la obligación de que los Estados intervinientes adopten las medidas legislativas necesarias para permitir a sus autoridades competentes ordenar la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático, y en particular cuando existan razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación. Además, según el mismo artículo, cuando dicha orden se impartiese a una persona para conservar determinados datos almacenados que se encuentren en posesión o bajo el control de dicha persona, la legislación debería permitir obligar a esa persona a conservar y a proteger la integridad de dichos datos durante el tiempo necesario, hasta un máximo de noventa días, de manera que las autoridades competentes pudieran conseguir su revelación. Igualmente, en el mismo artículo establecía la obligación de articular un mecanismo para obligar al encargado de la custodia de los datos o a otra persona encargada de su conservación a mantener en secreto la aplicación de dichos procedimientos durante el plazo previsto en su derecho interno[532].

Asimismo, el artículo 17 CSC preveía también la necesidad de establecer en los ordenamientos jurídicos los instrumentos necesarios para que fuera posible conservar rápidamente datos sobre el tráfico con independencia de que en la transmisión de esa comunicación participaran uno o varios proveedores de servicios y garantizar la revelación rápida a la autoridad competente de un volumen suficiente de datos sobre el tráfico para

---

[531] ORTIZ PRADILLO, J. C., "Europa", cit., p. 1.
[532] QUEVEDO GONZÁLEZ, J., *Investigación y prueba del ciberdelito*, cit., p. 144.

que pueda identificar a los proveedores de servicio y la vía por la que se transmitió la comunicación.

La figura del deber de colaboración se completa con el artículo 19.4 CSC, que prevé la posibilidad de que las autoridades puedan ordenar a una persona que conozca el funcionamiento del sistema informático (o las medidas aplicadas para proteger los datos informáticos que contiene) a que proporcione toda la información necesaria (dentro de lo razonable) para permitir la aplicación de las medidas de investigación.

En España, esta obligación fue abordada por primera vez en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, cuyo artículo 12 establecía la obligación que tenían los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos de retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período máximo de doce meses, si bien limitando dicho deber de conservación a los necesarios para facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información, el origen de los datos alojados y el momento en que se inició la prestación del servicio, sin afectar al secreto de las comunicaciones.

Dicho régimen se completaba con lo previsto en los artículos 33 y 36 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, así como en el artículo 579 Ley de Enjuiciamiento Criminal y la Ley Orgánica 2/2002[533]. En particular, el artículo 36.2 LGT establecía como condición de uso del cifrado de la información la posibilidad de imponer la obligación de facilitar a los organismos públicos los algoritmos o el procedimiento de cifrado utilizado, así como los aparatos utilizados para el cifrado de la información, a efectos de su control de acuerdo con la normativa vigente.

A nivel europeo, y como antecedentes relacionados, debe mencionarse la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002[534].

---

[533] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 392.

[534] Actualmente, los artículos 5.1 y 6.1 de la referida Directiva se encuentran temporalmente suspendidos en virtud del controvertido Reglamento (UE) 2021/1232 del Parlamento Europeo y del Consejo de 14 de julio de 2021, por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE en lo que respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración para el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea, DO L núm. 274 de 30.7.2021, p. 41/51.

Posteriormente, fue aprobada 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, por la que se modifica la Directiva 2002/58/CE. La regulación contenida en la Directiva 2006/24/CE fue objeto de diversas críticas en relación con el sistema de conservación generalizada de datos de comunicaciones electrónicas, como se puede comprobar en el Informe de la Comisión al Consejo y al Parlamento de evaluación sobre la Directiva de 18 de abril de 2011, en el Dictamen del Supervisor Europeo de Protección de Datos de 23 de septiembre de 2011, en los Dictámenes del Grupo de Trabajo del artículo 29 sobre dicha materia y en varios pronunciamientos de Tribunales Constitucionales nacionales de Estados miembros que transpusieron el contenido de la directiva[535].

En cumplimiento del deber de transposición de dicha Directiva, fue aprobada la Ley 25/2007, que regula el régimen de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, y que derogó el referido artículo 12 de la Ley 34/2002.

Al poco tiempo de su aprobación, la Directiva 2006/24/CE sufrió un primer golpe por parte del TJUE con su sentencia *Irlanda c. Parlamento Europeo* (C–301/06), de 10 de febrero de 2009. Finalmente, con la STJUE de 8 de abril de 2014

Seguidamente, la Directiva 2006/24/CE fue anulada por la STJUE de 8 de abril de 2014, Digital Rights Ireland (C–293/12) y otros y Seitlinger y otros (C–594/12), ello con base en los siguientes argumentos: i) los únicos límites de conservación previstos en dicha directiva eran temporales, omitiendo criterios geográficos o personales; ii) el concepto de delito grave se encontraba en una grave falta de definición; iii) no señalaba autoridades con facultades para conservar y utilizar los datos; iv) los plazos de conservación previstos eran demasiado laxos, de entre 6 meses y 2 años; v) y se advertía una falta de garantías de seguridad y confidencialidad, porque no se aseguraba destrucción tras el periodo de conservación ni se fijaba el órgano de control externo independiente que controlara la actuación. Esta sentencia marcó un hito en la jurisprudencia del TJUE, al contener pautas y criterios interpretativos de suma importancia, que tanto el legislador nacional o comunitario, como las autoridades judiciales, como garantes de la primacía normativa del

[535] ORTIZ PRADILLO, J. C., "Europa", cit., p. 6.

Derecho de la Unión, debieron tomar en cuenta en el futuro a la hora de examinar la compatibilidad de la regulación y práctica de las medidas que supusieran injerencias en la Carta de Derechos Fundamentales de la Unión Europea, en concreto con los artículos 7 y 8 y, sobre todo, en relación con las llamadas medidas de "vigilancia en masa."[536]

A raíz de dicha sentencia, varios Estados miembros reformaron sus legislaciones nacionales para que la figura de la conservación de datos quedara vinculada al artículo 15, apartado 1, de la Directiva 2002/58/CE, que permitía imponer obligaciones de conservación y cesión de determinados datos por razones de protección de la seguridad nacional, defensa, seguridad pública o prevención, investigación, descubrimiento y persecución de delitos.

España, por su parte, adoptó mínimas modificaciones en la Ley 25/2007, que mantuvo vigente[537]. Con posterioridad, fue aprobada la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, cuyos artículos 39 y 43 reproducen el contenido de los artículos 33 y 36 de la anterior ley.

No obstante, con posterioridad, el TJUE dictó la sentencia Tele2 Sverige (C–203/15) y Watson y otros (C–698/15), de 21 de diciembre de 2016, que declaraba prácticamente imposible tal adaptación, a la vista de los elevados requisitos que imponía para admitir previsiones de conservación de datos. Esta sentencia concluyó que el artículo 15, apartado 1, de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que se opone a una normativa nacional que establece, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica, y que se opone a una normativa nacional que regula la protección y la seguridad de los datos de

---

[536] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 442.
[537] RODRÍGUEZ LAINZ, J. L., "Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre conservación de datos relativos a las comunicaciones", *Diario La Ley*, 8308, 2014, Wolters Kluwer, p. 4.

tráfico y de localización, en particular el acceso de las autoridades nacionales competentes a los datos conservados, sin limitar dicho acceso, en el marco de la lucha contra la delincuencia, a los casos de delincuencia grave, sin supeditar dicho acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente, y sin exigir que los datos de que se trata se conserven en el territorio de la Unión.

Además, dicha sentencia, en sus parágrafos 108 a 111, establece una serie de requisitos, al indicar que el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, no se opone a que un Estado miembro adopte una normativa que permita, con carácter preventivo, la conservación selectiva de datos de tráfico y de localización a efectos de la lucha contra la delincuencia grave, siempre que la conservación de los datos esté limitada a lo estrictamente necesario en relación con las categorías de datos que deban conservarse, los medios de comunicación a que se refieran, las personas afectadas y el período de conservación establecido. Dichos requisitos serían i) que se trate de normas claras y precisas que regulen el alcance y la aplicación de una medida de conservación de datos y que establezcan unas exigencias mínimas, de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos personales frente a los riesgos de abuso, indicando en qué circunstancias y con arreglo a qué requisitos puede adoptarse, con carácter preventivo, una medida de conservación de datos; ii) que sean normas suficientes para garantizar que la orden de conservación de datos se limita a lo estrictamente necesario, dicha orden debe responder a criterios objetivos y debe existir una relación entre los datos que deban conservarse y el objetivo que se pretende lograr, de manera que dichos datos permitan que pueda delimitarse en la práctica de modo efectivo el alcance de la medida y, en consecuencia, el público afectado; y iii) que dichas normas establezcan criterios objetivos que permitan dirigirse a un público cuyos datos puedan presentar una relación, por lo menos indirecta, con delitos graves, contribuir de un modo u otro a la lucha contra la delincuencia grave o prevenir un riesgo grave para la seguridad pública, pudiendo adoptarse un criterio geográfico cuando existan elementos objetivos que evidencien un riesgo elevado de preparación o de comisión de tales delitos en una o varias zonas geográficas.

En cualquier caso, y aunque la normativa española debe interpretarse conforme a la doctrina del TJUE, nuestra jurisprudencia (SSTS 400/2017, de 1 de junio; 470/2015,

de 7 de julio y 768/2015, de 23 de noviembre) mantiene que la Ley 25/2007 continúa siendo aplicable, todo ello en un esfuerzo que ha sido tildado de numantino[538].

En concreto, la STS 272/2017, de 18 de abril, concluye, en un caso concreto que al no accederse al contenido de las comunicaciones, sino a los datos asépticos de los teléfonos móviles que se conectaron en un determinado momento a una concreta antena de telefonía, con la finalidad de cruzarlos con los de otras antenas que recogían los datos de otros en la zona donde se había perpetrado otro robo similar, la resolución judicial que la acordaba estaba ajustada a derecho. De igual modo, la STS 768/2015, de 23 de noviembre, concluye que una adecuada interpretación de Ley 25/2007 superaba esas objeciones, pues no puede considerarse que la transposición está subordinada al modo en que lo está el reglamento a la ley.

De conformidad con esta jurisprudencia, las exigencias señaladas por el TJUE en nuestra normativa interna están sujetas a la autorización de una autoridad independiente de la administrativa, cual es la judicial, y se contraen a la investigación y enjuiciamiento de delitos graves contemplados en el Código Penal y en las leyes penales especiales, de forma que en cada caso será el Juez de Instrucción correspondiente el que decida la cesión de los datos de tráfico en las comunicaciones electrónicas, lo que desde luego implica que la decisión debe ser ajustada al principio de proporcionalidad establecido expresamente en nuestra ley procesal. Todo ello no parece incompatible con la exigencia de una normativa nacional que no admita la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica.

Con posterioridad, ha sido dictada la STJUE (Gran Sala) de 2 de marzo de 2021 (caso Prokuratur; asunto C–746/2018) que, en la línea de las ya comentadas, vuelve a señalar que "El artículo 15, apartado 1, de la Directiva 2002/5810E del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo. de 25 de noviembre de 2009, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que se opone a

[538] ORTIZ PRADILLO, J. C., "Europa", cit., p. 10.

una normativa nacional que autoriza el acceso de autoridades públicas a un conjunto de datos de tráfico o de localización que pueden facilitar información sobre las comunicaciones efectuadas por un usuario de un medio de comunicación electrónica o sobre la localización de los equipos terminales que utilice y permitir extraer conclusiones precisas sobre su vida privada, a efectos de la prevención, la investigación, el descubrimiento y la persecución de delitos, sin que dicho acceso se limite a procedimientos que tengan por objeto la lucha contra la delincuencia grave o la prevención de amenazas graves contra la seguridad pública, y ello con independencia de la duración del período para el que se solicite acceder a los citados datos y de la cantidad o naturaleza de los datos disponibles en ese período".

A juicio de la doctrina[539], ello implica una clara desacreditación de esa línea jurisprudencial, representada por las SSTS 400/2017, de 1 de junio, y 723/2018. de 23 de enero de 2019, que, frente al órdago que representara la STJUE de 21 de diciembre de 2016, optaron por mantener la línea continuista ya iniciada por las SSTS 470/2015, de 7 de julio; 768/2015 de 23 de noviembre, y 272/2017, de 18 de abril, ancladas en la idea de que una aplicación rigorista de la LCDCE sí permitiría entenderla conforme a las exigencias del derecho comunitario.

B. RÉGIMEN JURÍDICO DE LA LEY 25/2007

De acuerdo con su artículo 1.1, el objeto de la ley es regular la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales. Por tanto, la previsión de dicho deber de obligación únicamente alcanza a los supuestos de investigación y prueba de los delitos que sean graves.

Los datos, además, únicamente podrán ser entregados a los agentes facultados en formato electrónico y para los fines del artículo 1, y sin que sea suficiente con la autorización del Ministerio Fiscal, sino que es necesaria autorización judicial. En ese sentido,

---

[539] RODRÍGUEZ LAINZ, J. L., "La STJUE de 2 de marzo de 2021 (Caso Prokuratur): ¿Una simple secuela de la Sentencia del Caso la Quadraute du Net sobre conservación de datos relativos a las comunicaciones electrónicas?", *Diario La Ley*, 9835, 2021, Wolters Kluwer, p. 5.

el acuerdo no jurisdiccional de 23 de febrero de 2010 del Tribunal Supremo concluía que *"es necesaria la autorización judicial para que los operadores que prestan servicios de comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo. Por lo cual, el Ministerio Fiscal precisará tal autorización para obtener de los operadores los datos conservados que se especifican en el artículo 3 de la Ley 25/2007."*

El plazo de conservación de los datos establecido en la ley es de 12 meses, y el de cesión del dato será el que fije la resolución judicial, según la urgencia de la cesión, la naturaleza y complejidad técnica de la operación y los efectos que pueda producir en la investigación de que se trate.

En el estudio del régimen jurídico de la Ley 25/2007 se plantea la problemática del concepto de delito grave. La ley 25/2007, de 18 de octubre, de conservación de datos de comunicaciones electrónicas y de redes públicas de comunicación, al incorporar al ordenamiento interno la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio, trajo consigo algunos de los defectos de que adolecía la normativa comunitaria, y entre ellos se cuenta la indefinición relativa al concepto de "delito grave".

Al respecto, cabe recordar que el artículo 1.1 de la Directiva disponía que las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro. En desarrollo de lo anterior la Ley 25/2007 establecía también la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales. Por

tanto, la previsión de dicho deber de obligación únicamente alcanza a los supuestos de investigación y prueba de los delitos que sean graves"[540].

Podemos identificar dos corrientes opuestas acerca de cómo ha de entenderse la referencia a "delito grave"[541]. Por un lado, surgió una interpretación de base formalista, que entendía el delito grave como todo aquel que estuviera castigado con las penas contempladas como graves en el artículo 33 CP, de acuerdo con el artículo 13 CP. Por otro lado, una interpretación de base sustancial defendía que el criterio de la gravedad debía atender a las circunstancias concretas del hecho delictivo y a la injerencia que supusiera la medida en los derechos fundamentales del investigado.[542]

Son varios los argumentos que se aducen en favor de la interpretación sustancial de la exigencia de "delito grave"[543]. Para empezar, la interpretación formal implicaría que no fuera posible investigar de manera eficaz múltiples *ciberdelito*s que, aun no mereciendo el calificativo de graves a los efectos de los artículos 13 y 33 CP, solamente podrían ser investigados mediante este tipo de diligencias de investigación. En ese sentido, se ha afirmado que "la exclusividad de acceso únicamente cuando se trate de delitos graves, si ha de entenderse como tales aquellos a los que les corresponda una pena grave según la retribución penológica contemplada en los artículos 13 u 33 CP, supondría otorgar un margen de impunidad a toda aquella infinidad de hechos delictivos que se materializan gracias al medio tecnológico en que se producen y que no alcanza tales penalidades (por ejemplo, las estafas mediante phishing o engaño para acceder a la banca telemática, amenazas, injurias, coacciones, *cyberbullying*, etc.). Por ello, precisamente, un sector de la doctrina se inclina por considerar que debiera tenerse en cuenta, además de la gravedad, el ámbito tecnológico y la trascendencia social de los hechos."[544]

---

[540] "El «delito grave» en relación a la obligación de conservación de datos, según la L 25/2007", *El Derecho*, fecha de consulta 29 marzo 2020, en https://elderecho.com/el–delito–grave–en–relacion–a–la–obligacion–de–conservacion–de–datos–segun–la–l–252007–y–las–reformas–penales–recientes.

[541] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 445.

[542] "La solicitud de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación en el marco de la instrucción: reflexión sobre la Ley 25/2007 – El Derecho – Derecho Tic, Penal, Sector Jurídico", *El Derecho*, fecha de consulta 29 marzo 2020, en https://elderecho.com/la–solicitud–de–datos–relativos–a–las–comunicaciones–electronicas–y–a–las–redes–publicas–de–comunicacion–en–el–marco–de–la–instruccion–reflexion–sobre–la–ley–252007.

[543] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 445.

[544] VALLÉS CAUSADA, L., "La investigación criminal basada en datos conservados de las comunicaciones electrónicas – Blog de Criminología – Iter Criminis", 2018, fecha de consulta 29 marzo 2020, en https://web.archive.org/web/20180220084318/http://blogs.ucjc.edu/criminologia–iter–criminis/la–investigacion–criminal–basada–en–datos–conservados–de–las–comunicaciones–electronicas/.

Además de dicho criterio "lógico", una interpretación sistemática apoyaría también el abandono de la interpretación formal, puesto que, en caso contrario, se estaría incurriendo en la contradicción de establecer unas mayores exigencias para la cesión de datos externos de la comunicación que para acceder a la propia comunicación, considerando que el Tribunal Constitucional viene exigiendo, para proceder a la interceptación de las comunicaciones, requisitos diferentes de la gravedad formal del delito: la trascendencia social del delito que se trata de investigar (STC 1305/2014, de 2 de abril), los bienes jurídicos protegidos, la comisión del delito por organizaciones criminales y la potencialidad lesiva de los instrumentos informáticos (STC 104/2006, de 3 de abril)[545].

Se ha entendido que es "razonable que el concepto de delito grave a la hora de recabar los datos conservados al amparo de lo dispuesto en la Ley 25/2007 sea el mismo que el manejado a la hora de adoptar una intervención telefónica (de no optar por esta interpretación se llegaría al absurdo de imponer mayores restricciones a la cesión de datos externos que al acceso al contenido de lo comunicado, cuando los derechos afectados tienen la misma categoría)"[546]. En términos parecidos se pronuncia la Fiscalía General del Estado en su Circular 1/2013, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas, al concluir que "ningún sentido tendría imponer mayores restricciones a la cesión de datos externos que al acceso al contenido de lo comunicado".

Con la entrada en vigor de la reforma de la LECrim de 2015, el artículo 588 *ter* a) permite interceptar las comunicaciones telefónicas telemáticas tanto para los delitos previstos en el artículo 579.1 LECrim como para todos aquellos delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación, sin hacer referencia alguna al artículo 33 CP.

Ambos argumentos permiten llegar a la conclusión[547] de que la expresión "delito grave" debe entenderse referida al resultado de la aplicación del juicio de proporcionalidad previo a toda restricción de derecho fundamental para la investigación y persecución de ilícitos penales. En este juicio de proporcionalidad, necesario para que el juez autorice

---

[545] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 446.
[546] VÁZQUEZ SECO, L., "Retención obligatoria de datos de tráfico de las comunicaciones telefónicas y/o electrónicas. Análisis de la sentencia del Tribunal de Justicia de la Unión Europea de 8 de abril de 2014 en los asuntos acumulados C–293/2012 y C–594/2012 (Digital Rights Ireliand y Seitlinger y otros)".
[547] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 446.

el acceso a los datos conservados, deberán tenerse presente varios criterios. Entre ellos, la gravedad de la pena señalada al delito o delitos investigados, pero complementado con otros criterios, como pueden ser los derivados de la propia naturaleza del bien jurídico lesionado, las formas de manifestación del hecho (como puede ser la habitualidad en la comisión delictiva o la peligrosidad social de los efectos del hecho), la relevancia social de la conducta, la potencialidad lesiva del uso de instrumentos informáticos para la comisión del delito e, incluso, las circunstancias relevantes que concurran tanto subjetivas del imputado, como la tendencia a cometer hechos de la misma naturaleza, como objetivas del caso concreto, como la especial intensidad del comportamiento delictivo[548]. A tal efecto, hay que recordar que "el juez debe tomar como referente inicial la relevancia social del os bienes que se tratan de proteger con la persecución del delito, que, si bien normalmente van asociados con la gravedad de las penas que en su día se pudieran imponer, ello no necesariamente es así"[549].

Tampoco puede admitirse que el acceso a los datos conservados por las operadoras pueda suponer un grado de afectación diferente de los derechos del investigado, según el caso. La STC 123/2002, de 20 de mayo, afirmaba que "aunque el acceso y registro de los datos constituye una forma de afectación del objeto de protección del derecho al secreto de comunicaciones, no puede desconocerse la menor intensidad de la injerencia en el citado derecho fundamental que esta forma de afectación representa en relación con la que materializan las escuchas telefónicas". A tal efecto, se ha venido reconociendo la llamada "ecuación de la proporcionalidad"[550], que viene a constituir una relación directamente proporcional entre la gravedad de la injerencia en el derecho fundamental y la profundidad del análisis en el examen y motivación de los elementos que justifiquen el juicio de proporcionalidad.

Con base en lo anterior, la resolución judicial que autorice el acceso deberá indicar qué datos concretos son los que deben ser facilitados, que en todo caso serán únicamente los indispensables para la investigación, conforme al artículo 588 *ter* j) 2 LECrim.

Como complemento de lo anterior, no puede dejarse de mencionar la STJUE de 8 de octubre de 2018, que previo reconocimiento de que el acceso por las autoridades

---

[548] *Ibid.,* p. 447.
[549] ESTRELLA RUIZ, M., "Entrada y registro, interceptación de comunicaciones postales, telefónicas, etc...", *Cuadernos de derecho judicial*, 12, 1996, Consejo General del Poder Judicial.
[550] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 448.

públicas a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas constituye una injerencia en el derecho fundamental al respeto de la vida privada del artículo 7 y en el derecho a la protección de los datos personales del artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, concluía que dicha injerencia, sin embargo no era grave cuando el acceso a dichos datos fuera limitado y estuviera justificado por el objetivo de prevenir, investigar, descubrir y perseguir delitos conforme con el artículo 15.1 de la Directiva 2002/58 (en el caso concreto, la solicitud policial se refería al acceso a datos para identificar a los titulares de las tarjetas SIM activadas de unos teléfonos sustraídos.). A su vez, concluyo que cuando la injerencia no es grave, puede quedar suficientemente justificada por el objetivo de prevenir, investigar, descubrir y perseguir delitos "a secas", y que solamente puede exigirse la gravedad del delito respecto de las injerencias que sean igualmente graves.

La interpretación material, amparada por las recientes reformas de la LECrim y los pronunciamientos del STJUE, es la que ha venido siendo asumida por nuestros tribunales, pudiendo citarse entre otros ejemplos los AAP Madrid 131/20115, de 25 de febrero, 1177/2015, de 30 de octubre, y 447/2016, de 14 de abril, entre otros muchos[551].

C. DATOS ASOCIADOS A COMUNICACIONES ELECTRÓNICAS

Partimos del artículo 1 del Convenio del Consejo de Europea sobre Ciberdelincuencia, cuando denomina datos como toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función. Dentro de ese conjunto de datos informáticos la doctrina distingue tres categorías: datos de contenido, datos de tráfico y datos de abonado.

Los datos de contenido son todos aquellos que constituyen el mensaje que se comunica o transmite.

Los datos de tráfico son todos aquellos relativos a un proceso comunicativo que tenga lugar mediante un sistema informático, generados por dicho sistema en su condición de elemento del proceso de comunicación, y que refieren el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación, así como el servicio subyacente.

---

[551] *Ibid.*, p. 451.

Por último, los datos relativos a los abonados quedan conceptuados en el artículo 18.3 CSC, al indicar que por datos relativos a los abonados se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar: a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio; b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios; c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios.

En un intento por simplificar la cuestión, se ha afirmado que por "datos asociados a comunicaciones electrónicas" debe entenderse que son, en definitiva, todos aquellos que circulan por redes de telecomunicación conjuntamente con las comunicaciones electrónicas y que sin embargo no constituyen ni forman parte del contenido de la comunicación.[552]

En los procesos de comunicación telemáticos se generan datos de tráfico cuyo rastreo permite la identificación del equipo que origina el proceso comunicación, así como obtener otras informaciones de utilidad para la investigación. Esto ha provocado que los datos externos se hayan convertido en un elemento fundamental en la investigación de delitos, desde el punto y hora en que permiten construir la huella o rastro digital.

Tras la reforma operada en 2015, el artículo 588 *ter* j) LECrim contiene la previsión legal para que la autoridad pueda acceder a los datos obrantes en archivos automatizados de los prestadores de servicios para los fines de investigación del delito. Antes de la citada reforma la única habilitación existía en el artículo 1.1 de la Ley 25/2007, de 18 de octubre, que regula el régimen de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

En ese sentido, las SSTEDH de 2 de agosto de 1984 (Malone c. Reino Unido) y de 3 de abril de 2007 (Copland c. Reino Unido) han declarado que el derecho al secreto de las comunicaciones no se despliega únicamente sobre el contenido de la comunicación,

[552] *Ibid.*, p. 114.

sino también sobre los aspectos externos de la misma. En el mismo sentido, la STC 114/1984, de 29 de noviembre; el mismo Tribunal Constitucional ha afirmado que forma parte del secreto de las comunicaciones la identidad subjetiva de los interlocutores, por lo que la entrega de listados de llamadas por las compañías telefónicas y el acceso al registro de llamadas entrantes y salientes de un teléfono móvil afecta al referido derecho (SSTC 142/2012, de 7 de julio y 230/2007, de 5 de noviembre).

Sobre el mismo concepto, el artículo 1.d del Convenio de Budapest indica que "cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento del a cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente". Igualmente, el artículo 588 *ter* b LECrim los define 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."

En ese sentido, se ha afirmado que el derecho fundamental al secreto de las comunicaciones abarca todo el proceso de comunicación, y por tanto i) el contenido del mensaje; ii) la identidad subjetiva de los interlocutores; y iii) todos los datos externos a la comunicación, como la existencia de la propia comunicación, el origen y su destino, la fecha y hora y la duración, etc.

Es necesario distinguir entre el acceso a los datos externos en función de las diferentes fases del proceso comunicativo. En el supuesto de acceso a datos externos cuando la comunicación aún no se ha iniciado, la doctrina se refiere a los datos operativos de puesta a disposición del servicio de comunicación, ya sea mediante el inicio del dispositivo o su conexión a la red, pero sin iniciar proceso de comunicación alguno, por lo que no se afectaría el derecho al secreto de comunicaciones, aunque sí el derecho a la intimidad[553].

En el supuesto de acceso a los datos externos de la comunicación cuando esta está teniendo lugar, quedaría protegido por el derecho fundamental al secreto de las comunicaciones.

---

[553] *Ibid.*, p. 115.

Finalmente, en cuanto al acceso a los datos externos una vez finalizado el proceso comunicativo, pueden distinguirse dos teorías. Una, defiende que la garantía del secreto de comunicación se extiende aún después de terminada la comunicación, que por tanto se extiende a todos los datos generados por la misma. Otra postura, por el contrario, entiende que, en la medida en que el proceso ha terminado, dicho acceso no afecta al secreto de las comunicaciones. En tal sentido, se ha afirmado que "superado el proceso comunicativo, tal protección formal perdía su razón de ser y aquello que quedara de la comunicación conservado en cualquier tipo de soportes pasaría a ser objeto de tutela por derechos relacionados con el concepto amplio de intimidad o privacidad, entre los que se encontrarían sin duda la intimidad domiciliaria, y especialmente en materia de datos de tráfico o asociados a las comunicaciones, la protección de datos personal"[554].

En este sentido, parece que en la jurisprudencia se consolida la idea de que, una vez ha finalizado el proceso comunicativo, la protección del artículo 18.3 CE deja de ser aplicable, algo que desde nuestro punto de vista no podemos compartir, en la medida en que la propia caducidad de la garantía afectará al libre ejercicio del derecho. En cualquier caso, en la STC 70/2002, de 3 de abril, se afirma que "la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos", y en la STS 786/2015, de 4 de diciembre, recordando la STS 342/2013, de 17 de abril, que "el correo electrónico y los programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato telemático, el derecho a la libre comunicación entre dos o más personas. Es opinión generalizada que los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por su destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito que sería propio de la inviolabilidad de las comunicaciones. La comunicación ha visto ya culminado su ciclo y la información contenida en el mensaje es, a partir de entonces, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad, cuya protección es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad de las comunicaciones". Al margen de lo acertado de este razonamiento, lo cierto es que pueden plantearse dificultades en los supuestos en que

[554] RODRÍGUEZ LAINZ, J. L., "Sobre la naturaleza formal del derecho al secreto de las comunicaciones: dimensión constitucional e histórica", *Diario La Ley*, 7647, 2011, Wolters Kluwer, p. 3.

el mensaje no es descargado, sino que permanece en la herramienta web, por lo que su acceso implica el acceso a los centros de datos de terceros y, aún más, que se comprometa el centro desde el que la persona investigada emite comunicaciones.

Parece asumirse por la doctrina[555] que cuando los datos se encuentran almacenados en un dispositivo electrónico –generalmente en forma de archivos temporales– el acceso a los mismos afecta al derecho a la intimidad, exigiendo autorización judicial excepto en los supuestos de consentimiento tácito del usuario (expectativa razonable de privacidad), consentimiento del interesado de manera expresa o intervención policial en caso de urgencia. El artículo 588 *ter* j LECrim, por su parte, exige la autorización judicial para acceder a dichos datos cuando estén almacenados por operadores de servicios de telecomunicación.

El artículo 588 *ter* j) LECrim, al referirse a "los datos que se encuentren vinculados a procesos de comunicación" obliga a distinguir entre datos vinculados a procesos de comunicación y aquellos que no lo están. Debe partirse de que por proceso de comunicación se entiende "toda transmisión de información entre dos o más personas determinadas o determinables con la intermediación de un tercero–prestador del servicio de comunicación unido a los interlocutores por vínculo de confidencialidad"[556].

Pueden distinguirse dos supuestos diferentes en cuanto a los datos conservados: los que se conservan en cumplimiento de la legislación sobre retención de datos, y los que son conservados por propia iniciativa por los prestadores de servicios, sean motivos comerciales o de cualquier otra índole. En el primer caso será de aplicación el artículo 588 *ter* j) y en el segundo caso será de aplicación también exclusivamente cuando los datos estén vinculados a un proceso de comunicación.

De conformidad con el referido artículo 588 *ter* j), "1. Los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial. 2. Cuando el conocimiento de esos datos resulte indispensable para la investigación, se solicitará del juez competente autorización

[555] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 116.
[556] *Ibid.*, p. 438.

para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión."

En consecuencia, los datos vinculados a procesos de comunicación únicamente pueden ser cedidos para su incorporación al proceso 1) cuando su conocimiento resulte indispensable para la investigación, y previa autorización judicial; 2) cuando en la solicitud se precisen los datos que deban conocerse y las razones que justifican la cesión; 3) respetando en todo caso las disposiciones comunes de los artículos 588 *bis* a) y siguientes.

Además de lo anterior, conviene tener presente que la solicitud de acceso puede comprender dos prestaciones de naturaleza diferente por parte de la entidad obligada a la colaboración. La primera prestación consistiría en facilitar de manera plana los datos específicos que se indicaran en la misma petición. La segunda, en realizar una búsqueda entrecruzada o inteligente de datos, que consiste en comparar de manera automatizada, a través de técnicas de cruce, comparación y contraste, los datos que obren en los archivos del obligado a colaborar, a fin de descubrir posible información adicional que resulte de utilidad para la investigación del delito. Esto supone un esfuerzo adicional para el obligado a la colaboración, que podría verse compelido incluso a asumir un coste económico adicional, pero también se viene entendiendo que supone una afección añadida a la propia cesión del dato para el derecho fundamental afectado[557].

Se entiende que los datos a los que se refiere el artículo 3 LCDCE son los datos estáticos, que deben distinguirse del propio contenido de las comunicaciones. Esta regulación permite complementar y elevar a rango de ley orgánica las previsiones de la LCDCE.

En cuanto al ámbito delictual en el que cabe solicitar esta medida, parece que al no señalar delitos concretos para los que puede acordarse la diligencia debería estarse al ámbito establecido por el artículo 588 *ter* a LECrim, que encabeza el capítulo –criterio sistemático–, y que se refiere a los delitos dolosos castigados con, al menos, 3 años de prisión en su límite máximo, los cometidos en el seno de un grupo u organización criminal, los de terrorismo y los que puedan considerarse como ciberdelincuencia, por haber

[557] *Ibid.*, p. 439.

sido cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación[558].

D. Sistema Integrado de Interceptación de Comunicaciones

Originariamente previsto en el artículo 33 de la Ley 32/2003, General de Telecomunicaciones, la interceptación de comunicaciones y retenciones de datos se realizaban mediante el "Sistema Integral de Interceptación de las Comunicaciones Electrónicas", contratado el 24 de octubre de 2001 por el Ministerio del Interior y adjudicada a la empresa danesa ET A/S, especializada en soluciones informáticas y de telecomunicaciones para fuerzas policiales. Originariamente, el contrato tenía como fecha de entrega el 31 de marzo de 2003, pero fue aplazado en dos ocasiones hasta el 30 de noviembre de 2003, debido a que los operadores de telecomunicaciones no habían instalado los correspondientes sistemas de interceptación en sus redes.[559]

Posteriormente, tras la aprobación de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, la existencia del sistema pasó a estar prevista en el artículo 39, y este pasó a denominarse como Sistema Integrado de Interceptación de Comunicaciones (SITEL).

Dicho sistema ha sido adjudicado a la empresa DARS Telecom el 13 de mayo de 2015. Una de las principales mejoras respecto es que soporta la mayor parte de los programas o aplicaciones de correo electrónico, mensajería instantánea y redes sociales.[560]

Con este sistema se consigue que toda la información que se origine o se dirija un a punto de terminación de red, identidad o etiqueta objeto de interceptación, pueda ser captada y remitida al centro de interceptación, aunque esté destinada a un dispositivo de almacenamiento o procesamiento de la información. La interceptación puede realizarse sobre un terminal conocido y con unos datos de ubicación temporal cuando se trate de comunicaciones emitidas desde lugares accesibles públicamente. En general, la redacción del artículo 39.4 LGT ha sido considerada como "ambiciosa"[561], en la medida en que

---

[558] BARRIO ANDRÉS, M., *Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 263.
[559] *Ibid.*, p. 257.
[560] RODRÍGUEZ LAINZ, J. L., *El secreto de las telecomunicaciones y su interceptación legal*, Sepín, p. 126.
[561] BARRIO ANDRÉS, M., *Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 258.

impone que la accesibilidad se garantice respecto de cualquier comunicación que tenga como origen o destino un dispositivo electrónico e, incluso, refiriéndose a conexiones que podrían escapar al concepto de comunicaciones *strictu sensu*, como son las que se destinan a un dispositivo de almacenamiento de la información (imaginemos los procesos de sincronización de los diferentes servicios en la nube, o las descargas directas, etc.), incluyendo, por supuesto, los datos previstos en los apartados 5, 6 y 7 LGT. Las sentencias del Tribunal Supremo de 13 de marzo, 5 de noviembre y 30 de diciembre de 2009 exponen el funcionamiento del sistema SITEL.

La titularidad de la plataforma la ostenta el Ministerio del Interior. Su desarrollo responde a la necesidad de articular un mecanismo moderno, automatizado, simplificador y garantista para la figura o concepto jurídico de la intervención de las comunicaciones. Según la STS 366/2019, de 17 de julio, el sistema se construye sobre la base de enlaces con las operadoras de telefonía, que transmiten la información correspondiente a la interceptación que dichas operadoras realizan en su sistema, para almacenarse en el sistema central del Cuerpo Nacional de Policía. Los enlaces "punto a punto" establecidos permiten únicamente la entrada de información procedente de la operadora, la cual, automáticamente, es almacenada por el sistema central en el formato recibido con características de solo lectura, sin intervención de los agentes facultados, y queda guardada con carácter permanente en el sistema central de almacenamiento a disposición de la autoridad judicial (vid SSTS1215/2009, de 30 de diciembre , 327/2010, de 12 de abril , 554/2012, de 4 de julio, 373/2016, de 3 de mayo ,358/2017, de 18 de mayo , etc.).

Según la STS 250/2009, de 13 de marzo, el funcionamiento del sistema queda inspirado en tres principios fundamentales: centralización, seguridad y automatización.[562]

El principio de centralización hace referencia a que el servidor y administrador del sistema se encuentra en la sede central de la Dirección General de la Guardia Civil, distribuyendo la información aportada por las operadoras de comunicaciones a los distintos usuarios implicados.

El principio de seguridad hace referencia a que el sistema establece numerosos filtros de seguridad y responsabilidad, apoyados en el principio de centralización. Existen dos ámbitos de seguridad: nivel central y nivel periférico. En el nivel central se encuentra

[562] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 435.

una unidad de procesamiento para cada sede reseñada, dotada de medidas de máxima alerta, con unos operarios de mantenimiento específicos, y desde donde se dirige la información a los puntos de acceso periféricos de forma estanca; la utilidad de este nivel consiste en almacenar y distribuir la información del sistema. En el nivel periférico el sistema cuenta con ordenadores específicos de enlace en las unidades encargadas de la investigación y responsables de la intervención de la comunicación, dotados de sistemas de conexión con la sede central. Se establece un sistema de acceso por usuario autorizado y clave personal, garantizando la conexión para ese usuario, que deberá ser componente de la Unidad de investigación encargada y responsable de la intervención.

El principio de automatización indica que el sistema responde a la necesidad de modernizar el funcionamiento de las intervenciones de las comunicaciones, dotándolo de mayor nivel de garantía y seguridad, reduciendo costes y espacio de almacenamiento, así como para adaptarlo al uso de nuevos dispositivos de almacenamiento.

Ya en 2009, la información facilitada por SITEL era la siguiente: i) fecha, hora y duración de las llamadas; ii) identificador de IMEI y nº de móvil afectado por la intervención; iii) distribución de llamadas por día; iv) tipo de información contenida (SMS, audio, etc.); y v) repetidor activado, mapa del mismo, y contenido de las llamadas y de los mensajes de texto.

En cuanto al sistema de trabajo, solicitada la intervención de la comunicación y autorizada por la Autoridad Judicial el empleo del programa SITEL, la operadora afectada inicia el envío de información al Servidor Central donde se almacena a disposición de los agentes encargados y solicitantes de la investigación de los hechos, responsable de la intervención de la comunicación. El acceso por parte del personal de esa unidad policial se realiza mediante código identificador de usuario y clave personal. Realizada la supervisión del contenido, se actúa igual que en el modo tradicional, confeccionando las diligencias de informe correspondientes para la Autoridad Judicial. La evidencia legal del contenido de la intervención es aportada por el Servidor Central, responsable del volcado de todos los datos a formato DVD para su entrega a la Autoridad Judicial pertinente, constituyéndose como la única versión original. De este modo el espacio de almacenamiento se reduce considerablemente, facilitando su entrega por la unidad de investigación a la Autoridad Judicial competente, verificándose que en sede central no queda vestigio de la información.

Sobre esta cuestión, llama la atención que el artículo 588 *ter* f LECrim obligue a la Policía Judicial a efectuar la transcripción de los pasajes que considere de interés, debiendo remitirlas al órgano judicial junto con las grabaciones íntegras. A este respecto, la doctrina plantea si bastará con transcripciones resumidas o si será necesario que se acompañe, además, transcripción literal completa, así como si bastará que el Letrado de la Administración de Justicia efectúe el correspondiente cotejo.[563]

Por otro lado, también aparecen algunos puntos conflictivos en el funcionamiento del sistema, y en particular en cuanto a i) la seguridad de que lo grabado en los DVD coincida con las conversaciones mantenidas, ii) el riesgo de automatización en el tratamiento de los datos; y iii) el destino de las grabaciones tras finalizar su utilización.

En cuanto a la primera de dichas problemáticas, la jurisprudencia parece afirmar que el sistema cumple con las exigencias suficientes[564], si bien es posible que las partes impugnen la autenticidad o integridad de las grabaciones contenidas en el DVD. A este respecto, debe tenerse en cuenta que, conforme a la STS 143/2013, de 28 de febrero, será necesario que las partes expliquen suficientemente la base de su sospecha y que la impugnación formulada tenga fundamentación sustantiva, además de deber plantearse en el momento procesal oportuno, con antelación al juicio oral.

Respecto a la segunda de las problemáticas comentadas, relativa a la posible extensión de las herramientas del sistema a todos los datos facilitados, el artículo 39.5 LGT establece que los datos facilitados serán los que se indiquen en la orden de interceptación legal, por lo que la extensión será la que determine el juez autorizante[565].

Por último, en cuanto al destino de las grabaciones tras finalizar su utilización, el artículo 588 *bis* k) LECrim despeja cualquier motivo de preocupación que pudiera existir al respecto, al establecer que una vez que se ponga término al procedimiento mediante resolución firme, se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida. Se conservará una copia bajo custodia del Letrado de la Administración de Justicia y se acordará la destrucción de las copias conservadas cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan

---

[563] BARRIO ANDRÉS, M., *Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 260.
[564] SSTS 554/2012, 753 y 250/2009.
[565] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 437.

prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación a juicio del Tribunal.

Este sistema hay que ponerlo en comparación con otros conocidos, como los sistemas *Carnivore*, *Echelon* y *Prism*. En particular, el programa *Prism* permitía a las agencias NSA, FBI y CIA recabar información de correos electrónicos, llamadas vía internet y chats *on line*, y contaba con la colaboración de grandes compañías como *Facebook*, *Google*, *Apple*, y *Skype*[566].

E. EL FUTURO DE LA RETENCIÓN DE DATOS

No podemos finalizar este apartado sin referirnos también a la posible evolución que la actualidad comunitaria parece dibujar en cuanto al régimen de la retención de datos. Si esta pudo sobrevivir a las sentencias del TJUE de 8 de abril de 2014[567] y de 21 de diciembre de 2016[568], las sentencias de 6 de octubre de 2020[569] vuelven a poner en el punto de mira aquellas legislaciones nacionales que, como la nuestra, imponen a un proveedor de servicios de comunicaciones electrónicas la obligación de conservar de manera general e indiscriminada los datos de tráfico y localización de sus usuarios[570].

El centro de la cuestión es que, para el TJUE, la conservación de datos constituye en sí una injerencia en el derecho al secreto de las comunicaciones y, en consecuencia, su adopción –la mera conservación de datos– debe tener lugar conforme al principio de proporcionalidad. Las legislaciones nacionales, aunque prevén en algunos casos, como sucede con la española, un régimen restrictivo y la exigencia de previa autorización judicial en el momento de la cesión de los datos conservados, prevén también una conservación generalizada, indiferenciada e indiscriminada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados, lo que en sí determina que no sea

---

[566] "U.S. v. Hasbajrami – Brief of Amici Curiae ACLU and EFF in Support of Defendant–Appellant and Reversal", *American Civil Liberties Union*, fecha de consulta 2 mayo 2020, en https://www.aclu.org/legal–document/us–v–hasbajrami–brief–amici–curiae–aclu–and–eff–support–defendant–appellant–and.
[567] Asuntos acumulados C–293/12 y C–594/12 Digital Rights Ireland y Seitlinger y otros.
[568] Asuntos acumulados C–203/15 Tele2 Sverige AB / Post– och telestyrelsen y C–698/15 Secretaty of State for the Home Department/Tom Watson y otros.
[569] Asuntos acumulados La Quadrature du Net y otros (C–511/18 y C–512/18), Ordre des barreaux francophones et germanophone y otros (C–520/18) y Privacy International (C–623/17).
[570] SÁNCHEZ GUARIDO, A.; MEDINA, A. M., "El TJUE reabre el debate entre privacidad o seguridad nacional", *Diario La Ley*, 9743, 2020, Wolters Kluwer, p. 2.

conforme con el Derecho de la Unión Europea y, en particular, con la Directiva 2002/58/CE y la CDFUE.

Hasta ahora, los Estados miembros habían defendido que los regímenes de retención y conservación de datos estaban exentos del ámbito de aplicación de la Directiva 2002/58 y del Derecho de la UE en materia de protección de datos porque servían al objeto de la seguridad pública, la defensa, la seguridad del Estado y la averiguación de delitos. No obstante, las últimas sentencias entienden que el concepto de "seguridad nacional" debe interpretarse de manera restrictiva, exclusivamente para los casos en que los Estados ejerzan de manera directa y por sus propios medios sus competencias en materia de seguridad nacional, de manera que sean actividades ajenas a la esfera de los particulares.

Ahora bien, es cierto también que las conclusiones de los Abogados Generales Campos Sánchez–Bordona y Pitruzzella señalan posibles vías de escape que permitan a los Estados miembros satisfacer su legítimo interés en mantener la seguridad interna, y para ello se hace referencia a varios elementos.

Por un lado, se recuerda la Decisión Marco 2006/960/JAI, del Consejo, de 1 8de diciembre de 2006, sobre simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea, que preveía la posibilidad de excluir las actividades estatales de obtención de información e inteligencia criminal del régimen de privacidad y comunicaciones electrónicas. Ello permitiría, en palabras de la doctrina más autorizada, que los Estados miembros elaborasen sistemas propios de recolección y almacenamiento de datos personales que sí podrían conservar[571]. A tal efecto, el Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración y por el que se modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816, prevé la creación de un Portal europeo de búsqueda (PEB) con objeto de facilitar el acceso en casos rápido, ininterrumpido, sistemático y controlado de las autoridades de los Estados miembros y de las agencias de la

[571] ORTIZ PRADILLO, J. C., "Europa", cit., p. 13.

Unión a los sistemas de información de la UE, a los datos de Europol y las bases de datos de Interpol.

Por otro lado, las conclusiones de los Abogados Generales prevén también la posibilidad de imponer una obligación de conservación de datos a empresas privadas siempre que se trate de situaciones excepcionales, en las que concurra una amenaza inminente o un riesgo extraordinario.

En lo que atañe a nuestro ordenamiento, la Ley 25/2007 peca, fundamentalmente, de no incluir criterios legales objetivos que permitan lo que se ha venido en denominar como "conservación selectiva" de los datos. No existen criterios subjetivos, geográficos, teleológicos o temporales que permitan argumentar que nuestra retención de datos es selectiva. Se hace necesario, por tanto, adoptar una reforma que incorpore dichos criterios para garantizar la proporcionalidad de la injerencia.

2. DIFERENCIAS CON LA ORDEN DE CONSERVACIÓN

La orden de conservación de datos se encuentra prevista en el artículo 588 *octies* LECrim, cuando establece que "El Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión con arreglo a lo dispuesto en los artículos precedentes. Los datos se conservarán durante un periodo máximo de noventa días, prorrogable una sola vez hasta que se autorice la cesión o se cumplan ciento ochenta días. El requerido vendrá obligado a prestar su colaboración y a guardar secreto del desarrollo de esta diligencia, quedando sujeto a la responsabilidad descrita en el apartado tres del artículo 588 *ter* e."

Constituye una auténtica medida de aseguramiento vinculada a investigaciones concretas y permite a España cumplir definitivamente los compromisos adquiridos en el artículo 16 del Convenio sobre Ciberdelincuencia, cuando dispone que "1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático, en particular cuando existan razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación. 2. Cuando una Parte aplique lo dispuesto en el anterior apartado 1 por medio de una orden

impartida a una persona para conservar determinados datos almacenados que se encuentren en posesión o bajo el control de dicha persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a esa persona a conservar y a proteger la integridad de dichos datos durante el tiempo necesario, hasta un máximo de noventa días, de manera que las autoridades competentes puedan conseguir su revelación. Las Partes podrán prever que tales órdenes sean renovables."

La medida permite garantizar la preservación de datos e informaciones que pudieran existir en sistemas de almacenamiento, que supera el ámbito de los meros obligados por el deber de colaboración al que nos hemos referido en apartados anteriores, pudiendo dirigirse, no sólo a los operadores de comunicaciones, sino a los proveedores de servicios de internet y, en general, a cualquier persona física y jurídica que tenga a su disposición los datos cuya conservación se interesa.

La orden de conservación permite que sea posible aportar estos datos como medio de prueba o utilizarlos para actividad forense, sin que su utilidad quede frustrada por una indeseable desaparición, alteración o deterioro. El plazo máximo de duración de la medida es de 90 días, prorrogable hasta los 180 días como máximo.

Debe destacarse que la orden de conservación de datos únicamente obliga al destinatario a asegurar su conservación, pero no implica que las autoridades puedan acceder a dicha información, para lo que será necesaria la autorización pertinente.

Por último, es necesario destacar que la orden de conservación de datos puede revestir especial importancia en las investigaciones relativas a ciberdelitos, considerando la especial volatilidad que afecta a los rastros de este tipo de actividades. Puede referirse a cualquier tipo de dato (ya sean datos de contenido, datos de tráfico, o incluso datos de abonado) y cualquier tipo de delitos, e incluso se prevé la posibilidad de que sea un instrumento de cooperación internacional, al prever el artículo 29.7 del Convenio sobre la Ciberdelincuencia que deban ser válidas, al menos, durante un periodo de 60 días, cn la finalidad de que la parte requirente pueda presentar una solicitud de registro, de embargo, de acceso obtención de los datos por un medio similar, o de divulgación de los datos sometidos a conservación.

3. MANIFESTACIONES DEL DEBER DE COLABORACIÓN EN LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA

Con la entrada en vigor de la LO 13/2015, el deber de colaboración queda definido de manera más completa en nuestra legislación procesal, concretando así la genérica previsión de la obligación de colaborar con los Jueces que imponen los artículos 118 CE y 17 LOPJ. La decisión del legislador ha sido la de tratarlo separadamente en todas aquellas medidas de investigación tecnológica en las que se prevé su necesidad, lo cual ha permitido incluir algunas especialidades concretas dependiendo de la medida de investigación en que dicha colaboración sea necesaria.

Así, el régimen jurídico del deber de colaboración queda previsto en los artículos 588 *ter* e, en materia de interceptación de comunicaciones electrónicas, 588 *quinquies* b), en materia de utilización de medios técnicos de seguimiento; iii) apartado quinto del artículo 588 *sexies* c, en materia de registros de dispositivos de almacenamiento masivo; y iv) 588 *septies* b, en materia de registros remotos. En este apartado exploraremos dichas manifestaciones, y en los demás apartados de este capítulo nos dedicaremos a elementos que afectan transversalmente a varias de dichas modalidades.

En todo caso, hay que partir de que la obligación de asistencia y colaboración viene complementada con otra de guardar secreto acerca de las actividades requeridas por las autoridades, pues si las personas investigadas llegaran a tener conocimiento de ellas podría frustrarse el fin de la investigación. El incumplimiento de cualquiera de estas dos obligaciones –asistencia y colaboración, y secreto– podrá dar lugar a un delito de desobediencia.

A. EL DEBER DE COLABORACIÓN EN LA INTERCEPTACIÓN DE COMUNICACIONES ELECTRÓNICAS

Este deber de colaboración se encuentra previsto en el artículo 588 *ter* e) LECrim, cuando establece que “Todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, están obligados a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración

precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones".

En términos sintéticos, podríamos decir que este precepto obliga a cualquier tercero –sin importar que se trate de persona jurídica o física, de gran empresa o pequeña empresa, mientras preste servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de sociedad de la información, o que contribuya de cualquier manera a facilitar la comunicación a través de cualquier medio telemático, lógico o virtual– que, de algún modo, intervenga para facilitar o hacer posible de cualquier forma las comunicaciones objeto de la medida de investigación tecnológica, a colaborar con el juez, con el Ministerio Fiscal y con la Policía Judicial para que pueda ejecutarse y llevarse a buen término la medida de intervención adoptada.

En comparación con la regulación anterior, con la entrada en vigor de la LO 13/2015 se han ampliado los sujetos obligados, distinguiéndose tres grupos principales[572]:

Por un lado, los prestadores de servicios de telecomunicaciones y de acceso a redes de telecomunicaciones, tradicionalmente obligados conforme a los artículos 33 y 36.2 de la antigua LGT, ahora artículos 39 y 43 de la vigente Ley General de Telecomunicaciones.

Por otro lado, los prestadores de servicios de la sociedad de la información, concepto en el que se incluyen, atendiendo a la exposición de motivos de la Ley 34/2002, los portales web, los motores de búsqueda o cualquier otro sujeto que efectúe contrataciones de bienes y servicios por vía electrónica, suministre información, o preste, en general, cualquier otro servicio a través de un sitio en internet[573].

Y, finalmente, *"cualquier otra persona que de algún modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual"*. La amplitud de esta previsión provoca que pueda englobar todo tipo de terceros y que, incluso, se plantee la cuestión de cuál es el contenido

---

[572] DELGADO MARTÍN, J. en Investigación tecnológica y prueba digital en todas las jurisdicciones, Wolters Kluwers, Madrid, 2016, p. 410.

[573] "Circular 2/2019, de 29 de marzo, del Banco de España, sobre los requisitos del Documento Informativo de las Comisiones y del Estado de Comisiones, y los sitios web de comparación de cuentas de pago, y que modifica la Circular 5/2012, de 27 de junio, a entidades de crédito y proveedores de servicios de pago, sobre transparencia de los servicios bancarios y responsabilidad en la concesión de prestamos.", p. 2, fecha de consulta 25 abril 2020, en https://www.boe.es/buscar/act.php?id=BOE–A–2019–4955&p=20190404&tn=2.

de la acción de "contribuir o facilitar" como requisito para quedar obligado. En principio, el abanico de posibilidades es tan amplio como servicios pueden presentarse en el *ciberespacio*.

En cuanto al alcance de dicha obligación, en el caso de prestadores de servicios de telecomunicaciones y de acceso a redes de telecomunicaciones que estén operando con redes públicas ubicadas en territorio español no se plantearán tantas dudas, pero sí surgen problemas (especialmente, de jurisdicción) cuando se trate de obligados que se encuentren ubicados fuera de las fronteras españolas, como ocurrirá frecuentemente con los prestadores de servicios de la sociedad de la información, habida cuenta de su marcado carácter internacional.

Podemos prever tres escenarios diferentes: i) que el obligado tenga un establecimiento del servicio en España, supuesto en el que conforme al artículo 2.4 LSSICE estarán sujetos a las demás disposiciones del ordenamiento jurídico español que les sean de aplicación, incluyendo, por tanto, los preceptos que regulan el régimen de colaboración; ii) que el obligado no tenga un establecimiento del servicio en España, pero sí en alguno de los Estados Miembros de la Unión Europea, supuesto en el que la colaboración deberá efectuarse conforme al régimen previsto en la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea; y iii) que el obligado no tenga un establecimiento del servicio en España ni en ningún Estado Miembro de la Unión Europea, supuesto en el que será necesario acudir al auxilio judicial internacional, mediante la comisión rogatoria correspondiente, en función de los instrumentos internacionales adoptados.

En la misma sección correspondiente a la interceptación de comunicaciones electrónicas la LECrim también prevé el deber de colaboración previo requerimiento judicial, de los mismos sujetos del artículo 588 *ter* e LECrim para ceder los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso, en los casos en que la Policía Judicial tuviera acceso a una dirección IP que estuviera siendo utilizada para cometer algún delito. Ya hemos comentado que está aceptado que la Policía Judicial pueda obtener una dirección IP sin autorización judicial, no sólo con base en consolidada jurisprudencia al respecto[574], sino también con

[574] SSTS 342/2013, de 17 de abril, y 680/2010, de 14 de julio, que cita la 739/2008 y la 236/2008, entre otras muchas.

base en lo dispuesto en el artículo 588 *ter* k LECrim, cuando se desenvuelve sobre la base lógica de que la Policía Judicial haya obtenido, sin necesidad de autorización judicial, la dirección IP objeto de investigación.

B. El deber de colaboración en la utilización de medios técnicos de seguimiento

Este deber está previsto en el apartado tercero del artículo 588 *quinquies* b) LECrim que, a su vez, remite expresamente a la regulación contenida en el artículo 588 *ter* e) LECrim, al establecer que "Los prestadores, agentes y personas a que se refiere el artículo 588 *ter* e están obligados a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos por los que se ordene el seguimiento, bajo apercibimiento de incurrir en delito de desobediencia".

Este deber de colaboración se regula en el marco de las diligencias de utilización de dispositivos o medios técnicos de seguimiento y localización. La geolocalización puede realizarse a través de dispositivos técnicos basados en sistemas de posicionamiento global (GPS, GLONASS, etc.) o a través de los datos electrónicos asociados a sistemas de comunicación telefónica. Esta segunda modalidad, denominada como *"medios técnicos de seguimiento"*, se basa en que la localización se efectúe mediante medios pertenecientes al *Global System for Mobile Communications* (GSM), cuyos datos obran en poder de las compañías de telecomunicaciones, a las que será de aplicación el régimen jurídico previsto para el deber de colaboración en materia de intervención de comunicaciones. Como señala la Circular 4/2019, de 6 de marzo, de la Fiscal General del Estado, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, el posicionamiento a través de los datos asociados a sistemas de comunicación telefónica se consigue gracias al llamado sistema global para las comunicaciones móviles (GSM, del inglés *Global System for Mobile Communications*), servicio proporcionado por las empresas de telecomunicaciones que permite determinar la posición aproximada de un teléfono móvil gracias a su constante conexión con las estaciones BTS.

En la localización GSM, por tanto, el oficio judicial deberá dirigirse a las compañías de telecomunicaciones y, en ambos casos, con sujeción a las prescripciones contenidas en los arts. 588 *quinquies* b) y c). De ahí la importancia del deber de colaboración en este aspecto.

Estos datos de geolocalización deben ser considerados datos asociados a las comunicaciones telefónicas, aunque no datos de tráfico, ya que pueden generarse independientemente del mantenimiento o no de una comunicación.

A ese respecto, merece la pena tener en cuenta que conocer un solo dato de geolocalización puede afectar a la intimidad del investigado; pero la recopilación sistemática de estos datos y su tratamiento informático puede proporcionar información precisa sobre los hábitos de una persona, lo que supone una intromisión mucho más intensa en la intimidad del investigado, por lo que se entiende que afecta también al derecho a la protección de datos personales del investigado (art. 18.4 CE).

En cuanto a si ese deber de colaboración se extiende también a otras personas que sean ajenas al proceso de comunicación telefónica, se ha concluido que ello sería posible porque el ámbito de posibles colaboradores que describe el artículo 588 *ter* e) LECrim es suficientemente amplio como para darles cabida[575].

C. EL DEBER DE COLABORACIÓN EN EL REGISTRO DE DISPOSITIVOS DE ALMACENAMIENTO MASIVO

Este deber está previsto en el apartado quinto del artículo 588 *sexies* c) LECrim. La necesidad de este deber de colaboración se justifica porque se entiende una medida necesaria para identificar y obtener los datos que puedan servir de prueba en el proceso ante dos posibles dificultades: i) la de localizar los datos en sistemas que contengan un gran volumen de información; y ii) la de acceder a datos protegidos por medidas de seguridad; y iii) la reducción de la duración del registro[576].

Del contenido del artículo, que sirve para dar cumplimiento a los compromisos adquiridos en el artículo 19.4 CDC, hay que destacar los siguientes aspectos: i) el deber de colaboración debe requerirse en el marco de una investigación por delito; ii) los acreedores de dicha colaboración serán el Juez, el Ministerio Fiscal, o los agentes de Policía Judicial que estén ejecutando la medida; iii) no existe limitación en cuanto al contenido

[575] "Circular 4/2019, de 6 de marzo, de la Fiscal General del Estado, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización.", fecha de consulta 25 abril 2020, en https://www.boe.es/diario_boe/txt.php?id=BOE–A–2019–4243.
[576] "Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre registro de dispositivos y equipos informáticos.".

o naturaleza de los datos a registrar, siempre que el alcance esté cubierto por el auto judicial que acuerda la medida.

En cuanto a los sujetos obligados, serán todos aquellos que conozcan el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos, por lo que cualquier persona que pueda tener algún conocimiento sobre la ubicación virtual de los datos o sobre el funcionamiento de las medidas de seguridad podría quedar, en principio, afectada por el deber de colaboración. Por tanto, ese deber no se limitará exclusivamente a personas con conocimientos técnicos, sino que, incluso, puede tratarse de empleados que tengan conocimiento de dónde se encuentra esa información o que dispongan de las claves de acceso. Incluso pudiera ser que el obligado no tuviera relación directa con el sistema informático a registrar, sino que pudiera entenderse obligado el fabricante del dispositivo, o incluso un investigador que tuviera especial conocimiento al respecto, y en todo caso, cuando el sujeto obligado por el deber de colaboración sea una persona jurídica, será necesario que identifique a la persona física que, dentro de ella, tuviera el conocimiento necesario.[577]

Los problemas de territorialidad y jurisdicción surgirán cuando el dispositivo o sistema informático a registrar sea accesible telemáticamente desde España, pero se sitúe en el extranjero (supuestos de *cloud computing*). Si la persona obligada se hallara en territorio español, estaría obligada a ese deber de colaboración con independencia del lugar donde se encontrasen los datos. Por el contrario, si el obligado no estuviese en territorio español, sería necesario hacer uso de los mecanismos de cooperación internacional.

En cuanto a los límites que pudieran surgir en torno a esta medida, desde un punto de vista subjetivo hay que excluir al propio investigado o encausado, a sus parientes más próximos y a quienes se vean exentos de la obligación de declarar en virtud del secreto profesional. Todo ello en virtud, respectivamente, del derecho de defensa del investigado, (artículo 416.1 LECrim, y del artículo 24.2 CE). Sobre este aspecto, merece la pena destacar que el art. 588 *sexies* c.5 limita el espectro de los sujetos dispensados de la obligación a los incluidos en el art. 416.2 LECrim, esto es, los abogados, pero no incluye a otros también afectados por el secreto profesional, como podrían ser los traductores o

[577] *Ibid.*

intérpretes (art. 416.3 LECrim), los eclesiásticos y ministros de cultos disidentes (art. 417.1 LECrim) o los funcionarios públicos (art. 417.3 LECrim), por ejemplo

Por su parte, desde un punto de vista objetivo habrá que excluir aquellos requerimientos que impliquen una carga desproporcionada para el afectado. El concepto de carga desproporcionada es un concepto jurídico indeterminado ya utilizado en el Convenio de Budapest, cuyo informe explicativo[578] cita como ejemplo de petición irrazonable los casos en los que "la divulgación de la contraseña u otra medida de seguridad pudiera poner en peligro injustificadamente la vida privada de otros usuarios o de otros datos cuya revisión no ha sido autorizada". La Fiscalía General del Estado añade como supuestos de irrazonabilidad los casos en los que facilitar la información supusiera desvelar secretos industriales que implicaran un perjuicio para la actividad empresarial. En general, admite la necesidad de ir "caso a caso", recordando en todo momento que será el auto judicial el que deberá valorar la proporcionalidad de la exigencia de colaboración, atendiendo al sacrificio de los derechos e intereses de la persona afectada, el beneficio para el interés público y el de terceros que quepa esperar de dicha colaboración[579].

D. El deber de colaboración en la práctica del registro remoto

Este deber queda previsto en el artículo 588 *septies* b) LECrim y excede del ámbito del contenido del apartado quinto del artículo 588 *sexies* c) porque incluye, también, a los prestadores de servicios y personas señaladas en el artículo 588 *ter* e, así como a los titulares o responsables del sistema informático o base de datos.

El apartado segundo del artículo 588 *septies* b) reproduce casi literalmente el apartado apartado quinto del artículo 588 *sexies* c), por lo que incluye aquí el mismo deber de colaboración que en el caso de los registros de dispositivos de almacenamiento masivo, con las mismas limitaciones materiales (facilitar información) y subjetivas (propio investigado y demás sujetos del artículo 416 LECrim) pero no incluye la posibilidad de que el requerido se excuse de la colaboración demandada cuando de ello se le derive una carga desproporcionada. Encontramos, sin embargo, que esta omisión cuenta con escasa eficacia, pues siempre deberá reconocerse la posibilidad de que el requerido se excuse por

[578] "Informe explicativo de Convenio sobre la Ciberdelincuencia", fecha de consulta 25 abril 2020, en https://rm.coe.int/16802fa403.
[579] "Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre registro de dispositivos y equipos informáticos.".

suponer para él la colaboración una carga desproporcionada cuando la colaboración le suponga la infracción de deberes legales o derivados del ejercicio legítimo de sus derechos, de un oficio o de un cargo (art. 20.7º CP). El respeto a los derechos fundamentales también aparece recogido en el art. 591 LEC como fundamento de la excusa del deber de colaboración con la Administración de Justicia.

Además del deber de facilitar información, el artículo 588 *septies* 1 incluye en el general deber de colaboración la obligación de prestar la colaboración precisa para la práctica de la medida y el acceso al sistema, así como para que los datos e información recogidos puedan ser objeto de examen y visualización. Serán sujetos obligados los prestadores de servicios y personas señaladas en el artículo 588 *ter* e y los titulares o responsables del sistema informático o base de datos objeto del registro, esto es, "los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual".

En la medida en que los obligados serán las entidades encargadas de facilitar la comunicación o los responsables de los sistemas informáticos, la colaboración a la que habrá que entender circunscrito el deber será la que pudiera facilitarse como intermediador en la comunicación entre los sistemas, o como responsable del diseño y seguridad del propio sistema y, en último término, como responsable de la legibilidad de los datos (que los datos e información recogidos puedan ser objeto de examen y visualización, dice el precepto). Entiende la Fiscalía General del Estado que esa interpretación ampararía la posibilidad de que el prestador de telecomunicaciones inocule un virus en el sistema del investigado o del responsable de un sistema informático para que pase por alto la alerta de seguridad que pudiera haber detectado como consecuencia de la monitorización de la actividad del investigado[580].

De todo ello resulta que la diferencia entre uno y otro deber reside en que en el caso del artículo 588 *septies* 2 (similar al 588 *sexies* c.5) la colaboración se agota en

[580] *Ibid.*, p. 67.

facilitar información (claves o ubicación de los archivos), mientras que en el caso del artículo 588 *septies* 1 la colaboración puede implicar la asunción de labores o trabajos[581].

A lo anterior hay que añadir, como ya se dijo, la obligación de guardar silencio (artículo 588 *septies* b) respecto de las actividades que les hayan sido demandadas por las autoridades. Es una especialidad de este deber respecto del deber del apartado quinto del artículo 588 *sexies* c), pero justificada por la posibilidad de frustrar el fin del registro remoto si el investigado, que mantiene la disponibilidad material del bien, llega a sospechar su ejecución.

4. DEBER DE COLABORACIÓN DEL PROPIO SUJETO INVESTIGADO: EL DEBATE ACERCA DE LA AUTOINCRIMINACIÓN

Debemos recordar que el derecho a no declarar contra sí mismo se encuentra recogido en el artículo 24.2 CE. Tradicionalmente, su previsión legislativa, en el artículo 520 LECrim, se refería exclusivamente respecto del detenido o preso, pero con la LO 5/2015, de 27 de abril, se previó específicamente el derecho, en general, a guardar silencio y a no declarar si no se desea. Posteriormente, la Directiva (UE) 2016/343 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, estableció la obligación de los Estados miembros de garantizar que los sospechosos y acusados tengan derecho a guardar silencio en relación con la infracción penal de que sean sospechosos o se les acuse, así como a no declarar contra sí mismos[582]. Nuestro Tribunal Constitucional declaró siempre que en el derecho a no declararse culpable se incluye también la negativa a someterse a un interrogatorio inculpatorio, entre otras en la STC 161/1997, de 2 de octubre, con cita de las STEDH de 17 de diciembre de 1996 –Saunders c. Reino Unido–, de 25 de febrero de 1993 (*Funke c. Francia*) y de 8 de febrero de 1996 (*John Murray c. Reino Unido*)[583].

El apartado quinto del artículo 588 *sexies* c) establece que el investigado o encausado, o las personas dispensadas de la obligación de declarar por razón de parentesco o

---

[581] Esta ampliación material encuentra su justificación, para la Circular 5/2019 de la Fiscalía General del Estado, sobre registro de dispositivos y equipos informáticos, en el ámbito más restringido en el que puede adoptarse un registro remoto, lo que justificaría tanto una mayor intromisión en los derechos del investigado como un deber de colaboración más complejo, como en la mayor dificultad que entrañan.

[582] Lo que incluye la improcedencia de las llamadas "preguntas a nadie". Esto es, la pretensión de alguna de las partes de hacer constar en el acto las preguntas que se formularían al investigado o acusado, si quisiera responderlas, práctica esta que ha merecido la reprobación de los tribunales, como sucede en las SSTS 686/2016, de 26 de julio, y 176/2008, de 24 de abril.

[583] DEL MORAL GARCÍA, A., "A vueltas con el derecho al silencio del acusado", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, pp. 1303–1322*, Ediciones Jurídicas Castillo de Luna, 2020, p. 1306, fecha de consulta 17 agosto 2021, en https://dialnet.unirioja.es/servlet/articulo?codigo=7871545.

que lo tienen prohibido en virtud del secreto profesional, no podrán verse ordenados por las autoridades o agentes encargados de la investigación, aunque conozcan el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo, a facilitar la información que resulte necesaria para el buen fin de la investigación.

El contenido de este artículo ha provocado que la doctrina[584] se plantee si ello implica que la entrega de las claves o códigos que permiten el acceso policial a dispositivos electrónicos o datos informáticos pueda constituir un supuesto de autoincriminación.

Por un lado, los pronunciamientos del TS y TC dejan poco margen a la duda en cuanto a que no debe considerarse como autoincriminación porque el investigado o encausado no está efectuando confesión alguna de haber participado en un hecho delictivo, sino que únicamente facilita determinada información para acceder a una fuente de prueba de la que se desconoce su utilidad incriminatoria y exculpatoria. Es la lógica que subyace a los pronunciamientos en materia de formación de cuerpos de escritura o de práctica de pruebas de alcoholemia, a lo que se refiere la STC 103/1985, de 4 de octubre, cuando establece que "el deber de someterse al control de alcoholemia no puede reputarse contrario al derecho a declarar contra sí mismo y a no confesarse culpable, pues no se obliga al conductor a emitir una declaración que exteriorice un contenido de voluntad o de conocimiento, admitiendo su culpabilidad, sino a tolerar que se le haga objeto de una modalidad de pericia, exigiéndole una colaboración que nunca podrá equiparase a la declaración mencionada en la Constitución", y la STS 151/2010, de 22 de febrero, cuando indica que "las pruebas de precisión alcoholométrica –, ya consistan en la expiración de aire, ya en la extracción de sangre, en el análisis de orina o en un examen médico, no constituyen actuaciones encaminadas a obtener del sujeto el reconocimiento de determinados hechos o su interpretación o valoración de los mismos, sino simples pericias de resultado incierto que, con independencia de que su mecánica concreta no requiera solo un comportamiento exclusivamente pasivo, no pueden catalogarse como obligaciones de autoincriminarse, es decir, como aportaciones o contribuciones del sujeto que sostengan o puedan sostener directamente" (STC 161/1997, 2 de octubre)".

[584] MARTÍN RÍOS, P., "La colaboración del investigado/encausado en el registro de dispositivos de almacenamiento masivo de información", cit., p. 154.

Sin, embargo, por otro lado, el legislador de la Ley Orgánica 13/2015, de 5 de octubre ha provocado que surja la duda en cuanto a la facilitación por el investigado o encausado a los agentes policiales de la información que resulte necesaria para el buen fin de la investigación, en la medida en que lo dispensa de atender dicha obligación[585].

Esta circunstancia ha obligado a recordar que, para ser coherentes con el tratamiento dispensado por el legislador, tal vez podría exigirse la presencia de abogado del investigado en el momento en que a este se le plantease la posibilidad de suministrar cualquier información relativa a la obtención de datos, así como la necesidad de que la policía judicial informe debidamente al mismo investigado de la posibilidad que le asiste de negarse a facilitar dichas información, con las consiguientes consecuencias en caso de incumplimiento de dicha obligación[586].

La situación descrita contrasta con las medidas adoptadas en otras jurisdicciones, en las que sí se ha previsto que los poderes de investigación tengan la facultad de exigir a los investigados las contraseñas de acceso a sus archivos o dispositivos de almacenamiento masivo de la información, y que la negativa de estos a atender dicho requerimiento constituya un ilícito penal.

En Reino Unido, dicha posibilidad está prevista en la *Regulation of Investigatory Powers Act 2000* (RIPA), y más en concreto en su S.49, que entró en vigor en 2007. Según esa previsión, la policía puede reclamar la desvelación de la contraseña si la razón es prevenir o detectar el delito, proteger la seguridad nacional o el bienestar económico de Reino Unido. Se ha denunciado que esas definiciones permiten ser aplicadas de manera amplia hasta el punto de cubrir la investigación de cualquier crimen, con independencia de su gravedad.[587] Posteriormente, en 2016, se ha aprobado otra[588] Investigatory Powers Act[589] que atribuye nuevos poderes investigativos[590], así como una regulación de la

---

[585] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., p. 416.
[586] MARTÍN RÍOS, P., "La colaboración del investigado/encausado en el registro de dispositivos de almacenamiento masivo de información", cit., p. 156.
[587] "Prosecuted for your password", fecha de consulta 10 abril 2020, en https://www.saunders.co.uk/news/prosecuted–for–your–password.html.
[588] "Investigatory Powers Act 2016", *Wikipedia*, 2020, fecha de consulta 10 abril 2020, en https://en.wikipedia.org/w/index.php?title=Investigatory_Powers_Act_2016&oldid=942893147.
[589] "Investigatory Powers Act 2016", Queen's Printer of Acts of Parliament, fecha de consulta 10 abril 2020, en http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.
[590] "Police Computer Hacking Powers and Civil Liberties", fecha de consulta 24 octubre 2020, en http://www.civilrightsmovement.co.uk/police–computer–hacking–powers–civil–liberties.html.

retención de datos[591]. La negativa a cumplir dicho requerimiento puede resultar en una pena de dos años de prisión, y hasta de cinco si el delito investigado perjudica la seguridad nacional o está relacionado con el abuso de menores.

Dicha posibilidad también está prevista en la *Terrorism Act 2000*[592], que igualmente permite a la policía reclamar las contraseñas de acceso a los dispositivos de los requeridos. Esta disposición también permite a la policía parar, registrar, preguntar y detener a cualquier persona en los puertos y aeropuertos británicos para determinar si han estado involucrados en la comisión, preparación o instigación de actos de terrorismo, con independencia de lo razonable que sea la sospecha[593].

Aunque no parece que sea un recurso profusamente utilizado, lo cierto es que su uso si se está incrementando, y podría generar un resultado completamente desproporcionado en la medida en que alguien pudiera resultar encarcelado por no entregar una contraseña cuando fuera objeto de una investigación criminal por un crimen que en realidad no hubiera cometido.

Parece evidente que, desde el comienzo de la *War on Terror*, los países occidentales han adoptado medidas gravemente restrictivas de los derechos fundamentales más básicos, justificándose su adopción bajo la necesidad de responder en igualdad de condiciones respecto de aquellos que utilizan nuestro sistema garantista para provocar terror en nuestras estructuras sociales y políticas. Pero lo que sucede ahora es que dichas graves disposiciones pueden trasladarse a las investigaciones domésticas, tradicionales, afectando y aplicándose a todo el espectro de individuos que utiliza dispositivos informáticos.

5. APORTACIÓN VOLUNTARIA DE DATOS A PRESTADORES DE SERVICIOS

A nadie escapa que, si existen algoritmos que permiten a las empresas detectar tendencias, gustos y necesidades, predecir comportamientos y, en definitiva, anticiparse a los deseos de las personas para facilitarles los productos y servicios demandados, dichos

[591] "The Data Retention and Acquisition Regulations 2018", Queen's Printer of Acts of Parliament, fecha de consulta 10 abril 2020, en http://www.legislation.gov.uk/uksi/2018/1123/made/data.htm.
[592] "Terrorism Act 2000", Statute Law Database, fecha de consulta 10 abril 2020, en https://www.legislation.gov.uk/ukpga/2000/11/schedule/7.
[593] Es el caso de Muhammad Rabbani, por ejemplo, que puede encontrarse aquí: https://www.bbc.com/news/uk–41394156

algoritmos podrían permitir también al poder público reconstruir los movimientos e interacciones de las personas en el marco de cualquier investigación criminal[594].

A. LA VOLUNTARIEDAD Y LIBERTAD EN LOS COMPORTAMIENTOS EN LA RED

Quisiéramos hacer referencia también a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información. Estos sujetos, con ocasión de la prestación de sus servicios, registran y almacenan datos vinculados a procesos de comunicación que se hayan efectuado mediante las redes de telecomunicación o en el ciberespacio. Estos datos tienen una relevancia fundamental en la investigación y prueba de los *ciberdelito*s, en la medida en que sirven para poder acreditar o construir el relato de hechos, y también para el resto de ilícitos.

El rastro de dichos datos queda, especialmente, en los llamados ficheros históricos o ficheros *log*. Estos registros se llevan de manera automática y su conservación es lo que permite que posteriormente pueda trazarse el histórico de hechos sucedidos en el *ciberespacio*. Dentro de los datos que se guardan en dichos ficheros, tienen especial relevancia los que permiten vincular una dirección IP con un usuario específico[595].

La utilidad de estos datos puede reconocerse desde una doble perspectiva[596]: por un lado, sirve para establecer o refutar tesis policiales, verificar coartadas, excluir o incluir objetivos, identificar testigos, determinar lugares relacionados con la acción criminal, localizar medios de resarcimiento de las víctimas, etc.; por otro lado, sirven como fuente de pruebas para acreditar los hechos sucedidos y son fundamentales para construir la prueba de indicios.

En la actualidad, la generalidad[597] de las personas ya conoce las prácticas en las que incurren las compañías dedicadas a la prestación de servicios de la sociedad de la información –o, al menos, aquellas cuyo modelo productivo gira en torno a la prestación de servicios publicitarios–[598].

---

[594] ORTIZ PRADILLO, J. C., "Europa", cit., p. 4.
[595] LÓPEZ, A., "La investigación policial en Internet: estructuras de cooperación internacional", *IDP: revista de Internet, derecho y política = revista d'Internet, dret i política*, 5, 2007, Universitat Oberta de Catalunya.
[596] VALLÉS CAUSADA, L., "La polícia judicial en la obtención de inteligencia sobre comunicaciones electrónicas para el proceso penal", cit., p. 339.
[597] HARRIS, T., "Cómo un grupo de compañías tecnológicas controlan billones de mentes cada día".
[598] "El dilema de las redes (2020) – FilmAffinity", fecha de consulta 29 septiembre 2020, en https://www.filmaffinity.com/es/film640069.html.

En su plan de negocio, contemplan ofrecer servicios gratuitos atractivos y útiles para los usuarios, pero no porque este sea su verdadero producto en el mercado, sino porque con la masa de usuarios que utilizan sus servicios –y durante el tiempo que lo utilizan– construyen el verdadero producto, que es el de la posibilidad de anunciarse ante todo ese gran número de usuarios. Así, los verdaderos clientes de estas compañías son quienes contratan sus servicios de publicidad, lo que ha dado nueva vida al aforismo *if it is free, you are the product*, que ya apareció con ocasión de la televisión de acceso gratuito.[599]

La cuestión es que, como sucediera con los diferentes canales de televisión, las grandes prestadoras de servicios de internet deben competir entre sí para captar la mayor cantidad posible de atención de los usuarios, puesto que es un recurso naturalmente limitado en cada momento. Y, de igual modo, como la victoria en esa competición por el consumo de contenido por los usuarios es lo que determina la viabilidad financiera de esas empresas, dicha competición ha quedado completamente desnaturalizada.

En esa competición entre compañías, en la que el usuario queda relegado a una mera materia prima objeto de explotación, se han desarrollado técnicas cada vez más refinadas para mejorar "la experiencia de usuario" en sus plataformas, y conseguir así que el mayor número de usuarios posibles pase el mayor tiempo posible en el portal de sus contenidos. En persecución de ese objetivo se construyen departamentos enteros con equipos multidisciplinares destinados a maximizar la exposición de los usuarios a sus productos y, así, poder ofrecer un espacio publicitario mayor.

En nuestra opinión, esta circunstancia ayuda a poner de manifiesto dos elementos fundamentales del ciberespacio. Aun pudiendo parecer lo contrario, el ciberespacio no es un espacio "libre", en el que cada individuo pueda actuar a su antojo. Más bien al contrario, en el ciberespacio la gran mayoría de usuarios nos sometemos a la influencia de los diseños de "experiencia de usuario" y, a gran escala, a la propia estructura de cualquier servicio cibernético que, por su conveniencia, utilicemos –aunque desconozcamos los pormenores de su funcionamiento–. Hay que hacer constar que una parte del tráfico cibernauta no supone un "actuar consciente" de los usuarios, sino una manifestación de una suerte de "inercia conductual" realizada por la propia sistemática de los diseños,

[599] "Richard Serra «Television Delivers People» (1973)", fecha de consulta 10 mayo 2020, en https://www.youtube.com/watch?ab_channel=KunstSpektrum&v=LvZYwaQlJsg.

concebidos para maximizar nuestro tiempo de exposición. No somos completamente libres ni "deambulamos" como podríamos hacerlo en la realidad física; más bien somos influidos para quedarnos, movernos, o ir a un sitio y a otro. Y en este contexto de sublime manipulación, aparecen las Fuerzas y Cuerpos de Seguridad del Estado para "rastrear" las actividades de la red. No pretendemos con este breve apunte eximir al ciudadano de la responsabilidad por su conducta, aun cuando en muchas ocasiones no sea más que víctima de una carrera desnaturalizada por su atención, pero sí creemos necesario reconocer las especialidades del *ciberespacio* que, necesariamente, deben aplicarse a la hora de interpretar y extraer conclusiones sobre la información que pueda extraer la policía al rastrear la red.

B. CONSTANTE RECOLECCIÓN DE DATOS POR LAS COMPAÑÍAS TECNOLÓGICAS

Continuando con las compañías prestadoras de servicios de la sociedad de la información –y sin limitarnos en esta vez a aquellas orientadas a la publicidad–, es también necesario llamar la atención sobre la masiva recolección de datos que llevan a cabo con ocasión de la prestación de sus servicios.

El círculo, como es públicamente sabido, queda cerrado en una estructura en la que i) se ofrecen servicios de utilidad –relativa, generándose a veces la propia necesidad– de manera gratuita al consumidor, que sirven como escaparate de los clientes de la propia proveedora del servicio; ii) se recolectan los datos de los usuarios de dicho servicio, con lo que este no sólo es un escaparate, sino una herramienta permanente de adaptación de la publicidad para obtener el mejor resultado; y iii) con dichos datos, se configura un perfil del usuario y un perfil de los anuncios, obteniendo la mejor exposición a la publicidad posible.

A pesar de los cada vez más intensos esfuerzos en este sentido, los usuarios de dicho servicio no tienen más remedio que aceptar la extensiva labor de recolección de datos de que son objeto cuando utilizan los servicios de dichas compañías –a profundidades muy superiores a las que se permitirá a cualquier acción penal publica–, construyendo perfiles, detectando patrones y generando predicciones.

Se presta especial atención a las actuaciones de ciberpatrullaje de la policía, pero se considera en menor medida que, en muchos casos, dicho ciberpatrullaje ha sido

externalizado, cedido a las propias titulares de las plataformas web en las que se verifican dichas conductas.

C. INFORMES DE TRANSPARENCIA

La imposición del deber de colaboración que hemos analizado en las páginas anteriores ha traído consigo, entre sus muchas consecuencias, el nacimiento de un sentimiento de desconfianza de los usuarios finales respecto de los servicios que prestan los sujetos obligados. En particular, esta desconfianza aparece con más fuerza, vinculada también al tratamiento de datos personales y a modelos de negocio basados en la publicidad respecto de aquellos obligados que prestan servicios de la sociedad de la información.

Esta situación, que se observa de forma más acusada en la figura del consumidor, ha llevado a estos prestadores de servicios, obligados a colaborar con las autoridades, a idear instrumentos para contrarrestar la influencia negativa que tales colaboraciones podrían tener en su reputación, así como para reforzar la confianza de sus clientes en sus buenas prácticas relativas a la seguridad de la información y respeto al propio espacio virtual.

Entre estos instrumentos, queremos destacar aquí los que se han venido en denominar "informes de transparencia", que son dosieres en los que las entidades exponen, de manera sistematizada, entre otros datos, las peticiones de información y colaboración que reciben de los diferentes Estados, entre los que por supuesto se encuentra España. Todos los informes se encuentran disponibles a través de las páginas web de las propias empresas, cuentan con varios filtros para consultar la información y, con mayor o menor facilidad, permiten su descarga en formatos de tratamiento de datos. Entre otras empresas, habitualmente publican informes de transparencia las siguientes entidades: *AOL*, *Apple*, *AT&T*, *Cheezburger*, *Cloudflare*, *Comcast*, *Credo Mobile*, *CyberGhost*, *Daum Kakao*, *Deutsche Telekom*, *Dropbox*, *Facebook*, *GitHub*, *Hong Kong Transparency Report*, *Kickstarter*, *Korea Internet Transparency Report*, *LeaseWeb*, *LinkedIn*, *Lookout*, *Microsoft*, *Naver*, *Nest*, *Oath*, *Pinterest*, *reddit*, *Rogers*, *SaskTel*, *Snap*, *TekSavvy*, *TeliaSonera*, *Telstra*, *TradeMe*, *Tumblr*, *Twilio*, *Twitter*, *Uber*, *University of California, Berkeley*, *Verizon*, *Vodafone*, *Wikimedia Foundation*, *WordPress*, y *Yahoo!*

Nosotros, a modo de muestra y por su especial trascendencia para el usuario final, habida cuenta del alcance de sus servicios y cuota de ocupación de mercado, hemos considerado de interés analizar los informes de transparencia de Microsoft, Apple y Google.

Con carácter previo, no obstante, tenemos que indicar que los informes de transparencia categorizan las solicitudes en función de su naturaleza, distinguiendo, *grosso modo*, entre aquellas penales, civiles y "de emergencia". Nosotros, en aras de la brevedad hemos recopilado los datos relativos a las primeras, pero creemos que resultaría especialmente interesante estudiar las solicitudes "de emergencia", por si en ellas se incluyen los supuestos "de urgencia" previstos en los apartados tercero del artículo 588 ter, cuarto del artículo 588 *quinquies* b), y tercero y cuarto del artículo 588 *sexies* c).

En su informe de transparencia para España, Microsoft no diferencia los tipos de solicitudes de información, sino el resultado de estas solicitudes, tanto en relación a su aceptación o rechazo como al alcance de la información facilitada.

Esta decisión es interesante y útil porque permite comprobar que en todos los periodos ninguna de las solicitudes planteadas generó una entrega de datos "con contenido" por contraposición a las entregas de datos "sin contenido". Así, es posible determinar el alcance de la injerencia, que al fin y al cabo es a donde se dirige en la actualidad la sensibilidad social sobre este asunto.

Según la propia información facilitada, las entregas de datos "con contenido" se refieren a aquello que los clientes de Microsoft crean, comunican o almacenan en sus servicios, como las palabras de correos electrónicos, las fotografías o los documentos almacenados en OneDrive o cualquier otro servicio en la nube. Por el contrario, las entregas de datos "sin contenido" se refieren a la dirección de correo electrónico, el nombre, el Estado, código postal y la dirección IP del tiempo del registro. La propia Microsoft indica que exigen una autorización judicial antes de entregar cualquier contenido de ese tipo a una autoridad.

Llama la atención que ninguna de las solicitudes de colaboración supuso la entrega de datos "con contenido", la progresiva reducción del número total de solicitudes (de 927 en 2013 a 409 en 2018) y el también paulativo incremento en el porcentaje de solicitudes que resultaron rechazadas (del 0,5% en 2013 al 19,07% en 2018).

El informe de transparencia de Apple también se encuentra disponible a través de la página web corporativa de la empresa, aunque es accesible directamente desde cualquier buscador.

Apple diferencia cuatro tipos de solicitudes de información: “device”, “financial identifier”, “account” y “emergency”. En la categoría “device” encuadran las solicitudes recibidas sobre datos que permitan identificar dispositivos, como el número de serie o el número IMEI. En la categoría “financial identifier” encuadran las solicitudes recibidas del gobierno sobre datos financieros, como una tarjeta de crédito o una tarjeta regalo.

En la categoría “account” encuadran las solicitudes recibidas del gobierno sobre datos que permitan la identificación de cuentas, como el ID de Apple o la dirección de correo electrónico, así como datos que constituyan contenido creados por los clientes. Finalmente, en la categoría de “emergency” engloban todas aquellas solicitudes recibidas del gobierno con carácter urgente. Nosotros, como ya hemos indicado, hemos dejado fuera las solicitudes pertenecientes a las categorías “financial identifier” y “emergency”.

Aquí, las diferentes categorías en las que se dividen las solicitudes hacen difícil alcanzar conclusiones homogéneas que sean comparables con el informe de transparencia de Microsoft, pero, en general, podemos destacar lo siguiente: para las solicitudes “device”, el progresivo incremento del número de ellas (308 en 2013 y 1736 en 2018) y del porcentaje de las mismas en que se entregó información (66% en 2013 y 78% en 2018).

En cuanto a las solicitudes “account”, sobresale la disminución del número de ellas (102 en 2013 y 48 en 2018), pero acompañado de un incremento del porcentaje en el que se entregó información (22% en 2013 y 50%) en 2018. Se mantienen en cero las solicitudes en las que se entregó “información de contenido”, de forma similar a cuanto suceda en los informes de Microsoft.

Finalmente, el informe de transparencia de Google también se encuentra disponible a través de la página web corporativa de la empresa, aunque es accesible directamente desde cualquier buscador. Google facilita una única tabla con los siguientes datos, y la descarga no es fácil:

En el caso del informe de transparencia de Google, encontramos que quizás es el que menos detalle de investigación permite: únicamente comienza a diferenciar categorías de solicitudes a partir del segundo semestre de 2014, aunque la empresa venía recogiendo datos desde 2009.

Además, no están categorizados de igual modo, con lo que se pierde cierta utilidad y, aparte, no distingue especialmente en función del alcance de la solicitud de

colaboración (con la excepción de las solicitudes de preservación que no han generado "datos"), sin mayor precisión en el informe. En general, no obstante, podemos decir que los números de las solicitudes han venido ascendiendo progresivamente.

CAPÍTULO VI: COOPERACIÓN POLICIAL INTERNACIONAL

Como hemos tenido ocasión de destacar en apartados anteriores, uno de los elementos característicos de la ciberdelincuencia es el señalado componente transfronterizo que se encuentra en los delitos cometidos. Esta característica es, a su vez, consecuencia directa de la ubicuidad del medio en el que se verifican tales conductas delictivas: el ciberespacio.

Dado que uno de los elementos definidores de la ciberdelincuencia es su carácter transfronterizo, resulta que la obtención de evidencias de conductas delictivas cometidas en el ciberespacio no puede encontrarse limitada a un territorio nacional, Así, ante lo acusado de dicha transnacionalidad, las autoridades encargadas de investigar y perseguir las conductas ciberdelictivas se encuentran con que no pueden limitar la búsqueda de evidencias en el ámbito territorial de un Estado concreto[600], sino que, para que las labores de persecución e investigación mantengan su eficacia, se encuentran en la necesidad de expandir el alcance de dicha búsqueda al espacio de otros Estados en los que se hallan algunos de los elementos, instrumentos o personas que estén relacionados con el hecho investigado, debiendo así acudir a mecanismos de cooperación internacional.

Ocurre, por tanto, que la mayoría de las investigaciones penales en este ámbito de la ciberdelincuencia tendrán que ser transfronterizas, en el sentido de que el proceso penal se estará desarrollando en un Estado, pero se precisa, para su avance, la realización de alguna diligencia de investigación en otro, pues es en este último donde se encuentran los objetos o las personas sobre los que deben proyectarse la pesquisa[601].

En ese sentido, esta nota de la transnacionalidad, ha obligado a la comunidad internacional a establecer mecanismos de cooperación y colaboración nuevos, así como a reforzar los ya existentes, al tratarse de una herramienta fundamental en la lucha contra el imparable avance y expansión de los ciberdelitos. En ese sentido, la cooperación

---

[600] Al menos, no si se pretende que la investigación resulte eficaz para los fines de prevención e investigación del delito.

[601] GASCÓN INCHAUSTI, F., "La eficacia de las pruebas penales obtenidas en el extranjero al amparo del régimen convencional: apogeo y declive del principio de no indagación", en *Orden europea de investigación y prueba transfronteriza en la Unión Europea, 2019, pp. 31–63*, Tirant lo Blanch, 2019, p. 32, en https://dialnet.unirioja.es/servlet/articulo?codigo=6949793, fecha de consulta 27 julio 2021..

internacional entre las diferentes autoridades nacionales encargadas de la investigación de tales ilícitos ha sido abordada como una estrategia imprescindible y una herramienta de imposible renuncia, obligando a las organizaciones, órganos y organismos internacionales y supranacionales a reforzar y redefinir los mecanismos de cooperación.

En nuestro ordenamiento, el artículo 276 LOPJ establece que *"Las peticiones de cooperación internacional se tramitarán de conformidad con lo previsto en los tratados internacionales, las normas de la Unión Europea y las leyes españolas que resulten de aplicación."* En consecuencia, la base aplicable está constituida por los convenios internacionales de los que España sea parte.

Tales instrumentos jurídicos, a su vez, pueden ser catalogados en tres grupos diferenciados, dependiendo del ámbito territorial de cooperación. De ese modo, distinguimos un ámbito internacional propiamente dicho, representado por los instrumentos surgidos al amparo de la Organización de las Naciones Unidas (en adelante, ONU) –tratados, acuerdos, convenios y pactos celebrados en su seno, así como las resoluciones emitidas por sus organismos– y que en el contexto penal permitirían hablar de una verdadera cooperación internacional; a continuación, si descendemos al ámbito europeo, nos encontramos con un nivel de cooperación regional compuesto por las actuaciones desarrolladas por el Consejo de Europa y, finalmente y como tercer ámbito, la política de cooperación judicial penal y policial –atendiendo a la materia que nos ocupa– definida en el Tratado de la Unión Europea (en adelante, TUE) y desarrollada en el Tratado de Funcionamiento de la Unión Europea (en adelante, TFUE).

1. COOPERACIÓN POLICIAL EN EL ÁMBITO DE LA ONU

A. PRINCIPALES RESOLUCIONES

La ONU, en su ejercicio de la responsabilidad asumida en materia de prevención del delito y justicia penal, ha emitido las siguientes resoluciones:

Resolución 46/152, de 18 de diciembre de 1991, en la que se establece el compromiso, por parte de los Estados miembro, de que los congresos de las Naciones Unidas sobre prevención del delito y justicia penal se celebraran cada cinco años con el objetivo de servir de foro, entre otras cosas, para el intercambio de ideas entre Estados, organizaciones intergubernamentales, organizaciones no gubernamentales y expertos individuales de diversas profesiones y disciplinas. Además, destaca la importancia del intercambio de

experiencias en materia de investigación, derecho, formulación de políticas y determinación de nuevas tendencias en materia de prevención del delito y justicia penal.

Resolución 57/270 B, de 23 de junio de 2003, relativa a la aplicación y el seguimiento integrados y coordinados de las decisiones adoptadas en las grandes conferencias y cumbres de las Naciones Unidas en las esferas económica y social, en la que se destacó que todos los países debían promover políticas coherentes y compatibles con los compromisos contraídos en las grandes conferencias y cumbres de las Naciones Unidas y puso de relieve que el sistema de las Naciones Unidas tenía la importante responsabilidad de ayudar a los gobiernos a seguir participando plenamente en el seguimiento y la aplicación de los acuerdos y compromisos alcanzados en esas conferencias y cumbres e invitó a sus órganos intergubernamentales a que siguieran promoviendo la aplicación de las decisiones adoptadas en ellas.

Recordando además su resolución 64/180, de 18 de diciembre de 2009, en que exhortó al 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal a que formulara propuestas concretas de seguimiento y medidas ulteriores, prestando particular atención a las disposiciones prácticas relacionadas con la aplicación efectiva de los instrumentos jurídicos internacionales relativos a la delincuencia organizada transnacional, el terrorismo y la corrupción y a las actividades conexas de asistencia técnica, y solicitó a la Comisión de Prevención del Delito y Justicia Penal que, en su 19º período de sesiones, concediera máxima prioridad al examen de las conclusiones y recomendaciones del 12º Congreso, con miras a recomendar, por conducto del Consejo Económico y Social, medidas apropiadas de seguimiento a la Asamblea General en su sexagésimo quinto período de sesiones.

Declaración del Milenio, aprobada por los Jefes de Estado y de Gobierno en la Cumbre del Milenio el 8 de septiembre de 2001, en la que resolvieron, entre otras cosas, consolidar el respeto del Estado de Derecho en los asuntos internacionales y nacionales, adoptar medidas concertadas contra el terrorismo internacional y adherirse cuanto antes a todos los instrumentos internacionales pertinentes.

Resolución 65/230, de 21 de diciembre de 2010, en la que hizo suya la Declaración de El Salvador sobre Estrategias Amplias ante Problemas Globales: los Sistemas de Prevención del Delito y Justicia Penal y su Desarrollo en un Mundo en Evolución. De dicha declaración es necesario señalar el parágrafo 39, en el que las partes intervinientes

declararon que “el desarrollo de las tecnologías de la información y las comunicaciones y el uso cada vez más frecuente de Internet crean nuevas oportunidades para los delincuentes y facilitan la proliferación de la delincuencia”.

También es necesario mencionar las Resoluciones 22/7 y 22/8 de la Comisión de Prevención del Delito y Justicia Penal, por las que acordaba tomar conocimiento del encuentro del Grupo de Expertos, celebrado en Viena entre los días 25 y 28 de febrero de 2013 para realizar un estudio comprensivo de la figura del cibercrimen y solicitaba a la Oficina de las Naciones Unidas contra la Droga y el Delito que elaborase un programa global sobre la ciberdelincuencia reforzando la asistencia técnica entre los Estados parte para contrarrestar el cibercrimen y sirviera como repositorio internacional en materia de cibercrimen, a fin de facilitar la toma de conocimiento por parte de los demás Estados.

Seguidamente, debemos también hacer constar a la Resolución 73/187, de la Asamblea General, por la que se solicitaba al Secretario General que recabase las opiniones de los Estados Miembros sobre los problemas en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos y que presentase un informe basado en esas opiniones para examinarlo en su septuagésimo cuarto período de sesiones. Fruto de dicha solicitud fue el Informe del Secretario General, titulado “Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos”, conteniendo información sobre las opiniones de los Estados parte en materia de cibercriminalidad.

Finalmente, es necesario señalar la Resolución 74/247, de la Asamblea General, 27 de diciembre de 2019, en la que se decidía establecer un comité *ad hoc,* denominado “Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos”. Por Resolución 75/282, de 26 de mayo de 2021, de la Asamblea General , quedó definitivamente constituido el referido comité , estando previsto que se celebren varias sesiones durante los años 2021, 2022, 2023 y 2024, que deberán finalizar con un borrador del acuerdo definitivo [602].

[602] Disponible en https://undocs.org/en/A/AC.291/2, fecha de consulta 7 de mayo de 2022.

B. OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO Y COMISIÓN DE PREVENCIÓN DEL DELITO Y JUSTICIA PENAL

La Oficina de las Naciones Unidas contra la Droga y el Delito y Comisión de Prevención del Delito y Justicia Penal constituye el órgano fundamental de la ONU en la elaboración e implementación de políticas contra el cibercrimen.

En cumplimiento de la ya citada Resolución 65/230, de 21 de diciembre, de la Asamblea General, y de las también citadas resoluciones 22/7 y 22/8, de la Comisión de Prevención del Delito y Justicia Penal, ha elaborado un Programa Global contra el Cibercrimen, sufragado exclusivamente por Australia, Canadá, Japón, Noruega, Reino Unido y Estados Unidos, que persigue auxiliar a los Estados parte en su lucha contra dicha modalidad de criminalidad.[603]

Facilita herramientas, como un repositorio sobre cibercrimen, en el que se aglutinan buenas prácticas de los diferentes Estados parte, legislaciones vigentes y resultados judiciales[604]. Con ello, se persigue facilitar a las autoridades policiales de los diferentes Estados la persecución del cibercrimen.

Dentro de la estructura de la Oficina de las Naciones Unidas contra la Droga y el Delito es necesario hacer referencia a la Comisión de Prevención del Delito y Justicia Penal (CCPCJ), que fue creada por el Consejo Económico y Social (ECOSOC) mediante la resolución 1992/1, a petición de la Asamblea General (GA) en su resolución 46/152, en calidad de comisión orgánica.

Este último organismo actúa como el principal órgano normativo de las Naciones Unidas en cuestiones de prevención del delito y justicia penal. Está formada por más de 40 Estados Miembros elegidos por el ECOSOC, y está presidida por una Mesa, que incluye un miembro de cada grupo regional. Su función principal consiste en desarrollar

[603] Disponible en https://www.unodc.org/documents/organized–crime/cybercrime/Cybercrime_Study_Spanish.pdf, fecha de consulta 7 de mayo de 2022.

[604] https://sherloc.unodc.org/cld/v3/sherloc/index.jspx?tmpl=cybrepo, fecha de consulta 7 de mayo de 2022.

políticas en materia de criminalidad a través de resoluciones y decisiones, reglas y normas, así como en debates temáticos y reuniones de grupos de expertos.[605]

En su resolución 1992/22 el ECOSOC encomendó a la Comisión mandatos y prioridades, que incluyen la mejora de la acción internacional para combatir la delincuencia nacional y transnacional, así como la mejora de la eficiencia y la imparcialidad de los sistemas de administración de justicia penal. La CCPCJ también ofrece a los Estados miembros un foro para el intercambio de conocimientos, experiencias e información para el desarrollo de estrategias nacionales e internacionales, y para la definición de prioridades en la lucha contra la delincuencia.

La CCPCJ se reúne anualmente en sesiones regulares y en reuniones entre sesiones. Al final de cada año, la CCPCJ celebra la continuación del período de sesiones para tratar asuntos presupuestarios y administrativos como órgano rector del Programa de las Naciones Unidas en materia de prevención del delito y justicia penal.

En 2006, la Asamblea General adoptó la resolución 61/252, que amplió los mandatos de la CCPCJ a fin de que pudiera funcionar como órgano rector de la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD) y que aprobara el presupuesto del Fondo de las Naciones Unidas para la Prevención del Delito y la Justicia Penal.

Por último, no puede dejarse de hacer constancia a los Congresos de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, cuyo órgano preparatorio es también la CCJPCJ y cuyas declaraciones se transmiten mediante la CCPCJ y el ECOSOC a la Asamblea General para su aprobación.

C. ORGANIZACIÓN INTERNACIONAL DE POLICÍA CRIMINAL (INTERPOL)

En el ámbito internacional es necesario referirnos la Organización Internacional de Policía Criminal, más conocida como INTERPOL. Esta organización agrupa a fuerzas policiales de 192 países convirtiéndose así en la mayor en la mayor organización policial internacional global cuyo objetivo es posibilitar la cooperación policial internacional con independencia de que existan relaciones diplomáticas entre los diferentes Estados. Sus fines, limitados por los ordenamientos jurídicos y siempre velando por el respeto a la

[605] Disponible en https://www.unodc.org/unodc/es/commissions/CCPCJ/index.html, fecha de consulta 7 de mayo de 2022.

Declaración Universal de Derechos Humanos, son conseguir y desarrollar de la forma más amplia la asistencia recíproca de las unidades de policía criminal y establecer todas las instituciones que puedan contribuir a la prevención y represión de las infracciones de derecho comunitario.

La organización fue creada en 1923 con la denominación de Comisión Internacional de Policía Criminal, con sede en Viena. Su secretaría General se encuentra en Lyon y dispone de siete oficinas regionales repartidas por todo el mundo con sedes principales en Nueva York y Bruselas para su representación ante la ONU y la UE, y cada país miembro tiene también una oficina central nacional. En su lucha contra la ciberdelincuencia, cuenta con las siguientes herramientas:

- Centro de intercambio de información sobre la ciberdelincuencia como punto único de recogida de información vinculada a la ciberdelincuencia a escala mundial. Incluye un conducto de recepción, análisis y almacenamiento protegido de ese tipo de información, además de elaborar documentos con información policial y difundirlos entre los países miembros interesados. Igualmente, ayuda a los países miembros a comprobar las nuevas solicitudes, la existencia de nueva información y en la ejecución de operaciones policiales en tiempo real.

- Red permanente de contactos especializados entre las centrales de cada estado miembro. Tiene como objetivo el intercambio de información policial especializada de manera ágil, haciendo posible la colaboración internacional.

- Grupos de trabajo regionales destinados a analizar y valorar las tendencias ciberdelictivas de cada territorio, formular planes de actuación y coordinar operaciones transnacionales. Existen grupos de trabajo en todos los continentes y realizan reuniones anuales para elaborar planes de actuación.

- Unidades de apoyo a las investigaciones sobre delincuencia digital, que, mediante la investigación transaccional, propician el intercambio de información, ofreciendo asesoramiento y orientación a los cuerpos especializados de los países miembros.

Además, debemos de añadir a los anteriores instrumentos el Complejo Mundial de INTERPOL para la Innovación, que desarrolla el programa mundial de INTER-POL sobre ciberdelincuencia.

Según se define en el artículo 5 de su Constitución, la Interpol se compone de la siguiente estructura:

- Asamblea General: Es el supremo órgano de gobierno, con reunión anual, pudiendo reunirse con carácter extraordinario a petición del Comité ejecutivo o de la mayoría de los miembros. Se compone de los delegados designados por cada país miembro. La asamblea toma todas las decisiones relacionadas con la política, los recursos, los métodos de trabajo, las finanzas, las actividades y los programas. También elige a la Organización del Comité Ejecutivo. En términos generales, la Asamblea toma decisiones por mayoría simple, en forma de resoluciones, salvo que el Estatuto requiera expresamente mayoría de dos tercios. Cada país miembro tiene un solo voto representado.

- Comité ejecutivo: Es el órgano deliberativo. Se reúne tres veces al año, generalmente en marzo, julio e inmediatamente antes de la Asamblea General. De conformidad con el artículo 15 de la Constitución de la Interpol, el Comité Ejecutivo tiene 13 miembros: el presidente, 3 vicepresidentes y 9 delegados. Estos miembros son elegidos por la Asamblea General y deben pertenecer a distintos países, además, el presidente y los 3 vicepresidentes deben proceder de diferentes continentes. Su función, de conformidad con el artículo 22 de la Constitución, es la de supervisar el cumplimiento de las decisiones de la Asamblea General, preparar la agenda para las sesiones de la Asamblea General, presentar a la Asamblea General todo programa o proyecto de trabajo que considere útiles y supervisar la administración y la labor del Secretario General.

- Secretaría General: Ubicado en Lyon, Francia. La Secretaría General funciona las 24 horas del día, 365 días al año y está dirigida por el Secretario General. Compuesta por funcionarios de más de 80 países, quienes trabajan en cualquiera de los cuatro idiomas oficiales: árabe, inglés, francés y español. La Secretaría cuenta con seis oficinas regionales en Argentina, Costa de Marfil, El Salvador, Kenia, Tailandia y Zimbabue y una oficina de enlace en las Naciones Unidas en Nueva York. Es elegida por la Asamblea General por un período de 5 años; para el cumplimiento de sus funciones se estructura en 4 sub–divisiones: asamblea general, asuntos criminales, documentación general y estudios.

- Apoyo técnico: Cuyas funciones son ejecutar los acuerdos de la Asamblea General y el Comité Ejecutivo, actuar como centro internacional de lucha contra la delincuencia, ejercer de entro técnico de información de las oficinas nacionales y organizar y

ejecutar los trabajos de secretaría en las reuniones de la asamblea general y del Comité Ejecutivo.

- Oficinas Centrales nacionales: Cada uno de los países miembros de Interpol mantiene una Oficina Central Nacional (OCN), integrada por funcionarios encargados de hacer cumplir la legislación nacional. El papel de las mismas es participar en todas las actividades de la Interpol y la prestación constante de cooperación de forma activa y compatible con la legislación interna de los estados miembro, con el fin de que Interpol pueda lograr sus objetivos. La OCN es típicamente una división de un país miembro de la policía nacional, agencia de investigación o servicio o se encuentra bajo la jurisdicción del ministerio o departamento encargado de la seguridad pública o la justicia. El jefe de la OCN es normalmente uno de los funcionarios de más alto rango encargados de hacer cumplir la ley en el país. Dependiendo del tamaño del país, la OCN pueden tener sólo dos o tres funcionarios responsables de todas las actividades relacionadas con la Interpol o de varias decenas de oficiales.

- Divisiones regionales: Para prestar servicios de manera eficaz a las OCN, la Interpol y los grupos de países miembros trabajan en cinco regiones diferentes, África, América, Asia y Pacífico Sur, Europa, y Oriente Medio y Norte de África. Esto permite que las OCN coordinen las actividades operacionales regionales en el contexto de las prioridades locales y planes de acción, para compartir las mejores prácticas e identificar las soluciones a sus necesidades de aplicación de la ley. Cada región cuenta con el apoyo de un subdirector en la Secretaría General.

2. COOPERACIÓN POLICIAL EN EL ÁMBITO DEL CONSEJO DE EUROPA

Analizada la cooperación policial desarrollada al amparo de la Organización de Naciones Unidas, corresponde dedicar este capítulo a explorar la figura de la cooperación policial desplegada bajo el paraguas del Consejo de Europa, que ordena una cooperación regional europea, por incluir a Estados que no forman parte de la Unión Europea pero que sí se encuentran incluidos o íntimamente vinculados con el continente europeo.

A este respecto, el instrumento fundamental y principal es el informalmente denominado "Convenio de Budapest"[606], pero del que debemos destacar algunos antecedentes.

A. ANTECEDENTES AL CONVENIO DE BUDAPEST

La realidad es que, como se encargó de destacar la doctrina[607], el Convenio de Budapest fue el primer instrumento internacional existente hasta la fecha en la materia a la que se refería. A pesar de ello y de la inexistencia de antecedentes normativos directos, es necesario hacer referencia, al menos, a los siguientes elementos, que entendemos conforman parte de la perspectiva histórica previa al Convenio en cuestión.

Por un lado, debemos destacar el Convenio europeo de asistencia judicial en materia penal[608], que ha constituido y constituye una pieza clave sobre la que se ha construido la práctica de la cooperación regional en Europa –al menos, hasta la aparición de instrumentos adicionales en el ámbito de la Unión Europea, como veremos en apartados posteriores–. Este Convenio ha sido sustituido en parte por la Directiva 2014/41/CE (art. 34 Directiva 2014/41/CE) para todos los Estados miembros, excepto Dinamarca e Irlanda donde sigue siendo aplicable. Se mantiene, además, en vigor para las medidas de investigación expresamente excluidas de la OEI y peticiones de auxilio judicial internacional, que no sean medidas de investigación.

Por otro lado, también es necesario recordar el Convenio europeo sobre transmisión de procedimientos en materia penal[609]. Se trata de una norma de fundamental importancia porque permite a los Estados parte solicitar a otro que sustancie un procedimiento en su nombre contra el responsable de un delito, no pudiendo negarse el Estado peticionario salvo que se trate de crímenes políticos o basados en raza, religión o nacionalidad.

---

[606] Convention on Cybercrime (ETS No. 185), disponible en https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185, fecha de consulta 7 de mayo de 2022.
[607] DÍAZ GÓMEZ, A., "El delito informático, su problemática y la cooperación internacional como paradigma de su solución", cit., p. 195.
[608] European Convention on Mutual Assistance in Criminal Matters (ETS No. 030), disponible en https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=030, fecha de consulta 7 de mayo de 2022. Ratificado por España mediante Instrumento de Ratificación de 14 de julio de 1982 del Convenio Europeo de Asistencia Judicial en Materia Penal, hecho en Estrasburgo el 20 de abril de 1959, BOE núm. 223, de 17 de septiembre de 1982, páginas 25166 a 25174.
[609] European Convention on the Transfer of Proceedings in Criminal Matters (ETS No. 073), disponible en https://rm.coe.int/0900001680072d42, fecha de consulta 7 de mayo de 2022. Ratificado por España mediante Instrumento de Ratificación del Convenio Europeo sobre la Transmisión de Procedimiento en Materia Penal, hecho en Estrasburgo el 15 de mayo de 1972, BOE núm. 270, de 10 de noviembre de 1988, páginas 32060 a 32065.

Además, establece que todo acto que tenga por objeto la instrucción de procedimiento, efectuado en el Estado requirente, de conformidad con las leyes y reglamentos vigentes en dicho Estado, tendrá en el Estado requerido la misma validez que hubiera tenido ese acto efectuado por las autoridades de este Estado, sin que esta asimilación pueda tener como efecto conferir a dicho acto una fuerza probatoria superior a la que tiene en el Estado requirente[610].

Asimismo, también resulta interesante hacer referencia a la reunión de 1983[611], en la que un grupo de expertos recomienda a la Organización para la Cooperación y Desarrollo Económico (OCDE) la necesidad de afrontar una armonización en el ámbito de la delincuencia informática, lo que finalmente se materializa en un informe tres años después[612].

Debemos señalar que se trataba de una materia de especial dificultad y complejidad, prueba de ello era que llegasen a existir hasta treinta versiones del proyecto, y que el mismo no fue publicado hasta el 27 de abril de 2002, fecha en la que ve la luz el "Proyecto de Convención sobre el Delito Cibernético", que resultó finalmente aprobado el 8 de noviembre de 2001 por el Comité de Ministros y abierto a la firma el día 23 del mismo mes de noviembre.

B. ESTRUCTURA DEL CONVENIO DE BUDAPEST

El Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, en vigor para España el 1 de octubre de 2010, es el primer tratado internacional sobre delitos cometidos a través de internet, que trata en particular de las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de la seguridad en redes.

En cuanto a la estructura del Convenio sobre la Cibercriminalidad, consta de 48 artículos y un preámbulo inicial, organizados en cuatro capítulos con secciones y títulos. El primer capítulo solamente contiene un precepto, relativo a las definiciones y términos empleados en el texto del Convenio. El capítulo segundo, denominado "Medidas que

---

610 GASCÓN INCHAUSTI, F., "La eficacia de las pruebas penales obtenidas en el extranjero al amparo del régimen convencional", cit., p. 36.

611 BERNAL, A. R., "España: Los Cibercrimenes en el Espacio de Libertad, Seguridad y Justicia", *AR: Revista de Derecho Informático*, 103, 2007, Alfa-Redi, p. 13.

612 DÍAZ GÓMEZ, A., "El delito informático, su problemática y la cooperación internacional como paradigma de su solución", cit., p. 196.

deberán adoptarse a nivel nacional", comprende elementos tanto de derecho material como de derecho procesal, como podremos comprobar. El capítulo tercero se refiere a la figura de la cooperación internacional, abarcando cuestiones como como la extradición, la asistencia entre Estados, la información, el intercambio de datos y el establecimiento de una red 24/7. El último capítulo contiene las disposiciones finales propias de un Tratado internacional: adhesión, entrada en vigor, aplicación territorial, efectos, régimen de reservas, denuncias, notificaciones, etc.

Además de dicha estructura, del contenido de los artículos resulta que su contenido se puede dividir, conceptualmente, en dos partes diferenciadas: Derecho Penal Internacional, constituido por las disposiciones 2 a 13, y Derecho Procesal Penal Internacional, en los artículos 14 a 35. A este respecto, merece la pena señalar que la parte relativa al Derecho Procesal contiene prácticamente el doble de artículos que la parte dedicada al derecho material.

Los principales objetivos de del Convenio eran armonizar los elementos nacionales de derecho penal material en materia de delitos relacionados con el uso de la informática, y establecer un régimen rápido y eficaz de la cooperación internacional. Con este instrumento, se establecieron unas bases generales que debían acogerse desde el punto de vista normativo por los diferentes Estados que lo suscribieron[613].

También se ha dicho que el Convenio en cuestión perseguía básicamente tres objetivos en torno a los cuales se estructura, a saber: armonizar el Derecho Penal material, establecer medidas procesales o cautelares adaptadas al medio digital y poner en funcionamiento un régimen rápido y eficaz de cooperación internacional[614].

Por último, y antes de analizar el contenido material del Convenio, queremos hacer referencia también al preámbulo del Convenio, en el que se reconoce la necesidad de "aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional". También defiende la

---

[613] CUADRADO SALINAS, C. C., "La obtención de pruebas electrónicas transfronteriza: Nuevos retos y nuevas consideraciones desde la perspectiva de la Unión Europea", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, pp. 517–534*, Ediciones Jurídicas Castillo de Luna, 2020, p. 519, en https://dialnet.unirioja.es/servlet/articulo?codigo=7870321, fecha de consulta 25 noviembre 2021.

[614] LERMA, E. M.; PUERTA, M. J. R., "Traducción y breve comentario del convenio sobre cibercriminalidad", *Revista de derecho y proceso penal*, 7, 2002, Aranzadi Thomson Reuters, p. 169.

intensificación de la cooperación internacional para lograr "una lucha efectiva contra la ciberdelincuencia […] en materia penal reforzada, rápida y operativa". Asimismo, subraya que el Convenio pretende completar otros Convenios en materia de cooperación en materia penal con la finalidad de dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos.

C. MEDIDAS EN MATERIA DE DERECHO PENAL INTERNACIONAL EN EL CONVENIO DE BUDAPEST

Analizamos ahora la primera parte del Convenio de Budapest, compuesta por los artículos 2 a 13 del mismo y que contiene medidas de orden sustantivo.

Así, y como señala la doctrina[615], en dichos artículos introduce obligaciones para que los Estados tipifiquen determinadas conductas[616] relacionadas con el ámbito de la ciberdelincuencia. Esto supone un gran avance hacia la armonización del derecho sustantivo de los Estados parte, elemento fundamental para una lucha transnacional eficaz y eficiente contra la ciberdelincuencia, al permitir aunar los criterios punitivos en torno a dichas conductas.

Asimismo, merece la pena destacar que, precisamente con el ánimo de garantizar la posibilidad de cumplimiento de dichas obligaciones de tipificación, el Convenio mantiene abiertas las diferentes posibilidades de castigar tales conductas, permitiendo así la aplicación flexible de los tipos por cada Estado parte y garantizando, de esa manera, un mínimo de unificación entre los ordenamientos jurídicos nacionales. Se aprecia así la voluntad de conseguir un tratamiento global coherente de la ciberdelincuencia, aun cuando para conseguir dicho fin sea necesario asumir cierta complejidad en la aplicación de los tipos previstos en el Convenio por cada Estado parte.

---

[615] DÍAZ GÓMEZ, A., "El delito informático, su problemática y la cooperación internacional como paradigma de su solución", cit., p. 198.

[616] Acceso ilícito a sistemas informáticos, interceptaciones ilícitas de comunicaciones, interferencia ilegítima que dañe, borre, deteriore, altere o suprima datos informáticos o que afecten a sistemas informáticos de manera que produzcan dicho resultado, abuso de dispositivos, falsificaciones, fraude, pornografía infantil e infracciones de propiedad intelectual.

A pesar de lo anterior, se ha llamado la atención sobre la falta de previsión de la problemática de la explotación sexual de la infancia en internet[617], así como la incriminación de actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos -si bien esta última carencia fue enmendada al poco tiempo, mediante el Protocolo Adicional relativo a la incriminación de actos de naturaleza racista y xenófoba cometidos a través de los sistemas informáticos de Estrasburgo, abierto a la firma el 28 de enero de 2003-.

Al respecto del contenido de dichos artículos, se ha criticado[618] la incriminación de la posesión de programas o datos, pues no siempre se infiere de la posesión una finalidad estrictamente delictiva. Se señalan los artículos 6 y 9, que expresamente prevén la punición de la mera tenencia de códigos de acceso o datos informáticos para la comisión de delitos informáticos, o la mera posesión de datos relativos a la pornografía infantil[619]. Es cierto que el Convenio permitía a los Estados establecer reservas en esos puntos, pero la realidad es que la tipificación de la conducta tal y como está planteada en el texto podría suponer una desmesurada expansión del Derecho Penal hacia órbitas que sobrepasan lo estrictamente necesario[620].

En relación con la responsabilidad de las personas jurídicas, también fue criticado el hecho de que el artículo 12 del Convenio únicamente se refiriese a la responsabilidad de estas, sin referirse de manera directa a la posible responsabilidad de las personas físicas que estén al cargo de la entidad en cuestión. Por este motivo, se ha dicho que la estructura definida en el Convenio constituye un modelo formalista que suscita dudas sobre la necesidad de instaurar un único modelo de imputación de la responsabilidad de la persona jurídica[621].

---

[617] PAVÓN PÉREZ, J. A., "La labor del Consejo en Europa en la lucha contra la cibercriminalidad: El protocolo adicional al convenio nº 185 sobre cibercriminalidad relativo a la incriminación de actos de naturaleza racista y xenófobos cometidos a través de los sistemas informáticos", *Anuario de la Facultad de Derecho. Universidad de Extremadura*, 21, 2003, Servicio de Publicaciones, p. 203.

[618] *Ibid.*

[619] ESQUINAS VALVERDE, P., "El tipo de mera posesión de pornografía infantil en el código penal español (art. 189.2): razones para su destipificación", *Revista de Derecho Penal y Criminología*, 18, 2006, Facultad de Derecho, p. 225. Facultad de Derecho de dónde? Habitualmente no se cita la editorial de las revistas, pero si lo tenéis así en toda la tesis, no he dicho nada.

[620] DÍAZ GÓMEZ, A., "El delito informático, su problemática y la cooperación internacional como paradigma de su solución", cit., p. 200.

[621] SILVA SÁNCHEZ, J. M., "La responsabilidad penal de las personas jurídicas en el convenio del consejo de Europa sobre cibercriminalidad", *Cuadernos de derecho judicial*, 9, 2002, Consejo General del Poder Judicial, p. 133.

D. MEDIDAS EN MATERIA DE DERECHO PROCESAL PENAL INTERNACIONAL EN EL CONVENIO DE BUDAPEST

Expuesto lo anterior, corresponde ahora analizar los preceptos del Convenio relativos a los aspectos procesales y, en su caso, procedimentales, materia a la que se refieren los artículos 14 y siguientes del Convenio.

Los artículos 14 y 15 contienen disposiciones comunes relativas a dichos aspectos procesales, pudiendo destacarse la obligación de los Estados parte de adoptar las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en el Convenio (artículo 14.1), así como el deber de asegurarse de que el establecimiento, la ejecución y la aplicación de los poderes y procedimientos previstos en la presente sección están sujetas a las condiciones y salvaguardas previstas en su derecho interno, que deben garantizar una protección adecuada de los derechos humanos y de las libertades.

Los artículos 16 a 21 se refieren a la preservación de datos informáticos, medidas relativas a la agilización de los trámites y la conservación de información fundamental en turno al ilícito. En concreto, se prevé la conservación rápida cuando existan razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación (artículo 16), la revelación rápida a la autoridad competente (artículo 17), la orden a personas o ISP de comunicar datos relevantes (artículo 18), disposiciones relativas a la agilización del registro y confiscación de datos (artículo 19), obtención de datos sobre el tráfico (artículo 20) y la interceptación del contenido de las comunicaciones para los delitos graves (artículo 21). La doctrina[622] destaca cómo se apuesta primordialmente por la rapidez, creando métodos tendentes a la recolección de evidencias para la persecución de los delitos informáticos, algo que es plausible desde el punto de vista de la eficacia policial, pero que puede entrar en conflicto con los derechos fundamentales que resulten de aplicación.

El artículo 22 del convenio se refiere a los problemas de la jurisdicción, de forma que sirve para unificar criterios, al menos parcialmente, al afirmar el principio de territorialidad y el de personalidad para todos los Estados.

---

[622] DÍAZ GÓMEZ, A., "El delito informático, su problemática y la cooperación internacional como paradigma de su solución", cit., p. 201.

El artículo 24 CB se refiere a la extradición, remitiendo en primer lugar a otros Tratados de extradición existentes previamente entre las partes, y supletoriamente, aplicando el Convenio de Cibercriminalidad en lo concerniente a los delitos determinados en la primera decena de artículos.

Los artículos 25 a 27 establecen las bases para la cooperación y ayuda entre los Estados (asistencia mutua), así como intercambio de información y fijación de autoridades de contacto, para llevar a cabo las investigaciones y la recolección de pruebas. A este respecto, hay que destacar que el artículo 35 ordena a cada parte designar un punto de contacto disponible las veinticuatro horas del día, siete días a la semana, con objeto de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o de los procedimientos relativos a los delitos vinculados con sistemas y datos informáticos, o para la obtención de pruebas electrónicas del delito.

Por su parte, los artículos 29 a 34 se refieren a los datos informáticos desde la perspectiva de la cooperación internacional. Se prevén solicitudes de conservación rápida de datos (artículo 29), solicitudes de revelación rápida de datos (artículo 30 CB.), solicitudes de obtención o confiscación (artículo 31 CB.), acceso libre a datos de fuente abierta (artículo 32 CB.) y asistencia mutua para obtención de datos sobre el tráfico e interceptación de comunicaciones (artículos 32 y 33 CB).

Por último, las disposiciones finales del tratado, artículos 36 a 38, contienen cláusulas generales propias de los Tratados internacionales elaborados en el seno del Consejo de Europa: adhesión, entrada en vigor, aplicación territorial, efectos, régimen de reservas, denuncias, notificaciones. Es de señalar que el artículo 46 señala la importancia del intercambio de información sobre novedades significativas de carácter jurídico, político o tecnológico relacionadas con la ciberdelincuencia y con la obtención de pruebas en formato electrónico entre los Estados.

E. APUNTES GENERALES SOBRE LOS DERECHOS FUNDAMENTALES

En general, del estudio del Convenio se evidencia el esfuerzo y el énfasis dedicado a la regulación de los relacionados con los datos informáticos, la necesidad del acceso a los mismos y que sean facilitados a la autoridad competente en caso de ser necesarios, reconociendo así su importancia en la lucha policial y procesal contra el cibercrimen.

No obstante, es necesario poner de manifiesto la imperante necesidad de conjugar esta colaboración con la protección del derecho a la intimidad y la confidencialidad de determinados datos. A este respecto, se ha puesto de manifiesto que la redacción del Convenio resulta demasiado vaga y confusa como para resultar verdaderamente protectora de los derechos fundamentales de los investigados e interesados[623]. Todo entra en contraste si tenemos en cuenta que queda fuera de duda la repercusión que muchos de los preceptos del convenio tienen para los Derechos Humanos, especialmente en lo que respecta a la intimidad y a la protección de datos.

Igualmente, se critica también que el convenio no haga referencia a la necesidad de autorización judicial cuando la injerencia en los datos personales, por parte de las autoridades estatales, supone una clara intromisión en la esfera privada de los derechos, siendo necesaria una resolución judicial motivada[624].

A este respecto, no pueden dejarse sin destacar las dudas que plantea la propia redacción del Convenio respecto de la legitimidad de las medidas en cuestión, considerando su carácter indiscriminado en cuanto a los sujetos pasivos de la medida (ya que no se especifica que quienes deban padecer la retención de sus datos se individualicen en virtud de la existencia de un procedimiento penal en el que se hallen involucrados), la ausencia de procedimiento penal en curso y el excesivo alcance de la medida para un propósito que se podría obtener a través de otras medidas.

Incluso se ha llegado a afirmar que las medidas contenidas en el Convenio podrían vulnerar el principio de especialidad, por cuanto no se especifica que quienes deban padecer la retención de sus datos se individualicen en virtud de la existencia de un procedimiento penal en el que se hallen involucrados[625].

3. COOPERACIÓN POLICIAL EN EL ÁMBITO DE LA UNIÓN EUROPEA

Para la Unión Europea, el cibercrimen constituye la prioridad dentro del ciclo de políticas 2018–2021. En este sentido, sus principales finalidades son: 1) interrumpir las actividades delictivas relacionadas con los ataques contra los sistemas de información; 2)

---

[623] Dictamen 4/2001 acerca del proyecto de convenio del Consejo de Europa sobre el ciberdelito, 5001/01/ES/Final WP 41, 22 de marzo de 2001.
[624] DÍAZ GÓMEZ, A., "El delito informático, su problemática y la cooperación internacional como paradigma de su solución", cit., p. 201.
[625] *Ibid.*, p. 200.

luchar contra el abuso sexual infantil y la explotación sexual infantil, incluyendo la producción y difusión de material con tal contenido; y 3) perseguir a los delincuentes involucrados en el fraude y la falsificación de medios de pago distintos del efectivo, incluido el fraude con tarjetas de pago a gran escala (especialmente el fraude con tarjeta no presente) y las amenazas a otros medios de pago distintos del efectivo.[626]

La cooperación judicial en materia penal (artículo 82 a 86 TFUE) y la cooperación policial (artículos 33, en materia de cooperación aduanera, y 87 a 89 TFUE) han constituido unas de las principales políticas[627] sobre los que se ha venido desarrollando el espacio común de libertad, seguridad y justicia, por lo que su estudio debe comenzar, necesariamente, por exponer los antecedentes y la evolución de este último[628].

A ese respecto, debemos adelantar que la situación actual, en la que la creación de un espacio de libertad, seguridad y justicia (ELSJ) ha devenido en una de las principales finalidades de la Unión Europea[629], es el resultado de un largo y complejo proceso de formación de la confianza mutua entre las instituciones de los diferentes Estados miembros[630]. Por ello, a continuación, destacamos los hitos que entendemos más importantes dentro del proceso de formación de dicho espacio de libertad, seguridad y justicia[631].

---

[626] "EU Policy Cycle – EMPACT", *Europol*, en https://www.europol.europa.eu/empact, fecha de consulta 7 marzo 2020.

[627] A ellas han de añadirse las políticas sobre controles en las fronteras (artículos 67 y 77 TFUE), asilo (artículos 67.2, 78 y 80 TFUE), inmigración (artículo 79 y 80 TFUE) y cooperación judicial en materia civil (artículo 81 TFUE y protocolos núm. 21 y 22).

[628] "Un espacio de libertad, seguridad y justicia: aspectos generales | Fichas temáticas sobre la Unión Europea | Parlamento Europeo", en https://www.europarl.europa.eu/factsheets/es/sheet/150/un-espacio-de-libertad-seguridad-y-justicia-aspectos-generales, fecha de consulta 25 marzo 2022

[629] El artículo 3.2 TUE sitúa la creación del espacio de libertad, seguridad y justicia como un fin de mayor importancia respecto al anterior Tratado de Niza, incluso por delante de otros como el establecimiento de un mercado interior o de una unión económica y monetaria, y únicamente precedido por la finalidad de promover la paz, sus valores y el bienestar de sus pueblos.

[630] REMOTTI CARBONELL, J. C., "El proceso de formación del espacio de libertad, seguridad y justicia en la Unión Europea. La lucha contra la delincuencia, cooperación policial y judicial y garantías del debido proceso en el ámbito penal", en *Garantías del proceso debido y Unión Europea: implicaciones para los ordenamientos internos, 2020, pp. 21-70*, Centro de Estudios Políticos y Constitucionales (España), 2020, p. 22, fecha de consulta 28 febrero 2022, en https://dialnet.unirioja.es/servlet/articulo?codigo=7765253.

[631] No pretendemos, sin embargo, desarrollar una cronología completa del proceso de formación de la Unión Europea, sino tan sólo señalar los eventos más importantes dentro del proceso de formación del ELSJ.

A. ANTECEDENTES: LA CONFIGURACIÓN DE UN ESPACIO DE LIBERTAD, SEGURIDAD Y JUSTICIA COMÚN EN LA UNIÓN EUROPEA

a) Las Comunidades Europeas

Los orígenes inmediatos de la Unión Europea pueden encontrarse en la voluntad de los Estados europeos, tras la II Guerra Mundial, de recuperar la capacidad económica perdida y de procurar evitar futuras guerras entre naciones europeas[632].

La prioridad[633] era formar un mercado común[634] que sirviera como instrumento para aproximar los diferentes Estados europeos, desarrollando así actuaciones comunes en materia de aranceles, libre circulación de bienes, capitales, situaciones monopolísticas, etc.

Con este fin, fueron constituidas la Comunidad Europea del Carbón y del Acero[635] (CECA) y, más adelante, la Comunidad Económica Europea (CEE) y la Comunidad Europea de la Energía Atómica (EURATOM) –estas dos últimas, mediante los llamados Tratados de Roma[636]–. Posteriormente, las instituciones creadas por estas *Comunidades*

---

[632] Como dijo Robert Schuman en su declaración de 9 de mayo de 1950: "L'Europe n'a pas été faite, nous avons eu la guerre […] L'Europe ne se fera pas d'un coup, ni dans une construction d'ensemble: elle se fera par des réalisations concrètes créant d'abord une solidarité de fait", disponible en https://european-union.europa.eu/principles-countries-history/history-eu/1945-59/schuman-declaration-may-1950_fr, fecha de consulta 26 de marzo de 2022.

[633] O mejor, podríamos decir que fue la mejor vía concebida para iniciar el proceso de convergencia europea: aglutinar los intereses económicos como un primer paso.

[634] RIPOLL NAVARRO, R.; TERRÁDEZ SALOM, D.; BELLIDO BARRIONUEVO, M., *La Unión Europea Organización y Funcionamiento*, Tirant lo Blanch, Valencia, 2015, p. 26.

[635] Tratado constitutivo de la Comunidad Europea del Carbón y del Acero, firmado el 18 de abril de 1951, con entrada en vigor el 23 de julio de 1952 y una duración de 50 años (expiró el 23 de julio de 2002). Inicialmente, reunió a 6 países (Bélgica, Alemania, Francia, Italia, Luxemburgo y los Países Bajos) con el fin de organizar la libertad de circulación del carbón y del acero y el libre acceso a las fuentes de producción, estableciendo *de facto* que ningún país pudiera movilizar sus fuerzas armadas sin que los demás países se percataran, mitigando así la desconfianza y tensiones existentes tras la II Guerra Mundial, como se indica en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Axy0022, fecha de consulta 25 de marzo de 2022.

[636] Tratado constitutivo de la Comunidad Económica Europea y Tratado constitutivo de la Comunidad Europea de la Energía Atómica, ambos firmados por Alemania Federal, Bélgica, Francia, Italia, Luxemburgo, y los Países Bajos el 25 de marzo de 1957, con entrada en vigor el 1 de enero de 1958 tras ser ratificados por los parlamentos de cada Estado miembro. El primero ha sido modificado en varias ocasiones y actualmente se llama Tratado de Funcionamiento de la Unión Europea y, entre otras cuestiones, estableció un mercado común, una unión aduanera y políticas comunes en materia agrícola, comercial y de transportes, como se indica en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=legissum:xy0023, fecha de consulta 26 de marzo de 2022. El segundo perseguía crear las condiciones necesarias para desarrollar una industria nuclear común en Europa, no ha experimentado nunca grandes cambios y sigue estando en vigor, sin que EURATOM se haya fusionado con la Unión Europea, por lo que conserva una personalidad jurídica distinta, como se indica en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:xy0024, fecha de consulta 25 de marzo de 2022.

Europeas para su funcionamiento fueron racionalizadas y unificadas[637] mediante el Tratado de Bruselas.

Durante este periodo inicial, como decimos, la aproximación de las naciones europeas se concentró en perseguir la convergencia de los diferentes y particulares intereses económicos de los Estados miembros, evitando –al menos, por el momento– entrar en cuestiones políticas o particulares de cada Estado, y que podrían generar más desavenencias que avances en el proceso de integración europea.

De esta manera, asuntos como la criminalidad internacional eran considerados cuestiones de competencia interna de cada uno de los Estados, que debían gestionar de manera independiente o, cuanto menos, a través de los instrumentos internacionales tradicionales que pudieran celebrar[638]. Siendo el principal objetivo reforzar el mercado común, se entendía que no correspondía a las incipientes Comunidades Europeas atender tales cuestiones, que escapaban a su ámbito competencial y supondrían una distracción de su principal objetivo, cuando no un motivo de conflictos[639] entre sus miembros que podría poner en peligro el proceso de integración europea[640].

b) El Grupo de Trevi

Ahora bien, durante la década de 1970 varias organizaciones terroristas se encontraban activas en Europa, como el Ejército Republicano Irlandés, la Facción del Ejército Rojo y los Grupos de Acción Revolucionaria Internacionalista. Según información disponible en la *Global Terrorism Database*, más de 1.500 ataques terroristas fueron

---

[637] También conocido como el Tratado de Fusión, firmado el 8 de abril de 1965 y con entrada en vigor el 1 de julio de 1967. Estableció la creación de una única Comisión y un único Consejo al servicio de las, por aquel entonces, tres Comunidades Europeas (CEE, Euratom y CECA) tal y como se señala en https://eur-lex.europa.eu/legal-content/ES/LSU/?uri=CELEX:11965F/TXT, fecha de consulta 26 de marzo de 2022.

[638] REMOTTI CARBONELL, J. C., *Constitución y medidas contra el terrorismo. La suspensión individual de derechos y garantías*, Colex, A Coruña, 1999, p. 67, en https://dialnet.unirioja.es/servlet/articulo?codigo=8127711, fecha de consulta 15 marzo 2022.

[639] Con el fracaso de los "planes Fouchet", los desacuerdos de 1963 y 1967 y la crisis de la "silla vacía" de 1965 y 1966, cuando Francia decidió no participar en las reuniones del Consejo en señal de protesta porque la toma de determinadas decisiones estuviera sometida a mayoría cualificada, en lugar de la unanimidad, y que finalizó con la adopción del Compromiso de Luxemburgo el 30 de enero de 1966, en la que se mantenía que, cuando estuvieran en juego intereses muy importantes de una o más partes, los miembros del Consejo se esforzarían, dentro de un plazo razonable, por alcanzar soluciones que pudieran ser adoptadas por todos los miembros del Consejo respetando sus intereses mutuos y los de la Comunidad.

[640] Sin perjuicio de que la cooperación política constituyera un objetivo a largo alcance. Sin ir más lejos, en la primera conferencia de la cumbre, que posteriormente evolucionaría hasta constituir el actual Consejo europeo, señalaba la finalidad de "[…] buscar los medios adecuados para organizar una cooperación política más estrecha […]", y de igual modo en las reuniones celebradas en Bonn (1961), Roma (1967) y La Haya (1969) como se puede comprobar en el resumen contenido en https://www.consilium.europa.eu/media/31019/qc3111406esc.pdf, fecha de consulta 27 de marzo de 2022.

perpetrados entre los años 1970 y 1975 y, de ellos, 1.289 tuvieron lugar en los Estados que comprendían la Comunidad Económica Europea, destacando los 962 atentados que fueron cometidos en Reino Unido[641]. A este respecto, se ha fijado[642] como punto de no retorno en el proceso de cooperación policial y judicial en Europa el atentado terrorista que tuvo lugar durante los Juegos Olímpicos de 1972[643], señalándose, así, que la lucha contra el terrorismo, en cualquiera de sus modalidades, constiuía uno de los fundamentos de la cooperación policial entre los Estados miembros de la entonces Comunidad Económica Europea.

De esta manera, se aprecia que los dirigentes europeos pudieron comprobar cómo la delincuencia internacional, en general, y el terrorismo, en particular, se convertían en una problemática generalizada e impeditiva no sólo para la paz europea, sino también para que continuara el proceso de integración económica de los Estados europeos[644].

En este contexto, con ocasión del Consejo Europeo de Roma de 1975, los Estados miembros aceptaron la propuesta del Primer Ministro del Reino Unido para que las autoridades nacionales con competencia en asuntos de interior pudieran reunirse con objeto de poner en común asuntos relativos a sus competencias[645]. No extraña que la propuesta procediera de Reino Unido, a la vista del número de atentados terroristas que tuvieron lugar en su territorio durante los años anteriores[646].

La ejecución de dicha propuesta dio lugar al nacimiento del grupo de Trevi, que se conformó como un espacio informal de cooperación policial caracterizado por el acceso restringido y confidencial, al margen de los Parlamentos y de la opinión pública, y

---

641 Empleando datos disponibles en la *Global Terrorism Database*, disponible en https://www.start.umd.edu/gtd/search/Results.aspx?page=1&casualties_type=b&casualties_max=&start_yearonly=1970&end_yearonly=1976&dtp2=all&region=8&charttype=line&chart=overtime&ob=GTDID&od=desc&expanded=yes#results-table, fecha de consulta 27 de marzo de 2022

642 GROENLEER, M. L. P., "The autonomy of European Union Agencies. A comparative study of institutional development.", 2009, Eburon, p. 278, en https://hdl.handle.net/1887/14519, fecha de consulta 10 abril 2022.

643 También conocido como "la masacre de Múnich" y "Operación Ikrit y Biraam", fue un atentado terrorista perpetrado el 4 de septiembre de 1972, durante los Juegos Olímpicos de Múnich, Baviera, al sur de Alemania Occidental, cuando once miembros del equipo olímpico israelí fueron tomados como rehenes y asesinados por un comando del grupo terrorista Septiembre Negro, organización terrorista palestina fundada en 1970.

644 REMOTTI CARBONELL, J. C., "El proceso de formación del espacio de libertad, seguridad y justicia en la Unión Europea. La lucha contra la delincuencia, cooperación policial y judicial y garantías del debido proceso en el ámbito penal", cit., p. 26.

645 Como puede comprobarse en la sección "other business" del boletín relativo al Consejo, disponible en http://aei.pitt.edu/1407/1/rome_dec_1975.pdf, y accedido el 10 de abril de 2022.

646 Hasta 962 atentados, según se puede comprobar en la *Global Terrorism Database*, a la que ya nos hemos referido.

en el que se buscaba un acercamiento y la construcción de confianza en torno a la cooperación policial en la lucha contra la criminalidad internacional.

En el grupo de Trevi se reunían los altos oficiales policiales europeos dos veces al año para intercambiar información y experiencias relativas a los actos terroristas internacionales. En un inicio se integró por los nueve Estados Miembro de las Comunidades Económicas Europeas (Alemania, Bélgica, Dinamarca, Francia, Holanda, Irlanda, Italia, Luxemburgo y Reino Unido)[647], y se establecieron cuatro reglas fundamentales con las que se pretendía establecer una participación igualitaria de todos los Estados, regida por las reglas de periodicidad, independencia y confidencialidad: 1) sólo podían participar los Ministros de Seguridad y Justicia nacionales en las discusiones sobre los temas y acciones que se llevarían a cabo, 2) a los acuerdos se llegaba por unanimidad, 3) se reunían dos veces al año y 4) no existía ningún mecanismo que obligara a intercambiar información[648].

En cuanto a la estructura del grupo de Trevi, estaba compuesto por los ministros de Interior y Justicia, oficiales y expertos de policía. El nivel decisorio correspondía a los Ministros de Interior y Justicia, los cuales se reunían en conferencias para acordar la agenda de actividades[649]. En régimen de dependencia respecto de los Ministros, se encontraban los altos oficiales nacionales de seguridad, quienes daban consejos, planeaban y organizaban las actividades de los oficiales de seguridad y expertos. Estos últimos eran quienes tenían la responsabilidad de organizar los grupos de trabajo en donde finalmente se llevaba a cabo el intercambio de información y de asistencia[650]. Posteriormente, este nivel operativo sería subdividido en cinco grupos de trabajo especializados: drogas y

---

[647] A los cuales se sumaron posteriormente como Estados Miembro o asociados Austria (1995), Canadá (1987), España (1986), Estados Unidos (1987), Grecia (1981), Marruecos (1993), Noruega (1995), Portugal (1986) y Suecia (1995). La diferencia entre el Estado miembro y el asociado radicaba en la capacidad de decisión: mientras que los primeros tenían voz y voto en la toma de decisiones y podían participar en los diferentes mecanismos que se fueron desarrollando, los asociados tenían solamente y no voto, y su participación en los mecanismos era reducida o condicionada.

[648] Albaladejo, F., Seguridad interior, seguridad exterior ¿dónde quedan las fronteras?, Fundación Policía Española, p. 60, en http://www.dykinson.com/libros/seguridad-interior-seguridad-exterior-donde-quedan-las-fronteras/9788461421992/, fecha de consulta 11 abril 2022.

[649] Estas conferencias tenían periodicidad semestral y en ellas se discutían los temas que serían desarrollados, las líneas de acción, los mecanismos deseables para cooperar y en general las inquietudes que existían sobre el fenómeno terrorista y los delitos relacionados. Resulta destacable que en los acuerdos de tales conferencias intervenían el anterior, actual y futuro director del grupo, con lo cual no había espacio para que los acuerdos no se cumplieran por un cambio de agenda de la dirección del grupo.

[650] KLOSEK, J., "The Development of International Police Cooperation within the EU and Between the EU and Third Party States: A Discussion of the Legal Bases of Such Cooperation and the Problems and Promises Resulting Thereof", *American University International Law Review*, vol 14, 1999, p. 635.

crímenes serios, equipamiento y entrenamiento policial y orden público, medidas de contingencia ante emergencias naturales, seguridad de instalaciones nucleares y de transportes, y terrorismo[651].

Tras varios años de funcionamiento[652] y reuniones semestrales, en 1991 se acordó prever la desaparición del grupo de Trevi, dando paso en primer lugar a la Unidad de Drogas de Europol. Finalmente, el grupo de Trevi desapareció en 1993 como tal y la Unidad de Drogas de Europol se consolidó dentro de la Unión Europea, como paso intermedio entre el grupo de Trevi y la formación completa de la Oficina de la Policía Europea (Europol)[653].

Durante el periodo de funcionamiento del grupo de Trevi, fueron dictadas varias resoluciones en materia de justicia y lucha contra el terrorismo y la criminalidad. Entre dichas resoluciones, podemos citar la Resolución del Parlamento Europeo de 14 de enero de 1977, por la que se invitaba a los Estados comunitarios a ratificar la Convención europea sobre la represión del terrorismo; el Acuerdo de la Reunión monográfica de carácter informal de los Ministros del Interior de los Estados comunitarios sobre la lucha contra el terrorismo, de 31 de mayo de 1977, en el que condenan enérgicamente cualquier acto de terrorismo; la Resolución del Parlamento Europeo de 16 de noviembre de 1977, en la que se invitaba a la Comisión Europea a organizar conferencias en materia de cooperación entre autoridades nacionales; el Acuerdo del Consejo Europeo de 7 y 8 de abril de 1978, en el que se acordaba priorizar los esfuerzos para mejorar la cooperación entre países comunitarios; y la resolución del Parlamento Europeo de 12 de abril de 1978, también dedicada al fortalecimiento de la lucha europea contra el terrorismo.

---

[651] Los trabajos de este último grupo darían lugar a la celebración, el 27 de enero de 1977, del Convenio Europeo para la Represión del Terrorismo.

[652] Podemos destacar las Conferencias de 1986 en la Haya, Estrasburgo y Londres, relativas al establecimiento de una línea de comunicación urgente en casos de terrorismo y al intercambio de información sobre licencias de armas; las de 1987 en Bruselas y Copenhague en materia de política común de visados; las de 1988 en Múnich y Atenas en materia de análisis de esquemas de seguridad para eventos deportivos masivos; las 1989 en Madrid y París, por las que se creó una oficina central o dirección para el grupo; las de 1990 en Dublín y Roma, relativas al establecimiento de instrumentos de cooperación y medidas de seguridad olímpica, y las de 1991 en La Haya y Luxemburgo, que acordaron presentar un proyecto en la cumbre de Maastricht para hacer frente de manera conjunta y coordinada al problema de la delincuencia organizada internacional, decisión, esta, que terminaría dando lugar a la formación de Europol.

[653] ALBALADEJO, F., *Seguridad interior, seguridad exterior ¿dónde quedan las fronteras?*, cit., p. 62.

Finalmente, el 28 y 29 de junio de 1985 la Comisión europea emite un Libro blanco sobre la realización del mercado interior[654]. Las medidas incluidas en el mismo estaban orientadas a la supresión de los controles de mercancías y personas en las fronteras interiores, con la finalidad de eliminar las barreras físicas que impedían la realización de dicho objetivo. Para ello, se configuraron dos instrumentos generales: el Acuerdo Schengen y el Acta Única Europea.

c) El Acta Única Europea

El 17 de febrero de 1986 en Luxemburgo y el 28 de febrero de 1986 en La Haya es firmada el Acta Única Europea[655] por los doce países miembros que en ese momento formaban la Comunidad Europea: Bélgica, Dinamarca, Alemania, Irlanda, Grecia, España, Francia, Italia, Luxemburgo, Países Bajos, Portugal, Reino Unido. Entró en vigor el 1 de julio de 1987.

La finalidad del Acta Única Europea (AUE) era revisar los Tratados de Roma, constitutivos de la Comunidad Económica Europea (CEE) y la Comunidad Europea de la Energía Atómica, todo ello para reactivar la integración europea, reformar el funcionamiento de las instituciones y agilizar la toma de decisiones para predisponer la llegada del mercado único.

Para facilitar la consecución de dicho objetivo, el AUE aumentó los supuestos en los que el Consejo podía decidir por mayoría cualificada en vez de por unanimidad. Ello hizo que la aprobación de las decisiones fuera más fácil, evitando los bloqueos inherentes a la búsqueda de un acuerdo unánime de los doce países miembros. En particular, el voto por mayoría cualificada se convirtió en la nueva norma en cuatro de los ámbitos existentes abarcados por los Tratados: el arancel aduanero común; la libre circulación de capitales; la libre circulación de servicios, y el transporte marítimo y aéreo. El AUE también introdujo varios ámbitos políticos nuevos en los cuales las decisiones se tomarían por mayoría cualificada[656].

---

[654] COM/85/0310 FINAL, disponible en EUR-Lex - 51985DC0310 - EN - EUR-Lex (europa.eu), fecha de consulta 11 de abril de 2022.
[655] Acta Única Europea, DOCE núm. L 169, de 29 de junio de 1987, pp. 1-30.
[656] Entre estos, se encontraban: el mercado interior; la cohesión económica y social: para compensar los efectos de la realización del mercado interior en las regiones menos desarrolladas; la política social: dos nuevos aspectos de esta política, la salud y la seguridad de los trabajadores, y el diálogo social entre candidatos y la patronal; investigación y desarrollo; el medio ambiente: mediante la introducción del principio

d) El Acuerdo de Schengen y posterior Convenio

Unos meses antes de la firma del Acta Única Europea, el 14 de junio de 1985, Bélgica, Francia, Alemania, Luxemburgo y los Países Bajos celebraron el Acuerdo de Schengen[657], por el que acordaban eliminar progresivamente los controles en sus fronteras interiores y establecer un régimen de libre circulación para todos los nacionales de los países signatarios. De acuerdo con el artículo 9 del Acuerdo, se perseguía reforzar la cooperación entre las autoridades aduaneras y policiales, la lucha contra la criminalidad, el tráfico ilícito de estupefacientes y armas, la estancia irregular de personas y el fraude fiscal y aduanero. Del mismo modo, el artículo 17 consagraba también como objetivo "suprimir los controles en las fronteras comunes y transferirlos a sus fronteras externas"[658].

Con posterioridad, el 19 de junio de 1990, fue firmado el Convenio de aplicación del Acuerdo de Schengen[659], que desarrolló y completó el acuerdo definiendo requisitos, condiciones, procedimientos, garantías y otras medidas que hicieran viable la libre circulación, entre ellos.

Como se ha encargado de destacar la doctrina[660], el Acuerdo Schengen conforma, al menos en esta etapa inicial, un supuesto de cooperación reforzada[661], en la medida en que constituyó un instrumento internacional adoptado de manera voluntaria por una parte de los que entonces eran Estados miembros de la Comunidad Europea[662]. De hecho,

---

de subsidiariedad (es decir, la adopción de medidas únicamente a escala europea cuando estas sean más eficaces que a escala de un país concreto), y la política exterior común: con la responsabilidad por parte de la presidencia del Consejo de iniciar la acción y coordinar las posiciones de los países miembros.

[657] Acuerdo entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 14 de junio de 1985, DOUE n° L 239, de 22 de septiembre de 2000, pp. 19-62.

[658] El artículo 9 del Acuerdo Schengen dispone expresamente que "Las partes intentarán armonizar las legislaciones y normas reglamentarias, en especial: – En materia de estupefacientes. – En materia de armas y explosivos. – En lo relativo a la declaración de los viajeros en los hoteles."

[659] Convenio de aplicación del Acuerdo firmado en Schengen el 19 de junio de 1990.

[660] REMOTTI CARBONELL, J. C., "El proceso de formación del espacio de libertad, seguridad y justicia en la Unión Europea. La lucha contra la delincuencia, cooperación policial y judicial y garantías del debido proceso en el ámbito penal", cit., p. 28.

[661] Instrumento que permite a un grupo de Estados miembros que puedan desarrollar conjuntamente unos objetivos, programas o líneas de actuación sin tener que contar con la totalidad de miembros de la UE.

[662] De hecho, los Estados que inicialmente suscribieron el Acuerdo y el Convenio Schengen se unirían posteriormente: Italia en 1990, España y Portugal en 1991. Grecia lo hizo en 1992, Austria en 1995, Dinamarca, Suecia, Finlandia en 1996. Por su parte Chipre, República Checa, República Eslovaquia, Eslovenia, Estonia, Hungría, Letonia, Lituania, Malta, Polonia en 2004, así como Bulgaria y Rumanía (2007). Por su parte, el espacio Schengen también es aplicable de acuerdo a convenios suscritos a Islandia, Noruega y Suiza, Liechtenstein, Mónaco, San Marino y la Ciudad del Vaticano.

aunque en la actualidad se encuentra integrado en los tratados de la Unión Europea, con ocasión del Tratado de Ámsterdam -al que después nos referiremos-, el acervo de Schengen fue integrado en el marco de la Unión Europea exclusivamente como un protocolo anexo, bajo la fórmula de la cooperación reforzada, de manera que solo era directamente aplicable a los países que lo hubieran reforzado.

En el acervo Schengen, en general, se establecían una serie de medidas de cooperación policial y judicial que es necesario destacar, además de la creación del espacio Schengen propiamente dicho.

En lo relativo a la cooperación policial, se adoptaron varias disposiciones. Entre ellas, podemos destacar la autorización a los cuerpos policiales nacionales a continuar en otro territorio, y dentro del marco de una investigación judicial, la vigilancia de una persona sobre la que recayera la sospecha de participación en un delito que pudiera dar lugar a una extradición (artículo 40 CSc); la posibilidad de que, en casos de urgencia, pudieran continuar la persecución en el territorio de otro Estado parte de una persona hallada en flagrante delito (artículo 41 CSc); la previsión de la cooperación y colaboración de los cuerpos de policía, siempre desde el respeto a la legislación nacional y dentro de los límites de sus competencias (artículo 39 CSc); y la obligación de que empresas dedicadas al hospedaje comprobasen la identidad de sus huéspedes con un documento de identidad vigente y retransmitieran las fichas a las autoridades competentes, quienes a su vez podrían remitirlas a otro Estado parte sin necesidad de solicitud previa (artículos 45 y 46 CSc)[663].

Por lo que se refiere a la cooperación judicial, se perseguía completar el Convenio europeo de asistencia judicial en materia penal de 20 de abril de 1959 y el capítulo II del Tratado Benelux de extradición y asistencia judicial en materia penal de 27 de junio de 1962[664]. En tal sentido, se previeron casos adicionales a los previstos en dichos instrumentos anteriores en los que también se prestaría asistencia judicial[665].

---

[663] REMOTTI CARBONELL, J. C., "El proceso de formación del espacio de libertad, seguridad y justicia en la Unión Europea. La lucha contra la delincuencia, cooperación policial y judicial y garantías del debido proceso en el ámbito penal", cit., p. 31.

[664] Tal y como prevé el artículo 48 del Convenio Schengen.

[665] En concreto, el artículo 49 del Convenio Schengen enumera como supuestos adicionales los siguientes "a) en procedimientos por hechos que sean punibles con arreglo al Derecho nacional de una de las dos Partes contratantes como infracciones de los reglamentos perseguidas por autoridades administrativas cuya decisión pueda dar lugar a un recurso ante un órgano jurisdiccional competente, en particular en materia

Por último, es debido señalar también la previsión de la creación del Sistema de Información Schengen, por medio del cual todos los Estados parte podrían consultar de manera automatizada de las descripciones de personas y de objetos en el momento de realizar controles de frontera, de policía o de aduanas o expedición de visados realizados dentro de su país.

Para finalizar este apartado, y atendiendo a su proximidad cronológica (aunque no forme parte del Acervo Schengen), debemos hacer referencia a la Convención de Dublín de 15 de junio de 1990[666], especialmente referida a la cooperación policial en materia de asilo. La Convención de Dublín fue derogada por el Reglamento 343/2003 del Consejo, de 18 de febrero de 2003 (Reglamento Dublín II[667]), que posteriormente ha sido derogado por el Reglamento 604/2013, de 26 de junio de 2013, del Parlamento Europeo y del Consejo (Reglamento Dublín III[668]), complementado por el Reglamento 603/2013[669], por el que se crea el sistema Eurodac, que gestiona el almacenamiento y tratamiento de huellas dactilares de solicitantes de asilo y refugio, así como su transmisión entre los distintos Estados miembros.

---

penal; b) en procedimientos de indemnización por medidas de instrucción o condenas injustificadas; c) en los procedimientos de gracia; d) en las acciones civiles conexas a las acciones penales, mientras el órgano jurisdiccional penal aún no se haya pronunciado definitivamente sobre la acción penal; e) para la notificación de comunicaciones judiciales relativas a la ejecución de una pena o medida de seguridad, de la percepción de una multa o del pago de las costas procesales; f) para medidas relativas a la suspensión del veredicto o el aplazamiento de la ejecución de una pena o medida de seguridad, a la puesta en libertad condicional, al aplazamiento de la ejecución o a la interrupción de la ejecución de una pena o medida de seguridad."

[666] Convenio relativo a la determinación del Estado responsable del examen de las solicitudes de asilo presentadas en los Estados miembros de las Comunidades Europeas (97/C 254/01), DOCE núm. L 254 de 19 de agosto de 1997, pp. 1-12.

[667] Reglamento (CE) nº 343/2003 del Consejo, de 18 de febrero de 2003, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de asilo presentada en uno de los Estados miembros por un nacional de un tercer país, Documento l33153, DOUE núm. L 50 de 25 de febrero de 2003, pp. 1-10.

[668] Reglamento (UE) n ° 604/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, DOUE núm. L 180, de 29 de septiembre de 2013, pp. 31-59.

[669] Reglamento (UE) n ° 603/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013 , relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) n ° 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, y por el que se modifica el Reglamento (UE) n ° 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia, DOUE núm. L 180 de 29.6.2013, p. 1/30.

e) El Tratado de Maastricht

El 7 de febrero de 1992 fue firmado el Tratado de Maastricht[670], que entró en vigor el 1 de noviembre de 1993, produciéndose con ello una modificación sustancial de la estructura y el funcionamiento de las instituciones europeas[671].

De conformidad con el artículo A, mediante dicho Tratado los Estados parte constituyeron la Unión Europea, que nace conceptualmente en dicho momento, sosteniendo su actividad en tres pilares.

El primer pilar se identifica con las Comunidades Europeas formadas hasta entonces[672], centradas en la formación de un mercado común (artículos G, H e I del Tratado de Maastricht).

El segundo pilar se refería a la política exterior y de seguridad común, con objetivos como proteger los valores comunes, los intereses fundamentales y la independencia de la UE; reforzar la seguridad de la UE y de sus países miembros; preservar la paz y la seguridad internacionales de acuerdo con los principios de las Naciones Unidas; promover la cooperación internacional; desarrollar y consolidar la democracia y el Estado de Derecho así como el respeto por los derechos humanos y las libertades fundamentales (artículo J del Tratado de Maastricht).

Finalmente, el tercer pilar se identificaba con la cooperación en el ámbito de la justicia y los asuntos de interior, con la finalidad de instituir un alto nivel de seguridad mediante el establecimiento de normas y controles para las fronteras exteriores de la UE; la lucha contra el terrorismo, la delincuencia organizada, el tráfico de drogas y el fraude internacional; la organización de la cooperación judicial en materia penal y civil; la creación de una Oficina Europea de Policía[673] (Europol) para el intercambio de información entre las fuerzas nacionales; el control de la inmigración ilegal; y el desarrollo de una política común de asilo (artículo K del Tratado de Maastricht).

---

[670] Tratado de la Unión Europea, DOUE núm. C 191 de 29 de julio de 1992 pp. 1-10.
[671] REMOTTI CARBONELL, J. C., "El proceso de formación del espacio de libertad, seguridad y justicia en la Unión Europea. La lucha contra la delincuencia, cooperación policial y judicial y garantías del debido proceso en el ámbito penal", cit., p. 34.
[672] La Comunidad Económica Europea, la Comunidad Europea del Carbón y del Acero, y la Comunidad Europea de la Energía Atómica, a las que ya nos hemos referido con anterioridad.
[673] En apartados posteriores volveremos sobre la figura de la Europol.

A este respecto, resulta interesante destacar que, en dicho momento, los acuerdos relativos al primer pilar se adoptaban de conformidad con las pautas y procedimientos legislativos comunitarios, mientras que los otros dos pilares, referidos a la política exterior y de Seguridad Común (PESC) y a la cooperación en Asuntos de justicia e interior, estaban sometidos a los procedimientos y a las vías propias de la cooperación intergubernamental, si bien en el espacio institucional de la Unión Europea[674].

En lo que nos interesa al respecto de la formación del ELSJ, el Tratado de Maastricht es fundamental porque establece la cooperación estrecha en el ámbito de la justicia y de los asuntos de interior como uno de los principales objetivos de la Unión Europea, quedando así amparado este particular por el paraguas de la Unión Europea.

De esta manera, se preveían mecanismos incipientes de cooperación en materia de justicia y asuntos de interior, destinados a facilitar la actuación conjunta en materia de prevención y lucha contra el terrorismo, tráfico de drogas y, en general cualquier forma grave de delincuencia internacional (artículo K.1.9). Asimismo, se creó Europol como fórmula para articular la cooperación policial de los diferentes Estados miembros (artículo K.1.9), y se previó expresamente que la Unión Europea debía respetar en el desarrollo de sus actividades lo dispuesto por el Convenio Europeo de Derechos Humanos, así como lo establecido en la Convención sobre el Estatuto de los refugiados (artículo K.2)[675].

f) El Tratado de Ámsterdam y el Programa de Tampere

Tras el Tratado de Maastricht, el siguiente hito fundamental en la formación del espacio de libertad, seguridad y justicia fue el Tratado de Ámsterdam[676], firmado el 2 de octubre de 1997 y que entró en vigor el 1 de mayo de 1999, cuyo objetivo general era actualizar el Tratado de Maastricht para preparar a la Unión Europea (UE) para su futura

[674] REMOTTI CARBONELL, J. C., "El proceso de formación del espacio de libertad, seguridad y justicia en la Unión Europea. La lucha contra la delincuencia, cooperación policial y judicial y garantías del debido proceso en el ámbito penal", cit., p. 35.
[675] Convención sobre el Estatuto de los Refugiados, hecha en Ginebra el 28 de julio de 1951, y al Protocolo sobre el Estatuto de los Refugiados, hecho en Nueva York el 31 de enero de 1967.
[676] El Tratado de Ámsterdam por el que se modifica el Tratado de la Unión Europea, DOCE núm. C 340 de 10 de noviembre de 1997, pp. 1-144.

ampliación[677], estableciendo mecanismos que permitieran garantizar una estructura y funcionamiento más eficaz, transparente y democrático[678].

Con el Tratado de Ámsterdam, el título VI del Tratado de Maastricht fue sustituido por otro, denominado "disposiciones relativas a la cooperación policial y judicial en materia penal". En dicho Título VI, quedó establecido como objetivo principal "ofrecer a los ciudadanos un alto grado de seguridad dentro de un espacio de libertad, seguridad y justicia", para lo que se reconoció como necesario la elaboración de una acción en común entre los Estados miembros en los ámbitos de la cooperación policial y judicial en materia penal para la prevención y la lucha contra la delincuencia, mediante el establecimiento de una mayor cooperación entre las fuerzas policiales, una mayor cooperación entre las autoridades judiciales y la aproximación de las normas de los Estados miembros en materia penal (artículo K.1). De esta manera, la consecución del espacio de libertad, seguridad y justicia aparece íntimamente ligada al desarrollo de la cooperación policial y judicial y a la aproximación de los ordenamientos jurídicos nacionales.

Además, no puede olvidarse que, mediante el Protocolo Anexo, todo el contenido del Acuerdo Schengen fue integrado en el marco jurídico de la Unión Europea, que pasó a ser vinculante para todos los Estados miembros con excepción de los países que hubiera optado expresamente por no participar en todo o parte del Acuerdo de Schengen (Irlanda y Reino Unido). Se aprecia en estas actuaciones el cambio de postura de las instituciones europeas, pretiriendo la flexibilización de criterios y la búsqueda de elementos de unidad (característico de momentos anteriores, en los que aún estaba por conformarse la Unión Europea) a favor del establecimiento de unos principios mínimos que los futuros Estados miembros deberían aceptar si querían incorporarse a las Comunidades Europeas.

En general, con el Tratado de Ámsterdam se amplió el ámbito de cooperación policial, incluyendo el intercambio de información, aspectos formativos y operativos en relación con la prevención, ubicación e investigación de las actividades delictivas. También se persiguió aumentar el protagonismo de Europol, configurándose como un instrumento para facilitar la preparación y coordinación de acciones de investigación por las

---

[677] MANGAS MARTÍN, A., "La reforma institucional en el Tratado de Amsterdam", *Revista de Derecho Comunitario Europeo*, vol. 2, 3, 1998, Centro de Estudios Políticos y Constitucionales, p. 2.
[678] REMOTTI CARBONELL, J. C., "El proceso de formación del espacio de libertad, seguridad y justicia en la Unión Europea. La lucha contra la delincuencia, cooperación policial y judicial y garantías del debido proceso en el ámbito penal", cit., p. 36.

autoridades competentes, y se reconoció la necesidad de expandir la cooperación judicial en materia penal, de manera que no se limitara a la cooperación entre Ministerios y autoridades judiciales, iniciándose de esta manera un proceso de aproximación o armonización de la normativa penal de cada Estado miembro, a fin de establecer normas mínimas comunes en relación con los elementos constitutivos de los delitos y las penas aplicables (artículo K).[679]

Dentro de este periodo temporal, el Consejo Europeo celebrado el 15 y 16 de octubre de 1999 en la ciudad de Tampere, fijó los objetivos prioritarios necesarios para impulsar la formación del espacio común de libertad, seguridad y justicia, desarrollando así lo establecido en el Tratado de Ámsterdam.

De esta manera, y entre otras cuestiones[680], en las Conclusiones de la Presidencia del Consejo de Tampere (CdPT, en adelante) se señaló la necesidad de encontrar vías para que: i) los ciudadanos de la Unión pudieran defender sus derechos intereses legítimos ante los órganos jurisdiccionales y autoridades de los demás Estados de la Unión (punto 5 CdPT); ii) los autores de hechos delictivos huidos del país en el que cometieron tales actos pudieran ser presentados ante los tribunales de justicia (punto 35 CdPT); iii) fuera posible establecer un sistema de reconocimiento mutuo de resoluciones judiciales (punto 48 CdPT); y iv) se incrementara el nivel de compatibilidad y convergencia entre los diferentes ordenamientos jurídicos europeos (punto 42 y43 CdPT)[681].

Adicionalmente, en materia de cooperación policial, se acordó también crear una unidad operativa internacional participada por los jefes de policía de los diferentes Estados miembro en la que estos pudieran intercambiar información (punto 44 CdPT), potenciar Europol para que cumpliera con un papel más activo, desarrollando funciones de prevención, análisis e investigación de la delincuencia, y la creación de la Academia europea de policía (punto 47 CdPT).

En materia de colaboración judicial, también fue ideada la creación de Eurojust (punto 46 CdPT), a fin de coordinar la actuación de los poderes judiciales de cada Estado

---

[679] DONAIRE VILLA, F. J., "El Tratado de Amsterdam y la Constitución", *Revista española de derecho constitucional*, vol. 18, 54, 1998, Centro de Estudios Políticos y Constitucionales (España), p. 135.
[680] También se convocó la Convención que redactaría el Proyecto de Carta de los Derechos Fundamentales de la Unión Europea.
[681] Disponibles en https://www.europarl.europa.eu/summits/tam_es.htm, fecha de consulta 27 de abril de 2022.

miembros, y avanzar en la aproximación legislativa de los diferentes ordenamientos para establecer un régimen de tipos delictivos y penas comunes entre los diferentes Estados miembros (punto 48 CdPT)[682].

Por último, no podemos terminar este apartado sin referirnos al principio de reconocimiento muto en el ámbito penal, considerado como piedra angular en la cooperación judicial civil y penal el cual "debe aplicarse tanto a las sentencias como a otras resoluciones de las autoridades judiciales" (punto 33 CdPT), instando, así mismo, al Consejo y a la Comisión para que adoptaran un programa de medidas para llevarlo a cabo, respetando los principios fundamentales de los Estados miembros (punto 37 CdPT).

g) El Tratado de Niza y el Programa de La Haya

Tras el Tratado de Ámsterdam, el 26 de febrero de 2001 es firmado el Tratado de Niza[683], que entra en vigor el 1 de febrero de 2003, y modifica el Tratado de la Unión Europea (TUE) y el Tratado constitutivo de la Comunidad Europea (TCE) con la finalidad de reformar las instituciones para que la Unión Europea pudiese funcionar eficientemente tras sumar 25 Estados miembros[684]. Las principales adiciones perseguían incrementar la legitimidad y la eficacia de las instituciones de la UE ante la perspectiva de la ampliación de los miembros de la UE en materia de composición de la Comisión Europea, sistema de votación en el Consejo de la Unión Europea, composición del Parlamento Europeo.

En lo que nos interesa, debemos destacar la reforma del Tribunal Superior de Justicia de la Unión Europea, con salas de 3 a 5 jueces, en gran sala (11 jueces) o en pleno (1 juez por cada país de la UE), mayores competencias del Tribunal de Primera Instancia (cuya denominación pasa a ser Tribunal General) para incluir algunas categorías de peticiones de decisión prejudicial, y la posibilidad de que el Consejo cree por unanimidad tribunales subsidiarios para tramitar en primera instancia ámbitos especiales del Derecho tales como las patentes. De igual modo, en materia de cooperación reforzada[685] se

---

[682] REMOTTI CARBONELL, J. C., "El proceso de formación del espacio de libertad, seguridad y justicia en la Unión Europea. La lucha contra la delincuencia, cooperación policial y judicial y garantías del debido proceso en el ámbito penal", cit., p. 40.

[683] Tratado de Niza por el que se modifican el Tratado de la Unión Europea, los Tratados Constitutivos de las Comunidades Europeas y determinados actos conexos, DOCE núm. C 80 de 10.3.2001, pp. 1-87.

[684] En este sentido, preparó la adhesión de 10 nuevos países miembros (República Checa, Chipre, Estonia, Hungría, Letonia, Lituania, Malta, Polonia, Eslovaquia y Eslovenia) en mayo de 2004 y 2 más (Bulgaria y Rumanía) en enero de 2007

[685] MANGAS MARTÍN, A., "Las cooperaciones reforzadas en el Tratado de Niza", en *Tratado de Niza: análisis, comentarios y texto, 2002, pp. 67-82*, Constitución y Leyes, COLEX, 2002, p. 70, fecha de consulta 28 abril 2022.

introdujeron nuevas normas: pasó a precisarse tan solo que la solicitaran un mínimo de 8 países de la Unión Europea, y no una mayoría (como sucedía hasta entonces), eliminándose la posibilidad de que un Estado miembro pudiera vetar el inicio de una cooperación reforzada, especialmente en el ámbito de la justicia y los asuntos de interior, en los que tampoco se requiere la aprobación de la Comisión o del Parlamento[686].

Tras la celebración del Tratado de Ámsterdam el 26 de febrero de 2001, pero antes de su entrada en vigor, con los atentados del 11 de septiembre de 2001 (New York) y, más concretamente, del 11 de marzo de 2004 (Madrid) y 7 de julio de 2005 (Londres), la lucha contra la delincuencia organizada y el terrorismo pasó a convertirse en una de las prioridades de la Unión Europea[687].

Dentro de ese proceso de reorganización de prioridades, debemos destacar la Decisión Marco 2002/475/JAI del Consejo, sobre la lucha contra el terrorismo, de 13 de junio de 2002[688], y la Decisión Marco 2002/584/JAI del Consejo, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros, de 13 de junio de 2002[689].

Asimismo, con ocasión del Consejo Europeo celebrado el 4 y 5 de noviembre de 2004 en La Haya fue adoptado el llamado Programa de la Haya[690], configurado como el reemplazo del Programa de Tampere y consistiendo en un programa plurianual en el que

---

686 Como se indica en el resumen oficial disponible en https://eur-lex.europa.eu/legal-content/ES/LSU/?uri=CELEX:12001C/TXT, fecha de consulta 27 de abril de 2022

687 Ante las reiteradas referencias a los atentados de Madrid y Londres como causa principal del cambio de rumbo en las políticas de la Unión Europea hacia el reforzamiento en materia de lucha contra el terrorismo, parece debido recordar que dichos actos terroristas se cometieron después de que fuera ejecutada la Operación Libertad Iraquí, previa Cumbre de las Azores celebrada el 16 de marzo en 2003 por los entonces Jefes de gobierno de Estados Unidos, Reino Unido, España y Portugal: George W. Bush, Tony Blair, José María Aznar y José Manuel Durão Barroso.

688 Decisión marco del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo, DOCE núm. L 164 de 22 de junio de 2022, pp. 3/7. Procedió a la armonización de la normativa penal en materia de terrorismo en los diferentes Estados miembros, estableciendo una lista común de conductas que deberían ser consideradas como delitos de terrorismo si perseguían ciertas finalidades (artículo 1), los delitos que podrían considerarse como relacionados con actividades terroristas (artículo 3), y las penas mínimas que deberían ser impuestas (artículo 5), entre otras medidas de armonización como los requisitos necesarios para disfrutar de una reducción de la pena o algunas disposiciones para proteger a las víctimas del terrorismo. Fue modificada posteriormente por la modificada posteriormente por la Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo, DOCE núm. L 330 de 9 de diciembre de 2008, pp. 21/23.

689 2002/584/JAI: Decisión Marco del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros, DOCE núm. L 190 de 18 de julio de 2002, pp. 1/20, disponible en que establecía un nuevo sistema para emitir y gestionar una orden de detención europea.

690 Programa de La Haya: 10 prioridades para los próximos cinco años, disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Al16002, fecha de consulta 28 de abril de 2022

se establecieron diez prioridades sobre las que la Unión Europea debía intensificar sus esfuerzos durante los cinco años siguientes. Entre dichos objetivos o prioridades podemos destacar la necesidad de promover y reforzar la protección y el respeto de los derechos fundamentales y de ciudadanía, la formación de la Agencia de Derechos Fundamentales de la UE (FRA, por sus siglas en inglés), sobre las bases del anterior Observatorio de Europeo del Racismo y la Xenofobia.

Es de destacar que, ya en este punto, se advertía de la necesidad de equilibrar la protección de la vida privada, de los datos personales, de la intimidad y demás derechos fundamentales con la posibilidad de que las distintas fuerzas y cuerpos de seguridad nacionales pudieran compartir de modo eficaz, entre sí o a través de la Oficina Europea de Policía (Europol), informaciones y datos en materia de lucha contra el terrorismo, así como de delincuencia transfronteriza[691].

De igual modo, en lo que refiere al principio de reconocimiento mutuo, lo cierto es que el Programa de la Haya vino en reafirmar, respecto de la justicia penal, la necesidad de aproximar las legislaciones con normas procesales mínimas de aplicación eficiente y oportuna, con la consiguiente sustitución de "la ayuda mutua tradicional por instrumentos nuevos basados en el reconocimiento mutuo" (prioridad 9), llegando a concluir que "la consecución del reconocimiento mutuo –como piedra angular de la cooperación judicial- supone la definición de normas equivalentes aplicables a los derechos procesales en los procesos penales"..

También es necesario señalar las Decisiones 2008/615/JAI[692], 2008/616/JAI[693] y 2009/905/JAI[694], que incluyeron en el ámbito de la Unión Europea el contenido del Tratado de Prüm[695], celebrado el 27 de mayo de 2005 entre Austria, Alemania, Bélgica,

---

691 REMOTTI CARBONELL, J. C., "El proceso de formación del espacio de libertad, seguridad y justicia en la Unión Europea. La lucha contra la delincuencia, cooperación policial y judicial y garantías del debido proceso en el ámbito penal", cit., p. 50.

692 Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza DOCE núm. L 210 de 6 de agosto de 2008, pp. 1/11.

693 Decisión 2008/616/JAI del Consejo, de 23 de junio de 2008, relativa a la ejecución de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, DOCE núm. L 210 de 6 de agosto de 2008, pp. 12/72.

694 Decisión marco 2009/905/JAI del Consejo, de 30 de noviembre de 2009, sobre acreditación de prestadores de servicios forenses que llevan a cabo actividades de laboratorio, DOCe núm. L 322 de 9 de diciembre de 2009, pp. 14-16.

695 Convención entre el Reino de Bélgica, la República Federal de Alemania, el Reino de España, la República Francesa, el Gran Ducado de Luxemburgo, el Reino de Holanda y la República de Austria sobre la

España, Francia, Luxemburgo y Holanda, a los que se adhirieron posteriormente Italia, Finlandia, Portugal y Eslovenia. Con estas decisiones, se intensificó la cooperación para luchar con mayor eficacia contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, estableciendo un intercambio de información mejorado en materia de huellas dactilares, ADN y matrículas de vehículos.

Debe recordarse que el Tratado de Prüm señalaba en su preámbulo que "es importante que los Estados miembros de la UE intensifiquen su cooperación para luchar con mayor eficacia contra el terrorismo, la delincuencia transfronteriza y la inmigración ilegal" y estableció como objetivo "sumir un papel pionero en la consecución del máximo nivel posible de cooperación, en aras del desarrollo de la cooperación europea y sin perjuicio del Tratado de la Unión Europea y del Tratado constitutivo de la Comunidad Europea» ofreciendo «la posibilidad de participar en esta cooperación a todos los demás Estados miembros de la Unión Europea"[696]. Entre las medidas adoptadas, destacaban la transmisión de información para la prevención de atentados terroristas (art. 16), la posibilidad de que los vuelos lleven escoltas armados (art. 17), la posibilidad de realizar patrullas conjuntas entre varios Estados (art. 24), y la autorización para que las fuerzas policiales nacionales puedan cruzar las fronteras en caso de peligro inminente o constatación de flagrancia (art. 25).

h) El Tratado de Lisboa

Con la firma del Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea el 13 de diciembre de 2007 en la ciudad de Lisboa[697], y que entraron en vigor conjuntamente el 1 de diciembre de 2009, se persigue conseguir que la Unión Europea sea más democrática, más eficiente y se encuentre mejor capacitada para abordar, con una sola voz, los problemas globales de la actualidad.

En lo que interesa a este trabajo, con el Tratado de Lisboa se consolida la voluntad manifestada por la Unión Europea en el Tratado de Maastricht de formar un espacio de

---

intensificación de cooperación transfronteriza, en particular en la lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, también conocido como Acuerdo de Schengen III, por el que los signatarios, bajo la fórmula de la cooperación reforzada acordaban intercambiar datos sobre ADN, huellas dactilares y registro de vehículos de las personas de interés y cooperar contra el terrorismo.

[696] REMOTTI CARBONELL, J. C., "Las medidas contra el terrorismo en el marco del Tratado de Prüm", *Revista de derecho constitucional europeo*, 7, 2007, Instituto Andaluz de Administración Pública, p. 188.

[697] Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea, firmado en Lisboa el 13 de diciembre de 2007, DOUE núm. C 306, de 17 de diciembre de 2007, pp. 1-231.

libertad, seguridad y justicia. De hecho, el ELSJ aparece como un objetivo de la UE en el párrafo 2 del artículo 3 del TUE, al establecer que "la Unión ofrecerá a sus ciudadanos un espacio de libertad, seguridad y justicia sin fronteras interiores, en el que esté garantizada la libre circulación de personas conjuntamente con medidas adecuadas en materia de control de las fronteras exteriores, asilo, inmigración y de prevención y lucha contra la delincuencia".

Prueba de lo anterior es, también, que el ELSJ da nombre al Título V del TFUE, (artículos 67 a 89), el cual establece cuatro grandes grupos de competencias: políticas sobre controles en las fronteras, asilo e inmigración (Cap. II); cooperación judicial en materia civil (Cap. III); cooperación judicial en materia penal (Cap. IV), y cooperación policial (Cap. V).

Los objetivos asignados al ELSJ se concretan en el artículo 67 del TFUE: i) construir un espacio de libertad, seguridad y justicia dentro del respeto de los derechos fundamentales y de los distintos sistemas y tradiciones jurídicos de los Estados miembros; ii) garantizar la ausencia de controles de las personas en las fronteras interiores y desarrollar una política común de asilo, inmigración y control de las fronteras exteriores que esté basada en la solidaridad entre Estados miembros y sea equitativa respecto de los nacionales de terceros países; iii) garantizar un nivel elevado de seguridad mediante medidas de prevención de la delincuencia, el racismo y la xenofobia y de lucha en contra de ellos, medidas de coordinación y cooperación entre autoridades policiales y judiciales y otras autoridades competentes, así como mediante el reconocimiento mutuo de las resoluciones judiciales en materia penal y, si es necesario, mediante la aproximación de las legislaciones penales; y iv) facilitar la tutela judicial, garantizando en especial el principio de reconocimiento mutuo de las resoluciones judiciales y extrajudiciales en materia civil.

Asimismo, debemos destacar especialmente que las medidas que pueda adoptar la Unión Europea en el ejercicio de tales competencias serán de coordinación y de cooperación entre autoridades policiales y judiciales y otras autoridades competentes (art. 63.3). De igual modo, la aproximación de los ordenamientos jurídicos de los diferentes Estados miembros, la cooperación judicial o policial en materia penal, y la cooperación en

sistemas de información se erigen como herramientas fundamentales para el desarrollo de dicho espacio de libertad, seguridad y justicia [698].

En materia de cooperación judicial, se prevé la posibilidad de adoptar medidas que incluyan la aproximación de las disposiciones legales de los Estados miembros en determinados delitos cuando tengan especial gravedad y dimensión transfronteriza (art. 82.3 y 83 TFUE). Dichos delitos son los actos terroristas, la trata de seres humanos, la explotación sexual de mujeres y niños, el tráfico ilícito de drogas, el tráfico ilícito de armas, el blanqueo de capitales, la corrupción, la falsificación de medios de pago, la delincuencia informática y la delincuencia organizada. De igual modo, también se establece la posibilidad de que la Unión Europea adopte medidas que impliquen el establecimiento de normas y procedimientos para garantizar el reconocimiento en toda la Unión Europea de las sentencias y resoluciones judiciales de los Estados miembros.

En materia de cooperación policial, se prevé la posibilidad de adoptar medidas en relación con la recogida, almacenamiento, tratamiento, análisis e intercambio de información pertinente; el apoyo a la formación de personal, así como la cooperación para el intercambio de personal, los equipos y la investigación científica policial[699]; y las técnicas comunes de investigación relacionadas con la detección de formas graves de delincuencia organizada. Asimismo, se establece que las medidas de cooperación policial deberán ser adoptadas por unanimidad del Consejo previa consulta al Parlamento, dejando a salvo la vía de la cooperación reforzada si no se alcanzan dichos mínimos[700]. También se refuerza la estructura y finalidad de Europol (delegando en reglamentos posteriores la determinación de su estructura, ámbito de actuación y competencias concretas) y se crea un comité permanente de cooperación operativa entre los diferentes cuerpos policiales de los Estados miembros (art. 87.3 TFUE).

Por último, debemos hacer mención también al denominado Programa de Estocolmo, adoptado por el Consejo Europeo el 2 de diciembre de 2009, y que establecía un

---

[698] REMOTTI CARBONELL, J. C., "El proceso de formación del espacio de libertad, seguridad y justicia en la Unión Europea. La lucha contra la delincuencia, cooperación policial y judicial y garantías del debido proceso en el ámbito penal", cit., p. 952.

[699] PÉREZ FRANCESCH, J. L., "El tratado de Lisboa: cooperación policial y judicial entre la europeización y las reservas estatales", en *Diálogos y desafíos euro-latinoamericanos: ensayos sobre cooperación derecho, educación y comunicación*, Ediciones Uninorte, 2010, pp. 80-111, esp. p..82, en https://dialnet.unirioja.es/servlet/articulo?codigo=4409625, fecha de consulta 28 abril 2022.

[700] REMOTTI CARBONELL, J. C., "El proceso de formación del espacio de libertad, seguridad y justicia en la Unión Europea. La lucha contra la delincuencia, cooperación policial y judicial y garantías del debido proceso en el ámbito penal", cit., p. 51.

plan quinquenal para determinar las acciones siguientes de la Unión Europea entre los años 2010 y 2015[701].

~~En materia de~~ Para reforzar la confianza mutua entre los distintos Estados, uno de los objetivos fue potenciar la formación común de magistrados, fiscales y personal judicial en general, valorándose la necesidad de desarrollar redes comunes de contactos entre magistrados, fiscales altos funcionarios tales como jefes superiores de policía, los directores y jefes de los centros de formación.

En materia de seguridad interior, se estableció como función prioritaria del Comité permanente de Cooperación operativa (COSI) el desarrollo supervisión y aplicación de la Estrategia de seguridad interior; la formación de una cultura común policial europea a partir del intercambio de experiencias y buenas prácticas, la formación y ejercicios conjuntos; la creación del modelo común que simplifique y facilite el intercambio de información e inteligencia entre los cuerpos y servicios de seguridad de los Estados miembros; la modernización de las herramientas tecnológicas que permitan alcanzar los máximos niveles de seguridad en las redes así como de la información a través de la prevención, preparación y recuperación de las infraestructuras críticas frente a los ciberataques.

En materia de cooperación policial, se buscaron nuevas herramientas para el traslado y la distribución de la información vía Europol; mejorar la cooperación operativa a través de sistemas de comunicación compatibles entre los distintos cuerpos de policía, así como regular e intensificar el uso de agentes infiltrados; posibilitar el intercambio de información entre las agencias de la Unión Europea Europol, Eurojust y Frontex.

B. La institucionalización de la cooperación policial europea

La cooperación policial en el ámbito de la Unión Europa tiene su máximo representante en la figura de la Agencia de la Unión Europea para la Cooperación Policial (conocida como Europol), que supone la institucionalización definitiva del objetivo de la cooperación policial establecido en los artículos 87, 88 y 89 del Tratado de Funcionamiento de la Unión Europea[702].

---

[701] ARIAS RODRÍGUEZ, J. M., "El Programa de Estocolmo", *Diario La Ley*, 7812, 2012, Wolters Kluwer, p. 1.

[702] Versión consolidada del Tratado de Funcionamiento de la Unión Europea, DOUE núm. C 326 de 26 de octubre de 2012, pp. 47/390.

Paralelamente, han sido creados otros organismos que también sirven al objetivo de la cooperación policial, y sobre los que nos detendremos en este apartado.

a) La "Unidad de Drogas de Europol"

Los antecedentes directos de la oficina europea de policía se encuentran en la llamada "Unidad de Drogas de Europol" (UDE, en adelante), que inició su funcionamiento en enero de 1994[703]. La UDE fue creada antes que la propia Europol en su conjunto (referida como "Oficina Europea de Policía") precisamente con la idea de que sirviera como primera fase para preparar el establecimiento completo de dicha institución[704].

La creación de la "Unidad de Drogas de Europol" tuvo lugar con el acuerdo ministerial para el establecimiento de la Unidad de drogas de Europol, celebrado en Copenhague, el 2 de junio de 1993[705], aunque no iniciara sus actuaciones hasta más adelante, en enero de 1994.

Posteriormente, con la Acción Común de 10 de marzo de 1995, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea relativo a la Unidad de Drogas de Europol[706], los Estados miembros establecieron de manera concreta los objetivos, la estructura y el funcionamiento de la UDE. Asimismo, mediante la Acción Común de 16 de diciembre de 1996[707], adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea relativo a la Unidad de Drogas de Europol, se amplió el ámbito material de la Unidad, pasando a incluir el tráfico de sustancias nucleares y radioactivas, las redes de migraciones clandestinas, el tráfico de personas y el de

---

[703] En la propia Acción Común de 10 de marzo de 1995, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea relativo a la Unidad de Drogas de Europol (DOCE núm. L 62 de 20 de marzo de 1995, pp.1-3), se deja constancia de que la Unidad de Drogas de Europol fue creada mediante acuerdo ministerial de 2 de junio de 1993 y que la misma funciona desde enero de 1994.

[704] Por otra parte, resulta lógico desde la perspectiva de la estrategia *step by step*. A este respecto, cabe señalar que el ámbito de las drogas fue el único en el que se pudo llegar al mínimo de acuerdo necesario para poner en marcha tal unidad. En el resto de las materias, como el terrorismo, aún no existía la confianza necesaria entre los funcionarios de los diferentes Estados miembro, como destaca JIMÉNEZ SÁNCHEZ, F., "Europol: cooperación y coordinación policial en la Unión Europea", 2015, Universidad Carlos III de Madrid, p. 88, fecha de consulta 2 mayo 2022, en https://dialnet.unirioja.es/servlet/tesis?codigo=95085.

[705]Acuerdo ministerial para el establecimiento de la Unidad de drogas de Europol, celebrado en Copenhague, el 2 de junio de 1993. DOCE núm. DO L 62 de 20.31995.

[706] Acción Común 95/73/JAI, de 10 de marzo de 1995, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea relativo a la Unidad de Drogas de Europol, DOCE núm. L 62 de 20 de marzo de 1995, pp.1-3.

[707] Acción Común de 16 de diciembre de 1996, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea relativo a la Unidad de Drogas de Europol. DOCE núm. L 342 de 31 de diciembre de 1996, p.1.

vehículos (artículo 1). También, mediante la Acción común 96/747/JAI, de 29 de noviembre[708], se añadió como misión de la UDE la creación de un directorio relativo a las competencias, los conocimientos y las técnicas especializados en materia de lucha contra la delincuencia que fueran de su competencia. Dicho directorio se elaboraba y actualizaba a partir de las contribuciones de los Estados miembros y era gestionado por la UDE.

El objetivo era constituir una institución que sirviera como instrumento para el intercambio y análisis de información en relación con delitos de tráfico ilícito de drogas, incluyendo la vigilancia de organizaciones criminales dedicadas a dicho ámbito y de las actividades de blanqueo de capitales, siempre que afectasen, al menos, a dos Estados miembros. En ese sentido, hay que destacar que las funciones únicamente eran de intercambio de información (incluyendo información personal) y de preparación de informes de inteligencia a partir de información no personal. Se trataba, en síntesis, de un equipo destinado a funciones de apoyo de las agencias de seguridad nacionales, de intercambio de datos y de elaboración de inteligencia[709].

En consecuencia, la UDE carecía de toda capacidad de despliegue o facultad para intervenir de manera directa en las investigaciones, debiendo en este caso remitirse a las actuaciones materiales que podrían realizar los cuerpos policiales de los Estados miembros.

No podemos dejar de mencionar que, a pesar de contar como antecedente directo al grupo de Trevi, en el ámbito de los Estados miembros se apreciaba cierta desconfianza inicial por parte de las agencias nacionales (e, incluso, de las propias instituciones europeas, como se puso de manifiesto con ocasión del Reporte Anual de 1996[710]) hacia la

---

[708] Acción común 96/747/JAI de 29 de noviembre de 1996 adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea, relativa a la creación y mantenimiento de un Directorio de competencias, conocimientos y técnicas especializados en materia de lucha contra la delincuencia organizada internacional con el fin de facilitar la cooperación entre los Estados miembros de la Unión Europea para garantizar el cumplimiento de la ley (DOCE núm. L 342 de 31 de diciembre de 1996, p. 2).

[709] Modesto García, diría "No es todavía el FBI europeo, no es un cuerpo con competencias directas en el territorio de los Quince, sino que actúa a través de las policías nacionales; es una Interpol europea mejorada" y Jurgen Storbeck diría también "es un servicio de inteligencia, pues analiza los datos, sigue las investigaciones nacionales y coordina la desarticulación de las organizaciones criminales", todos en VIDAL-FOLCH, X., "Europol, más que Interpol, menos que el FBI", El País, 1996, Madrid, fecha de consulta 2 mayo 2022, en https://elpais.com/diario/1996/07/14/internacional/837295206_850215.html.

[710] Disponible en https://www.europarl.europa.eu/doceo/document/A-4-1998-0305_EN.html?redirect, fecha de consulta 2 de mayo de 2022, en el que los eurodiputados llegaron a manifestar que era inadecuado por la poca información que contenía.

UDE. Sin embargo, este inicial recelo desaparecería ante la evidente utilidad de sus funciones.

La estructura de la UDE estaba basada en tres niveles, similar a la del grupo de Trevi. Estaba dirigida por un coordinador general, que podía contar, como máximo, con dos coordinadores adjuntos y otros dos miembros jerárquicamente dependientes. Este equipo directivo era el responsable del mantenimiento del funcionamiento ordinario de la Unidad[711].

Paralelamente, la estructura quedaba completada con la figura de los funcionarios de enlace, que eran nombrados por las agencias nacionales de cada Estado miembro y que respondían ante los órganos nacionales. Los funcionarios de enlace eran el canal contemplado para efectuar el intercambio de información y datos (incluidos los personales) entre los Estados Miembro. Contaban con acceso a toda la información y datos de las agencias de seguridad de su ordenamiento y tenían capacidad para localizar y, en su caso, entregar o denegar la información solicitada. En el intercambio de información y datos, un aspecto fundamental era el cumplimiento de las leyes nacionales. Los funcionarios de enlace eran los encargados de supervisar el ajuste de las transferencias a los marcos normativos. Para el traslado de la información era necesario que se cumplieran las leyes del Estado solicitante y del receptor, así como las condiciones que alguno de los dos participantes pusiera a la información o datos, ya que en algunos casos dicha información podía ser sensible, por tratarse de investigaciones en proceso o datos personales[712]. Junto a la información y datos sobre investigaciones penales, dichos funcionarios eran los encargados de elaborar los informes de situación y de análisis criminal con base en información (no personal) suministrada por los gobiernos a los que representaban.

A continuación, una vez que se efectuaba la solicitud entre los oficiales de enlace, estos se dirigían a las Unidades Nacionales, que eran los equipos en los que se centralizaba la cooperación internacional. La diversidad de estructuras policiales en los Estados miembro obligaba a tener un área que pudiera buscar en todos los archivos policiales la información o datos solicitados. Por ello se crearon Unidades Nacionales, con competencias para para gestionar en los órganos nacionales las solicitudes de información. De esta

---

[711] Como se indica en el artículo 5.1 de la Acción Común de 10 de marzo de 1995, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea relativo a la Unidad de Drogas de Europol, DOCE núm. L 62 de 20 de marzo de 1995, pp.1-3.
[712] JIMÉNEZ SÁNCHEZ, F., "Europol", cit., p. 93.

manera, las Unidades Nacionales, sin ser parte de la estructura orgánica de la Unidad de Drogas de Europol, pertenecían a la arquitectura del sistema de cooperación policial ya que eran un elemento sustancial para la localización de la información y datos necesarios[713].

De esta forma, se puede dibujar el siguiente esquema del funcionamiento de la UDE en aquél momento: a partir de una investigación policial de una agencia de seguridad nacional, el funcionario encargado solicitaba a la Unidad Nacional que enviara una solicitud de información al funcionario de enlace (desplegado en la Unidad de Drogas de Europol), para que revisara el cumplimiento normativo y, en su caso, la entregara a su par de otro Estado Miembro, para que diera nueva cuenta, revisara el cumplimiento normativo y en su caso la enviara a su respectiva Unidad Nacional para la localización de la información o datos en las agencias de seguridad de su Estado. Una vez que se obtenía respuesta a la solicitud, se efectuaba el procedimiento en sentido inverso para que regresara al funcionario a cargo de la investigación que inició la solicitud de información y datos[714].

Como se puede comprobar, el equipo directivo era muy reducido, con un máximo de cinco miembros (un coordinador general, dos coordinadores adjuntos y dos miembros adicionales opcionales), destacando frente a los cuarenta funcionarios de enlace[715] que, para 1996, figuraban como parte de la Unidad, lo que ha servido para evidenciar que la principal actividad de la Unidad era la transmisión de información entre las diferentes agencias nacionales de seguridad[716]. De hecho, el número de solicitudes de información y datos a partir del sistema de funcionarios de enlace fue en crecimiento desde su inicio. En el primer año de funcionamiento de la Unidad, 1994, los Estados miembro acudieron a ella en 585 ocasiones. Para el año siguiente el número creció en un 152% para llegar a

---

[713] Como se indica en el artículo 3.2 de la Acción Común de 10 de marzo de 1995, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea relativo a la Unidad de Drogas de Europol (https://op.europa.eu/de/publication-detail/-/publication/cff5ec9e-3ace-4a0d-9406-ead68198e259/language-es, fecha de consulta 30 de abril de 2022

[714] En 1996, el coordinador general Jürgen Storbeck explicó de la siguiente forma el funcionamiento de la UDE: "la policía de Colonia (Alemania) pide información del historial de un narcotraficante a los otros países, a través de los oficiales de enlace. Éstos se reúnen y discuten. Cada uno examina su fichero nacional o consulta a la unidad nacional, su policía judicial. En tres o cuatro horas se acopia toda la información y se le suministra a Colonia. Mientras tanto, se analiza, se establecen hipótesis probables, se coordina una operación. Y todo acaba en la desarticulación de una red mediante una entrega controlada", en la noticia que se reseña en la nota siguiente.

[715] VIDAL-FOLCH, X., "Europol, más que Interpol, menos que el FBI", *El País*, 1996, Madrid, fecha de consulta 2 mayo 2022, en https://elpais.com/diario/1996/07/14/internacional/837295206_850215.html.

[716] JIMÉNEZ SÁNCHEZ, F., "Europol", cit., p. 95.

las 1.474 solicitudes. En 1996 prosiguió con un aumento del 39% para llegar a las 2.053 solicitudes[717].

b) El "Convenio Europol" y sus posteriores enmiendas

La Oficina Europea de Policía (Europol) fue constituida mediante el Convenio[718] basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía (Convenio Europol), hecho en Bruselas el 26 de julio de 1995[719]. No obstante, Europol no comenzó a funcionar en dicha fecha, pues era necesario que cada Estado miembro ratificase el convenio de acuerdo con sus respectivas normas constitucionales, previa aprobación por el órgano legislativo correspondiente. De esta manera, el Convenio entró en vigor el 1 de octubre de 1998 y no se aplicó de forma efectiva hasta el 1 de julio de 1993, fecha en la que oficialmente Europol inició su actividad, sustituyendo[720] en ese momento a la Unidad de "Drogas" Europol (UDE), creada provisionalmente en 1995[721].

Debe recordarse que la creación de una Oficina Europea de Policía era una previsión establecida en el Tratado de Maastricht de 7 de febrero de 1992, al que ya nos hemos referido, y que, a su vez, era consecuencia de la propuesta alemana presentada en el Consejo Europeo de Luxemburgo de los días 28 y 29 de junio de 1991[722]. De esta manera, supuso la institucionalización de las actuaciones de cooperación de las fuerzas de policía

---

[717] Como se puede comprobar en el informe del Parlamento Europeo de 4 de septiembre de 1998, disponible en https://www.europarl.europa.eu/doceo/document/A-4-1998-0305_EN.html?redirect, fecha de consulta de 2 de mayo de 2022.

[718] En el Tratado de Maastricht se contemplaban tres instrumentos legales: convenciones, acciones y posiciones. Asimismo, en el artículo K.3-C de dicho Tratado se estableció que el Consejo era el encargado de redactar convenciones y de adoptarlas. Conforme a dicho marco legal, se elaboró el denominado "Convenio Europol" que ahora reseñamos, y que tuvo que ser ratificado por los parlamentos nacionales de los Estados miembros.

[719] Convenio basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía (Convenio Europol), hecho en Bruselas el 26 de julio de 1995, DOCE núm. C 316, de 27 de noviembre de 1995, pp. 1-33.

[720] Heredaría la estructura de la DUE, en el sentido de que se podrían distinguir los siguientes elementos organizativos: la unidad central como centro aglutinador de información y datos de interés común en la lucha contra la delincuencia en materias que sean competencia de Europol, las unidades nacionales, que sirven para facilitar el contacto con el conjunto de servicios policiales nacionales y que eran creadas por cada Estado miembro, y los funcionarios de enlace, enviados por cada unidad nacional a la unidad central con objeto de ejecutar las tareas de coordinación, petición y entrega de información.

[721] GOIZUETA VÉRTIZ, J., "La cooperación policial en el seno de Europol: el principio de disponibilidad y la confidencialidad de la información", *Revista española de derecho constitucional*, vol. 37, 110, 2017, Centro de Estudios Políticos y Constitucionales (España), p. 79.

[722] CASTILLEJO MANZANARES, R., "Europol y las investigaciones transfronterizas", *Dereito: Revista xuridica da Universidade de Santiago de Compostela*, vol. 17, 2, 2008, Servicio de Publicaciones = Servizo de Publicacións, p. 2.

de los Estados miembros. El Convenio fue preparado por un grupo especial de la UDE y no fue sometido a puntos de vista de expertos externos ni políticos, sino que, cuando fue adoptado por el Consejo Europeo, quedó pendiente de la ratificación por parte de los parlamentos nacionales, que solamente podían aceptarlo o rechazarlo[723]. Este proceso determinó, como hemos señalado, que el Convenio no entrara en vigor hasta el 1 de octubre de 1998, algo más de tres años después de su adopción por el Consejo.

Su misión continuaba siendo la de mejorar la eficacia y la cooperación de los servicios competentes de los Estados miembros, con el fin de prevenir y luchar eficazmente contra la delincuencia organizada internacional. La Oficina Europea de Policía (Europol) no tenía reconocidos poderes ejecutivos como los servicios de policía de los Estados miembros, por lo que no puede ni detener a individuos, ni registrar domicilios. Europol está encargada, por tanto, de facilitar el intercambio de información, analizar la inteligencia y coordinar las operaciones de investigación penal entre los Estados miembros[724].

No obstante, la institución acumuló más funciones además de gestionar el intercambio de información y datos entre los Estados miembro, ya que se le asignó la tarea de generar inteligencia común que sirviera para que la policía de los diferentes Estados miembros pudieran mejorar sus respuestas frente a la criminalidad[725], y también se ha destacado la utilidad de la Convención para dar oficialidad a la cooperación entre los cuerpos policiales de los Estados miembros, de manera que tales informaciones pudieran constituir evidencias utilizables en sede judicial[726].

Además de los ámbitos competenciales referidos, mediante la Decisión del Consejo de 3 de diciembre de 1998[727] se amplió el ámbito material de Europol a los actos terroristas contra la vida, la integridad física, la libertad o bienes jurídicos de naturaleza

---

[723] JIMÉNEZ SÁNCHEZ, F., "Europol", cit., p. 103.
[724] Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:l14005b, fecha de consulta 3 de mayo de 2022.
[725] El artículo 3 de la Convención distingue tres grupos de funciones. El primer grupo, de máxima prioridad, se equipara con el que venía desempeñando la UDE, consistente en facilitar el intercambio de información entre Estados miembros; el segundo grupo, de prioridad intermedia, consistía en profundizar en conocimientos especializados, facilitar datos estratégicos y elaborar informes de inteligencia; el tercer grupo, de inferior prioridad, encargaba a la institución labores de formación y asesoramiento de los servicios policiales nacionales.
[726] LEBEUF, M.-E., "Organized Crime and Police Cooperation in the European Union: Lessons Learned, an Interview with Professor Cyrille Fijnaut", *Trends in Organized Crime*, vol. 7, 4, 2004.
[727] Decisión del consejo, de 3 de diciembre de 1998, por la que se encomienda a Europol la lucha contra los delitos cometidos o que puedan cometerse en el marco de actividades terroristas que atenten contra la vida, la integridad física, la libertad o los bienes de las personas, DOCE núm. C 26 de 4 de junio de 1999, p. 1.

patrimonial. También se redefinió el concepto de trata de seres humanos y, finalmente, se incluyó entre sus atribuciones la protección del euro, al designarse a Europol como Oficinal Central para la Lucha contra la Falsificación del euro[728].

De igual modo, durante los años siguientes, fueron aprobados varios Protocolos que introdujeron enmiendas al régimen establecido en el Convenio[729], con el objeto de reforzar los poderes de Europol en su actividad de apoyo a los Estados miembros, permitiéndole, en particular, coordinar equipos de investigación comunes, pedir la apertura de una investigación, permitir la participación de terceros Estados (con los que Europol haya celebrado acuerdos operativos) en los grupos de análisis, etc.

De esta forma, y atendiendo al contenido de la Convención y las posteriores enmiendas, podemos decir que, en el marco de la cooperación policial entre los Estados miembros, Europol facilita el intercambio de información; reúne y analiza la información y los datos; comunica a los servicios competentes de los Estados miembros, por medio de las unidades nacionales, la información que les concierne y las posibles relaciones o vínculos entre actos delictivos; facilita las investigaciones en los Estados miembros; gestiona la recopilación de información informatizada; asiste a los Estados miembros en la formación de sus autoridades competentes; facilita apoyo técnico entre los Estados miembros; constituye el punto de contacto en materia de represión de la falsificación del euro.

Asimismo, también se amplía el ámbito material de Europol, que engloba ámbitos cada vez más numerosos, como: la prevención y la lucha contra el terrorismo; el tráfico de drogas; el tráfico de seres humanos; las redes de inmigración clandestina; el tráfico ilícito de materias radiactivas y nucleares; el tráfico de vehículos robados; la lucha contra la acuñación de monedas falsas y la falsificación de medios de pago; el blanqueo de dinero (excepto infracciones primarias). La competencia de Europol incluye las infracciones conexas, entendiéndose como tales aquellos delitos cometidos para procurarse los medios para perpetrar los actos para los que Europol sea competente, los cometidos para

---

[728] Decisión 2005/511/JAI del consejo de 12 de julio de 2005 relativa a la protección del euro contra la falsificación mediante la designación de Europol como organismo central para la lucha contra la falsificación del euro, DOCE núm. L 185, de 16 de julio de 2005, pp1-2.

[729] Primero, el convenio fue complementado por dos protocolos firmados el 24 de julio de 1996 y el 19 de junio de 1997 (publicados en el DOCE núm. C 299, de 9 de octubre de 1996, y en el DOCE núm. C 221, de 19 de julio de 1997, respectivamente) y, posteriormente, fue modificado por otros tres protocolos firmados el 30 de noviembre de 2000 (DOCE núm. C 358, de 13 de diciembre de 2000), el 28 de noviembre de 2002 (DOCE núm. 312, de 16 de diciembre de 2002) y el 27 de noviembre de 2003 (DOCE núm. de 6 de enero de 2004).

facilitar o consumar la ejecución de los actos para los que Europol sea competente y los perpetrados para conseguir la impunidad de los actos para los que la Agencia sea competente[730].

Cada Estado miembro creará o designará una unidad nacional Europol (UNE), que será el único órgano de enlace entre Europol y los servicios nacionales competentes. Dicha unidad enviará a Europol al menos ~~a~~ un funcionario de enlace encargado de representar sus intereses ante el órgano. Los jefes de las unidades nacionales se reunirán periódicamente. La unidad nacional se ocupará, entre otras cosas, de proporcionar a Europol la información y los datos que necesite para cumplir su misión y, en particular, garantizar la alimentación del sistema de información de Europol; responder a y enviar solicitudes de información a Europol; difundir a los servicios competentes la información suministrada por Europol. La UNE constituía la representación de los Estados en Europol y el punto operativo de aquellos en este órgano. No obstante, las modificaciones introducidas por el Protocolo de noviembre de 2003 en el Convenio Europol permitirían los contactos directos entre los servicios competentes de los Estados miembros y Europol, si bien, la UNE debía ser informada expresamente cada vez que se producía algunos de aquellos contactos.

c) Europol como agencia de la Unión Europea

Con el desarrollo de las funciones encomendadas a Europol tras la entrada en vigor del Convenio de 26 de julio de 1995 se pusieron de manifiesto, para los Estados miembros, dos cuestiones de trascendental importancia. La primera, la utilidad de la propia Europol, como institución dedicada a la coordinación europea de los esfuerzos policiales nacionales[731] ~~,~~ en la lucha contra la delincuencia internacional; la segunda, la necesidad de reformar el régimen jurídico del propio órgano, de manera que se redujera el componente burocrático[732] de su funcionamiento y, simultáneamente, se facilitase la

[730] GOIZUETA VÉRTIZ, J., "La cooperación policial en el seno de Europol", cit., p. 85.
[731] En el primer año de funcionamiento de la UDE, 1994, los Estados miembro acudieron a ella en 585 ocasiones. Para el año siguiente el número creció en un 152% para llegar a las 1.474 solicitudes. En 1996 prosiguió con un aumento del 39% para llegar a las 2.053 solicitudes.
[732] Como indica CASTILLEJO MANZANARES, R., "Europol y las investigaciones transfronterizas", cit., p. 93, todas las decisiones que adoptara el Director tenían que ser aprobadas unánimemente por los 27 Estados miembros de la UE, y se apreciaba una importante parálisis en el funcionamiento de la estructura, compuesta por la unidad central, las unidades nacionales y los funcionarios de enlace, así como en el sistema de información (que, a su vez, constaba de tres elementos: el sistema de información, los ficheros de trabajo y un sistema de índice).

introducción de las modificaciones que resultasen necesarias para la consecución de sus fines y la fiscalización de sus actividades.

Con dicho objetivo fue adoptada la Decisión del Consejo de 6 de abril de 2009, por la que se acordaba la creación de la Oficina Europea de Policía (Europol)[733], y que entró en vigor el 1 de enero de 2010, derogando el Convenio Europol y todas sus posteriores modificaciones.

Sin entrar en excesivo detalle[734], debemos señalar que con la Decisión 2009/371/JAI se creaba una Oficina Europea de Policía, con sede en La Haya, sucesora legal de la Europol creada por el Convenio Europol, con personalidad jurídica propia y condición de entidad de la Unión, sujeta a las normas y procedimientos generales de organismos y agencias similares, simplificando así su administración. Al mismo tiempo, Europol recibe financiación del presupuesto general de la UE, quedando bajo el control presupuestario del Parlamento Europeo[735].

Es responsable en situaciones en las que los países de la UE necesitan apoyo para abordar la delincuencia, el terrorismo y otras formas de delincuencia transfronteriza que afectan los intereses de la UE.

Las principales funciones de Europol son: recoger, almacenar, tratar, analizar e intercambiar información, comunicar a los países de la UE las relaciones entre los actos delictivos que les afecten, asistir a los países de la UE en las investigaciones y proporcionar apoyo en materia de análisis e información, coordinar, organizar y aplicar investigaciones y operaciones para apoyar o reforzar las acciones de los las fuerzas y cuerpos de seguridad de los países de la UE, solicitar a los países de la UE que inicien, realicen o coordinen investigaciones en casos específicos y sugerir la creación de equipos conjuntos de investigación, apoyar a los países de la UE en materia de prevención y lucha contra formas de delincuencia facilitadas, fomentadas o cometidas a través de internet, redactar evaluaciones de amenazas y otros informes. Actúa, asimismo, como la oficina central

[733] Decisión 2009/371/JAI del Consejo, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol) DOUE núm. L 121 de 15 de mayo de 2009, pp. 37/66.
[734] Pues, como se verá, esta regulación ya no se encuentra vigente.
[735] Hasta entonces, Europol se financiaba mediante las contribuciones de los Estados miembros. Las cuentas relativas a todos los ingresos y gastos consignados en el presupuesto, así como el balance de los elementos activos y pasivos de Europol, son sometidas a control anual. El presupuesto provisional y la ejecución presupuestaria son objeto de examen por el Consejo.

para luchar contra la falsificación del euro basándose en la Decisión 2005/511/JAI del Consejo.

En general, la comparación de funciones entre el artículo 3 del Convenio Europol y el artículo 5 de la Decisión 2009/371/JAI del Consejo evidencia una ampliación de los objetivos principales de la institución. Con la entrada en vigor de esta última, se aprecia que el espectro de acción de Europol resulta ampliado, extendiéndose desde el intercambio de información a funciones de inteligencia para la prevención de la criminalidad, elaborando informes y guías especializadas en la materia a partir de la información de que dispone.

En cuestiones de la incumbencia de Europol, su personal puede participar en equipos conjuntos de investigación; sin embargo, solo puede actuar en calidad de apoyo y no puede adoptar en ninguna medida coercitiva.

Asimismo, con la Decisión 2009/371/JAI se ampliaron los métodos de elaboración de documentos de inteligencia, se previó la posibilidad de que Europol propusiera la realización y coordinación de actuación de investigaciones, y la creación de equipos conjuntos de investigación (en los que únicamente podría intervenir como apoyo)[736].

El contacto entre Europol y la autoridad competente de un Estado se realiza a través de una unidad nacional designada. No obstante, de acuerdo con las condiciones establecidas por el Estado pueden permitirse el contacto directo con sus autoridades nacionales.

Europol puede tratar información y datos, incluidos datos personales, en el desempeño de sus funciones. Con este propósito, se ha creado un sistema de información de Europol y ficheros de trabajo de análisis. Las unidades nacionales, los funcionarios de enlace y el personal de Europol pueden introducir y recuperar datos directamente del sistema. Las autoridades competentes designadas de los países de la UE solamente pueden realizar una búsqueda en el sistema para cerciorarse de que los datos que necesitan están disponibles.

Europol puede cooperar con otros organismos de la UE en el desempeño de sus funciones, especialmente con la Unidad Europea de Cooperación Judicial (Eurojust) y la

[736] JIMÉNEZ SÁNCHEZ, F., "Europol", cit., p. 106.

Oficina Europea de Lucha contra el Fraude (OLAF). Europol también puede cooperar con países y organizaciones de fuera de la UE, incluida la Organización Internacional de Policía Criminal (Interpol).

Finalmente, debemos comentar también que se amplió la lista de delitos a un total de 24, según el anexo que acompañaba a la Decisión 2009/371/JAI: tráfico ilícito de estupefacientes, actividades ilícitas de blanqueo de capitales, delitos relacionados con materiales nucleares o sustancias radiactivas, tráfico de inmigrantes clandestinos, trata de seres humanos, delincuencia relacionada con el tráfico de vehículos robados, homicidio voluntario, agresión con lesiones graves, tráfico ilícito de órganos y tejidos humanos, secuestro, retención ilegal y toma de rehenes, racismo y xenofobia, robo organizado, tráfico ilícito de bienes culturales, incluidas las antigüedades y obras de arte, fraude y estafa, chantaje y extorsión, violación de derechos de propiedad industrial y falsificación de mercancías, falsificación de documentos administrativos y tráfico de documentos administrativos falsos, falsificación de moneda, falsificación de medios de pago, delito informático, corrupción, tráfico ilícito de armas, municiones y explosivos, tráfico ilícito de especies animales protegidas, tráfico ilícito de especies y variedades vegetales protegidas, delitos contra el medio ambiente, tráfico ilícito de sustancias hormonales y otros factores de crecimiento.

El régimen jurídico fue completado con otras decisiones que se emitieron ejecución de la Decisión 2009/371/JAI[737].

d) El nuevo Reglamento de Europol

Con la entrada en vigor de las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo, a las que nos hemos referido más arriba, Europol alcanza un nuevo nivel de protagonismo en la lucha diaria contra la delincuencia, hasta el punto de convertirse en la agencia europea con mayor volumen de información al intercambiar más de 200.000 mensajes en un solo cuatrimestre[738], como

[737] Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (DO L 135 de 24.5.2016, pp. 53-114).
[738] BLASI CASAGRAN, C., "El reglamento europeo de Europol: Un nuevo marco jurídico para el intercambio de datos policiales en la UE", *Revista General de Derecho Europeo*, 40, 2016, Iustel, p. 3.

se indica en el informe de la Comisión al Parlamento Europeo y al Consejo sobre la aplicación de Estrategia de seguridad Interior de la UE[739].

Atendiendo a esa realidad, el 27 de marzo de 2013 la Comisión elaboró una propuesta de Reglamento de Europol para reemplazar el régimen jurídico establecido por las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo y atribuir responsabilidades adicionales a Europol.

Como se expone en dicha propuesta[740], ~~con la misma~~ se perseguían varias finalidades, como: a) incrementar su función de apoyo a la actuación de los servicios con funciones coercitivas nacionales, así como su colaboración mutua en la prevención y la lucha contra la delincuencia grave y el terrorismo; b) dar cumplimiento al artículo 88 del TFUE, que específicamente preveía que Europol se regiría por un reglamento adoptado con arreglo al procedimiento legislativo ordinario y que se fijarían procedimientos de control de las actividades de Europol por el Parlamento Europeo, control en el que participarían los Parlamentos nacionales; c) dar cumplimiento al postulado contenido en el "Programa de Estocolmo – Una Europa abierta y segura que sirva y proteja al ciudadano", en el que el Consejo Europeo instaba a Europol a evolucionar para convertirse en "el eje para el intercambio de información entre las autoridades policiales de los Estados miembros, un prestador de servicios y una plataforma para los servicios policiales"; y d) ofrecer una respuesta comunitaria al aumento de la delincuencia grave y organizada y al desarrollo, en particular, de la ciberdelincuencia[741].

Finalmente, tras tres años de negociaciones en las instituciones europeas, fue adoptado el Reglamento de Europol[742], que entró en vigor el 1 de mayo de 2017, con la excepción de los artículos 71 (contratos y acuerdos jurídicos celebrados con arreglo a la

---

[739] Comunicación de la Comisión al Parlamento Europeo y al Consejo. Segundo informe sobre la aplicación de la Estrategia de Seguridad Interior de la UE, COM (2013) 179 final, 10.4.2013, p. 5, disponible en https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52013DC0179, fecha de consulta 4 de mayo de 2022.

[740] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la Agencia de la Unión Europea para la cooperación y la formación en funciones coercitivas (Europol) y por el que se derogan las Decisiones 2009/371/JAI y 2005/681/JAI, COM/2013/0173 final - 2013/0091 (COD), disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52013PC0173, fecha de consulta 4 de mayo de 2022.

[741] Europol (2013). Evaluación de la amenaza de la delincuencia grave y organizada (SOCTA). 6

[742] Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo, DOUE núm. L 135 de 24 de mayo de 2016, pp. 53/114.

Decisión 2009/371/JAI), 72 (medidas transitorias relativas al Consejo de Administración) y 73 (medidas transitorias relativas al personal), los cuales están en vigor desde el 13 de junio de 2016.

La doctrina ha destacado que el Reglamento de Europol supone una ampliación de las competencias de esta agencia, las cuales consolidan el valor añadido de Europol tanto dentro como fuera de la UE[743].

Para empezar, en el anexo I se expande el listado de delitos a los que se puede referir la actividad de Europol, reemplazando el concepto de "delito grave" por el de "delincuencia organizada", con mayor alcance, ampliando la definición de algunos delitos (como el robo y hurto con agravantes, que reemplaza al anterior robo organizado, o la adición de contaminación procedente de buques en el caso de los delitos contra el medioambiente), e incorporándose un delito nuevo, que es el de "abusos sexuales y explotación sexual, incluido el material sobre abuso de menores y la captación de menores con fines sexuales".

Por su parte, la lista del artículo 4 del Reglamento, relativa a las funciones de Europol, supone una versión más simplificada y depurada del antiguo artículo 5 de la Decisión del Consejo, que dividía las tareas en un orden de prelación confuso y, además, incorpora dos funciones de nuevo cuño: prestar apoyo técnico y financiero a las operaciones transfronterizas de los Estados miembros y crear centros de asesoramiento especializados, otorgando de esta forma base jurídica al desarrollo de algunos organismos como el Centro Europeo de Ciberdelincuencia[744]. Asimismo, en el apartado 1.c) del artículo 4 queda constancia también de la adaptación del régimen jurídico de Europol al texto del TFUE, ya que el contenido de dicho precepto es idéntico al del artículo 88.1.b) del TFUE. De este contenido, además, resulta que Europol no sólo puede asistir a los Estados miembros en sus investigaciones policiales, sino que, además, puede iniciar una investigación e incluso adquirir la posición de coordinador en un proceso de investigación concreto.

De igual modo, el artículo 5 del Reglamento también revisa el régimen de la participación de Europol en los equipos conjuntos de investigación, no siendo necesaria previa autorización para participar en los mismos, y previéndose la posibilidad de proponer

[743] BLASI CASAGRAN, C., "El reglamento europeo de Europol", cit., p. 4.
[744] *Ibid.*, p. 5.

su creación a los Estados miembros afectados y tomar medidas para ayudarles en el proceso de creación del equipo conjunto de investigación.

El artículo 6 del Reglamento introduce algunas modificaciones respecto de las investigaciones penales practicadas a instancia de Europol, estableciendo además que el Estado miembro afectado debe responder a la solicitud de inicio de investigaciones por parte de Europol sin demora alguna y, preferentemente, en el plazo de un mes. Además, en el caso de que el Estado miembro decida no continuar con la investigación, debe enviar una justificación a Europol salvo que ello sea contrario a los intereses fundamentales de seguridad del Estado o ponga en peligro el desarrollo de las investigaciones o de seguridad de las personas.

El artículo 7 del Reglamento, por su parte, se refiere a las Unidades Nacionales de Europol (UNE), introduciendo algunas modificaciones respecto del régimen anterior. Así, los Estados miembros deben proporcionar a Europol la información necesaria para que pueda cumplir sus objetivos, incluida información relativa a formas de delincuencia cuya prevención o combate considere prioritario la UE, y también se prevé la posibilidad de que Europol contacte directamente con las autoridades policiales competentes, sin necesidad de la intermediación con la UNE correspondiente[745].

Los artículos 9 y siguientes se refieren a la estructura administrativa y de gestión de Europol, señalando que está compuesta por un consejo de administración, un director ejecutivo y, en su caso, otro órgano consultivo establecido por el Consejo de Administración.

El consejo de administración está compuesto por un representante de cada Estado miembro y de la Comisión, que asiste como observador. Participa en la definición de las prioridades de Europol, define por unanimidad los derechos y obligaciones de los funcionarios de enlace, fija las condiciones relativas al tratamiento de los datos, se ocupa de la preparación de las normas aplicables a los ficheros de trabajo, examina los problemas sobre los cuales la autoridad común de control requiere su atención, etc. El consejo se reúne al menos dos veces al año. Cada año adopta por unanimidad un informe sobre las actividades de Europol y un informe provisional que tiene en cuenta las necesidades

[745] Lo que puede determinar un incremento de la eficacia y agilidad, si consideramos que, en algunos Estados, como el nuestro -el caso de los Mossos d'Esquadra- existen fuerzas policiales no centralizadas que no disponen de Unidad nacional de Europol.

operativas de los Estados miembros y las incidencias en el presupuesto de Europol. Estos informes son sometidos al Consejo de la Unión Europea (UE) para su aprobación, y de ellos se informa al Parlamento Europeo. La Presidencia del consejo de administración la ejerce el representante del Estado miembro que ostente la Presidencia del Consejo;

El director es nombrado por unanimidad por el Consejo de la UE, previo dictamen del Consejo de Administración, por un período de cuatro años, renovable una vez. Lo asisten tres directores adjuntos nombrados por el Consejo (UE) por un período de cuatro años, renovable una vez. Sus tareas las establece el director, que también es responsable de la ejecución de las tareas encomendadas a Europol, de la administración corriente, de la gestión del personal, etc. El director es igualmente responsable de su gestión ante el Consejo de Administración y es al mismo tiempo el representante legal de Europol.

Por último, debemos señalar que el artículo 43 del Reglamento establece que la supervisión externa del tratamiento de datos por Europol se llevará a cabo por el Supervisor Europeo de Protección de Datos (SEPD), por lo que este organismo vigilará que los datos manejados sean tratados debidamente, y será el encargado de dar autorización antes de cualquier tratamiento automatizado de datos sensibles, así como de investigar quejas iniciadas por particulares por una posible violación de su derecho de protección de datos. De igual modo, el apartado 3.f) de dicho artículo señala que el SEPD puede prohibir temporal o definitivamente las operaciones de tratamiento por parte de Europol que violen las disposiciones que rigen los principios que garantizan la protección de los datos personales gestionados.

Con respecto a lo indicado, hemos de destacar que el artículo 29 del Reglamento introduce un sistema de valoración de fiabilidad de la fuente y exactitud de la información, con lo que se pretende evitar confusiones que pudieran surgir en el momento de cruzar información. De igual modo, Europol continúa asegurando que los datos tratados responden a los principios de necesidad y proporcionalidad, y que los datos contenidos contienen información exacta y veraz. Los Estados miembro, por su parte, mantienen la obligación de garantizar que la información enviada a Europol es exacta y se encuentra actualizada[746].

[746] Estas obligaciones ya estaban previstas en los artículos 29 y 35 de la Decisión 2009/371/JAI.

Por otro lado, han sido aumentadas y fortalecidas las facultades de control y revisión del Parlamente sobre las actividades de Europol[747],. En concreto, los artículos 51 y 52 del Reglamento adjudican al Parlamento Europeo las siguientes ~~posiciones~~ competencias: a) El Consejo de Administración deberá consultar al PE (y a los parlamentos nacionales) sobre el programa anual, b) el PE (y los parlamentos nacionales) recibirán los análisis estratégicos y de valoración de amenazas elaborados por Europol, que no sean confidenciales, c) el PE puede pedir información clasificada, y d) el PE recibirá informes de actividades de Europol, no solo por parte su Director, sino que cualquier miembro o grupo de trabajo estará obligado a remitir la información reclamada por el Parlamento[748].

Se trata, en definitiva, de un poder ampliado concedido al Parlamento Europeo y a las cámaras legislativas nacionales que, al representar el elemento poblacional de la Unión y ostentar, en el caso de los parlamentos nacionales, la legitimación que le otorga la elección de sus miembros por parte de los ciudadanos, quedan investidos de un mayores facultades de fiscalización de la actividad de Europol. El control sobre las actuaciones de Europol es ejercido por el Grupo de Control Parlamentario Conjunto (GCPC), que, con base en el derecho de la Unión Europea, permite al Parlamento Europeo y a los Parlamentos nacionales fiscalizar la actividad de una agencia de la Unión europea y, al margen de los importantes desafíos a los que se enfrenta[749], supone una mejora del control democrático de Europol y, además, puede suponer un paso más en el proceso de integración europeo[750].

C. COOPERACIÓN POLICIAL EN LA PRÁCTICA DE EUROPOL

a) Organismos incluidos en Europol

La organización interna de Europol está diseñada para abordar el análisis de las diferentes formas de delincuencia. En concreto[751], el Centro Operativo de Europol[752], es

[747] Contenido en la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre los procedimientos de control de las actividades de Europol por el Parlamento Europeo, control en el que participarán los Parlamentos nacionales, COM (2010) 776 final, 17 de diciembre de 2010, disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52010DC0776, consultado el 5 de mayo de 2022.
[748] BLASI CASAGRAN, C., "El reglamento europeo de Europol", cit., p. 18.
[749] Por ejemplo, la necesidad de coordinar representantes de todos los Parlamentos nacionales.
[750] COOPER, I., "A new form of democratic oversight in the EU: The joint parliamentary scrutiny group for Europol", *Perspectives on Federalism*, vol. 10, 3, 2018, Centro Studi sul Federalismo, p. 230.
[751] Según se indican en la propia página web de Europol, disponible en https://www.europol.europa.eu/about-europol:es, fecha de consulta 4 de mayo de 2022.
[752]Disponible en https://www.europol.europa.eu/operations-services-and-innovation/services-support/operational-coordination-support/operational-centre, fecha de consulta 4 de mayo de 2022.

un eje permanente para el intercambio de datos entre la Oficina, los Estados miembros de la UE y terceros países; funciona de forma continuada (24 horas al día, 7 días a la semana), y, en la gestión del flujo de información entre Europol y los Estados, trabajan más de treinta especialistas y analistas, que reciben la información relativa a las operaciones activas o concluidas, proceden a su análisis para para incluir los datos en las bases Europol, asisten a las operaciones policiales nacionales que se estén ejecutando y emiten informes analíticos sobre las tendencias advertidas en la actividad criminal.

Por su parte, el Centro Europeo para la Ciberdelincuencia (EC3)[753] tiene como función reforzar la respuesta policial frente a la ciberdelincuencia dentro de la UE y contribuir, así, a la protección de los ciudadanos, las empresas y las administraciones europeas frente a la delincuencia de internet. Asimismo, el Grupo de Acción Conjunta sobre Ciberdelincuencia (J-CAT)[754] impulsa las acciones coordinadas y basadas en la información de inteligencia contra las principales amenazas de la ciberdelincuencia, y respecto a sus objetivos esenciales, mediante la estimulación y la facilitación de tareas conjuntas de identificación, priorización, preparación y puesta en marcha de investigaciones.

El Centro Europeo de Lucha contra el Terrorismo (CELT)[755], como refuerzo frente a la amenaza terrorista, es un centro de operaciones que constituye el eje de recursos técnicos especializados en esta ámbito; el Centro europeo sobre el tráfico ilícito de migrantes (EMSC)[756] asiste a los Estados miembros de la UE para combatir y desarticular las redes delictivas complejas y sofisticadas implicadas en el tráfico ilícito de migrantes y la Coalición Coordinada para Delitos contra la propiedad intelectual (IPC3)[757] desempeña una labor primordial en el marco de las iniciativas para erradicar los delitos contra la propiedad intelectual en la Unión, y fuera de esta.

---

[753] Disponible en https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3, fecha de consulta 4 de mayo de 2022.
[754] Disponible en https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce, fecha de consulta 4 de mayo de 2022.
[755] Disponible en https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc, fecha de consulta 4 de mayo de 2022.
[756] Disponible en https://www.europol.europa.eu/about-europol/european-serious-and-organised-crime-centre-esocc/european-migrant-smuggling-centre-emsc, fecha de consulta 4 de mayo de 2022.
[757] Disponible en https://www.europol.europa.eu/about-europol/european-financial-and-economic-crime-centre-efecc/intellectual-property-crime-coordinated-coalition-ipc3, fecha de consulta 4 de mayo de 2022.

b) Otros organismos relacionados con la cooperación policial

Además de Europol, en la Unión Europea existen otros organismos relacionados con la cooperación policial, y a los que también debemos hacer referencia. Son los siguientes[758]:

- La Agencia de la Unión Europea para la Formación Policial (CEPOL): la CEPOL es una agencia dedicada a desarrollar, implementar y coordinar la formación de los agentes nacionales con funciones policiales. La CEPOL contribuye a una Europa más segura al facilitar la cooperación y el intercambio de conocimientos entre los agentes con funciones policiales de los Estados miembros y, en cierta medida, de terceros países, sobre cuestiones derivadas de las prioridades de la Unión en el ámbito de la seguridad, en particular, del ciclo de actuación de la Unión en materia de delincuencia grave y organizada. La Agencia para la Formación Policial se creó en virtud del Reglamento CEPOL[759]. Tiene su sede en Budapest (Hungría).

- El Comité Permanente de Cooperación Operativa en materia de Seguridad Interior (COSI): previsto en el artículo 71 del TFUE, que establece que se creará un comité permanente en el Consejo con objeto de garantizar dentro de la Unión el fomento y la intensificación de la cooperación operativa en materia de seguridad interior. Sin perjuicio del artículo 240, dicho Comité propiciará la coordinación de la actuación de las autoridades competentes de los Estados miembros. Podrán participar en sus procedimientos los representantes de los órganos, organismos y agencias de la Unión pertinentes, manteniéndose informados, el Parlamento Europeo y los parlamentos nacionales sobre estos procedimientos. El COSI se creó en virtud de la Decisión del Consejo, de 25 de febrero de 2010, por la que se crea el Comité Permanente de Cooperación Operativa en materia de Seguridad Interior (2010/131/UE)[760].

- El Centro de Inteligencia y de Situación de la Unión Europea (INTCEN): no es un organismo de cooperación policial propiamente dicho, dado que realmente constituye

---

[758] Según se contienen en la ficha relativa a la cooperación policial disponible en https://www.europarl.europa.eu/factsheets/es/sheet/156/la-cooperacion-policial, fecha de consulta 4 de mayo de 2022.
[759] Reglamento (UE) 2015/2219 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre la Agencia de la Unión Europea para la formación policial (CEPOL) y por el que se sustituye y deroga la Decisión 2005/681/JAI del Consejo (DOUE núm. L 319 de 4.12.2015, pp. 1-20).
[760] 2010/131/: Decisión del Consejo, de 25 de febrero de 2010, por la que se crea el Comité permanente de cooperación operativa en materia de seguridad interior (DOUE núm. L 52 de 3 de marzo de 2010, pp.1).

el Servicio Europeo de Acción Exterior, y solo se ocupa de análisis estratégicos. No obstante, contribuye con la cooperación policial porque efectúa una evaluación de las amenazas basándose en la información que le proporcionan los servicios de inteligencia, las fuerzas militares, los agentes diplomáticos y los cuerpos policiales. Asimismo, el INTCEN puede realizar aportaciones útiles en términos operativos, como el suministro de información en la Unión sobre los destinos, las motivaciones y los desplazamientos de los terroristas.

c) Tratamiento de información y sistemas informáticos

El régimen del tratamiento de la información por parte de Europol queda contenido en el Capítulo IV del Reglamento, denominado "Tratamiento de la información".

El artículo 17 del Reglamento se refiere a la fuente de la información que Europol podrá tratar para desempeñar sus funciones de asistencia, prevención y elaboración de inteligencia. En concreto, el referido artículo señala que Europol únicamente puede tratar la información que le haya sido facilitada por los Estados miembros, los organismos de la Unión, países terceros y organizaciones internacionales y por entidades privadas y particulares.

Adicionalmente, se prevé la posibilidad de que Europol extraiga y trate directamente información que proceda de fuentes públicamente disponibles, internet y datos públicos, incluidos los datos personales. En nuestra opinión, esta previsión es merecedora de ser destacada, en la medida en que evidencia por parte de Europol una conducta activa de obtención y recopilación de información, y no sólo limitada al tratamiento o intercambio de información que le sea facilitada, lo que no estaba expresamente previsto en la Decisión anterior del Consejo.

Por último, el apartado 3 del artículo 17 prevé también la posibilidad de que Europol sea facultada para consultar por vía informática los datos que puedan estar almacenados en las bases de datos que se manejan en el contexto de la Unión los recogidos en los sistemas de información nacionales y en los internacionales.

El artículo 18, por su parte, señala cuatro fines principales que deberá perseguir Europol al tratar la información: a) efectuar controles cruzados destinados a identificar conexiones entre datos, b) realizar análisis estratégicos o temáticos, c) elaborar análisis

operativos y d) facilitar el intercambio de información entre los Estados miembros, Europol, organismos de la UE, países terceros y organizaciones internacionales.

A este respecto, destaca en el nuevo Reglamento la ausencia de referencia a los sistemas de tratamiento de información que estaban previstos en la anterior Decisión del Consejo, y que consistían en los Ficheros de Trabajo de Análisis, el Sistema de Información de Europol y la Función de Índice. El Reglamento, como decimos, opta por eliminar la previsión específica de estos tres sistemas, y ello con el objetivo de otorgar una mayor flexibilidad en el tratamiento de dicha información. Debe entenderse, no obstante, que tales sistemas se han fusionado en uno sólo que operaría de diferentes formas en función de la categoría de datos de que se tratase[761], si bien se ha criticado la falta de aclaración acerca de cómo Europol implementaría dicho sistema.

A pesar de ello, merece la pena destacar que la propia Europol continúa refiriéndose a su sistema informático por la misma denominación, "Sistema de Información de Europol"[762], y que en fichas actualizadas de la propia agencia[763] se refiere al programa en cuestión como la base de datos de información e inteligencia criminal central de toda Europol, estando especialmente integrada con la plataforma SIENA, utilizada por las autoridades nacionales para intercambiar información de carácter penal[764].

Por último, debemos hacer referencia, también, a la Plataforma de Europol para Expertos[765], empleada por las agencias policiales nacionales y la propia Europol para compartir conocimiento, mejores prácticas, información no clasificada y otros datos no personales que puedan servir para incrementar la capacitación de los cuerpos nacionales, y al sitio web FIU.net, una red informática compleja y descentralizada que proporciona soporte a las unidades de inteligencia financiera (UIF) en la UE en su lucha contra el blanqueo de dinero y la financiación del terrorismo.

---

[761] Según la clasificación establecida en el anexo II del Reglamento.
[762] Como se puede comprobar en el apartado web existente al respecto, disponible en https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-information-system, accedido el 6 de mayo de 2022.
[763] Por ejemplo, la que puede encontrarse en https://www.europol.europa.eu/publications-events/publications/europol-information-system-eis-leaflet#downloads, con fecha última de actualización de 6 de diciembre de 2021.
[764] Según se indica en https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena, fecha de consulta el 6 de mayo de 2022.
[765] Según se indica en https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-platform-for-experts, fecha de consulta 6 de mayo de 2022.

d) Garantías en materia de protección de datos

En principio, el Reglamento de Europol ofrece un régimen de tratamiento de los datos más garantista que el que estaba en vigor con la anterior Decisión del Consejo[766].

No en vano, el artículo 33 del Reglamento enarbola el principio "protección de datos desde el diseño, estableciendo la obligación de Europol de aplicar los procedimientos y medidas técnicas y organizativas apropiadas para que el tratamiento de datos sea conforme a la normativa vigente y respetuoso con los derechos de los interesados. Una de las manifestaciones más importantes de este precepto es, por ejemplo, que el acceso a los datos existentes en la base de datos solamente sea posible en base al procedimiento *hit / no-hit*[767], y siempre que conste investigación penal en curso[768]. Este artículo, a su vez, se incluye dentro del Capítulo VI, denominado "Garantías en materia de protección de datos".

A este respecto, debe recordarse que únicamente catorce días antes se había aprobado una Directiva Europea de Protección de Datos en el ámbito policial o judicial[769], lo que sin duda influyó en el contenido del Reglamento de Europol.

No obstante, también se ha señalado que tal regulación no es exhaustiva[770.] Por ejemplo, no se encuentra en el articulado del Reglamento referencia alguna a la herramienta

---

[766] BLASI CASAGRAN, C., "El reglamento europeo de Europol", cit., p. 210.

[767] El procedimiento *hit / no-hit* consiste en que el sistema compruebe en primer lugar si la información delictiva introducida en la búsqueda coincide con algunos de los elementos de la base de datos de Europol, y solo en ese caso el solicitante podrá pedir más información al respecto.

[768] BLASI CASAGRAN, C., "El reglamento europeo de Europol", cit., p. 212.

[769] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, DOUE núm. L 119, 4.5.2016, pp. 89-131.

[770] Por ejemplo, en el Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se crea la agencia de la Unión Europea para la formación y la cooperación de los servicios con funciones coercitivas (Europol) y se derogan las Decisiones 2009/371/JAI y 2005/681/JAI, DOUE núm. C 38 de 8 de febrero de 2014, p. 3/7, contenía recomendaciones como definir los conceptos de análisis estratégico, temático y operativo y eliminar la posibilidad de tratar los datos personales para un análisis estratégico o temático, definir claramente una finalidad específica para cada caso de análisis operativo y exigir que sólo se traten los datos personales pertinentes y definir en la propuesta los siguientes elementos: i) que todas las operaciones de obtención de datos cruzados por parte de los analistas de Europol deben estar específicamente justificadas, ii) que la recuperación de los datos tras una consulta deberá quedar limitada a lo mínimo estrictamente necesario y estar debidamente justificada, iii) que debe garantizarse la trazabilidad de todas las operaciones relacionadas con el cruce de datos y iv) que sólo pueden modificar dichos datos el personal autorizado encargado de la finalidad para la que se obtienen los datos. Esto se ajustaría a la práctica actual de Europol.

de comunicación Aplicación de la Red de Intercambio Seguro de Información (SIENA, por sus siglas en inglés) o de los códigos de manejo[771].

e) La elaboración de inteligencia en Europol

En el funcionamiento de Europol se encuentra plenamente implantado el elemento de inteligencia estratégica en materia policial para la prevención de la delincuencia, especialmente después de que se le achacara una inexcusable falta de previsión respecto de los fenómenos criminales que, por sus características, dificultan la comprensión de la evolución del delito, debiendo dicha carencia ser solventada a nivel de la Unión[772]. Atendiendo a dicha circunstancia, se elaboró un Modelo Europeo de Inteligencia Criminal, tal y como fue recogido en el Programa de la Haya[773]. El Modelo Europeo de Inteligencia fue descrito como un modelo policial en la cual se hace hincapié en la recolección de información y el uso de los recursos policiales en contra de las actividades criminales a partir del modelo seguido por las diferentes agencias de seguridad europeas[774].

En desarrollo de lo expuesto, y en cumplimiento de las funciones específicamente atribuidas por medio de su Reglamento, Europol lleva a cabo evaluaciones periódicas que proporcionan análisis prospectivos de gran exhaustividad de las actividades delictivas y el terrorismo en la UE.

A continuación, analizamos brevemente los referidos análisis:

- El Reporte de Crimen organizado: fue el primer producto estratégico que se comenzó a elaborar en la extinta Unidad de Drogas de Europol en 1993. Como podemos comprobar, con el paso del tiempo ha sido modificado y mejorado, para que las agencias nacionales de seguridad contaran con mejor información sobre la forma de funcionar e impacto de sus actuaciones en la criminalidad, aunque mantiene el objetivo de dar una visión general de las actividades criminales que se desarrollaban en la Unión.

---

[771] BLASI CASAGRAN, C., "El reglamento europeo de Europol", cit., p. 217.
[772] Entre otros, podemos señalar, como ejemplo, el documento "Council conclusions on intelligence-lead policing and the development of the Organised Crime Threat Assessment (OCTA)", Consejo de la Unión Europea, Diario Oficial de la Unión Europea, 10180/05, 27 de Julio, disponible en http://data.consilium.europa.eu/doc/document/ST-10180-2005-ADD-1/en/pdf, fecha de consulta 7 de mayo de 2022.
[773] The Hague Programme: strengthening freedom, security and justice in the European Union DO C 53 de 3.3.2005, p. 1/14, disponible en https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52005XG0303%2801%29, fecha de consulta 7 de mayo de 2022.
[774] JIMÉNEZ SÁNCHEZ, F., "Europol", cit., p. 173.

Con la puesta en marcha en 1999 de Europol, fue esta última quien continuó desarrollando la labor de elaboración de dicho Reporte de Crimen organizado y la metodología para su elaboración no sufrió grandes modificaciones. El documento estaba dividido en diferentes apartados y fue publicado de forma periódica hasta 2005[775], fecha a partir de la cual pasó a estar integrado en la Evaluación de la amenaza de la delincuencia grave y organizada en la UE (SOCTA)[776].

- El Informe de Evaluación de Amenazas del Crimen Organizado: por sus siglas en inglés IOCTA, es uno de los productos de Europol que ayudan a marcar la política de seguridad de la Unión Europea. En él se identifican y valoran las amenazas emergentes o y se describe la estructura de los grupos de delincuencia organizada (GDO), la forma en la que actúan y los principales ámbitos delictivos que afectan a la Unión.

La elaboración de los IOCTA se acordó entre los Estados miembro en el Programa de la Haya y constituía el primer paso para el establecimiento del principio de inteligencia estratégica en materia policial, ya que era el documento que definía la instauración de prioridades que debían ser necesariamente debidas en cuenta por las agencias policiales nacionales.

En el Programa de Trabajo de 2007[777], se aclara que el IOCTA parte de la recolección proactiva de datos de Europol en diálogo intenso con las autoridades competentes de los Estados Miembro, así como con las partes terceras y el sector privado, para lograr una perspectiva europea y mundial

Por otro lado, es necesario considerar también el Informe sobre la situación y las tendencias del terrorismo en la UE (TE-SAT[778]), en el que se refiere con detalle el estado del terrorismo en la Unión.

Asimismo, debe hacerse referencia a la publicación anual de Panorama de Europol[779] en la que se esbozan resultados y se facilita información específica sobre los tipos

---

[775] En la web aún se encuentra disponible el Reporte de Crimen organizado correspondiente a 2004, que puede encontrarse en https://www.europol.europa.eu/sites/default/files/documents/es_euorganisedcrimesitrep04-es.pdf, fecha de consulta 7 de mayo de 2022.
[776] JIMÉNEZ SÁNCHEZ, F., "Europol", cit., p. 178.
[777] Disponible en https://www.statewatch.org/media/documents/news/2006/apr/europol-work-programme-2007.pdf, fecha de consulta 6 de mayo de 2022.
[778] Disponible en https://www.europol.europa.eu/publications-events/main-reports/eu-terrorism-situation-and-trend-report, fecha de consulta 6 de mayo de 2022.
[779] Disponible en https://www.europol.europa.eu/publications-events/other-reports/europol-in-brief, fecha de consulta 6 de mayo de 2022.

de funciones y sistemas de los que dispone Europol, así como sobre la actividad de apoyo y coordinación con las operaciones policiales conjuntas que tienen lugar tanto en el ámbito de la Unión como en otros contextos geográficos.

También puede hacerse referencia al Programa de Europol, mapa de trabajo emitido por los órganos directivos de Europol[780].

[780] Se encuentra disponible el correspondiente al periodo 2022-2024, adoptado el 14 de diciembre de 2021 y disponible en https://www.europarl.europa.eu/cmsdata/244545/Europol%20Programming%20 Document%202022-2024.pdf, fecha de consulta 6 de mayo de 2022.

CONCLUSIONES

PRIMERA: La cibercriminalidad constituye una de las principales materias de nuestra época y la lucha contra ella es una de las cuestiones a las que los Estados y organizaciones internacionales dedican mayores recursos, por su facilidad de comisión, su amplio ámbito material de actuación, y la relevancia de los intereses a que puede afectar y de las consecuencias económicas que puede tener. En este sentido, la importancia del fenómeno de la cibercriminalidad en nuestra sociedad actual y en las agendas presentes y futuras de Estados y demás poderes reguladores es innegable.

SEGUNDA: Paralelamente, la figura de la ciberdelincuencia recibe, como concepto, intensas connotaciones políticas y relativas a relaciones internacionales. No sólo el concepto de ciberdelito varía de un Derecho Penal a otro, sino que bajo el paraguas de la figura de la ciberdelincuencia se clasifican también actuaciones internacionales de ciberataque o ciberespionaje, organizadas desde otras potencias u organizaciones internacionales. Incluso, la cibercriminalidad como servicio es ofrecida, contratada y ejecutada como herramienta empleada en los equilibrios de poder internacionales. Simultáneamente, actuaciones de mero activismo o reivindicatorias de derechos humanos también son englobadas bajo el paraguas de la ciberdelincuencia. En fin, la etiqueta "cibercrimen" se emplea para calificar actuaciones de muy diversa naturaleza, con independencia de si los intereses afectados son públicos o privados, si la finalidad perseguida es el enriquecimiento personal o la puesta en valor de determinados principios de reconocimiento universal, etc.

TERCERA: Según ha declarado la jurisprudencia, la persecución y prevención de la delincuencia (y, por tanto, de la ciberdelincuencia) constituye una finalidad legítima que justifica la adopción por parte de los poderes públicos de medidas que supongan una injerencia en derechos fundamentales, siempre que, además del ya meritado principio de persecución de un fin legítimo, se respeten los principios de previsión legal suficiente y proporcionalidad en sentido genérico (compuesto, a su vez test de proporcionalidad en sentido estricto, principio de idoneidad y principio de necesidad). A este respecto, cuando la injerencia en el derecho no sea especialmente grave, el simple objetivo de prevenir, investigar, descubrir y perseguir infracciones que carezcan de especial gravedad puede ser justificación suficiente de la diligencia de investigación que se adopte.

CUARTA: Aunque las diligencias de investigación tecnológica, efectuadas en fase procesal, cuentan con previsión legal suficiente al respecto desde la entrada en vigor de la Ley Orgánica 13/2015, de 5 de octubre, el ordenamiento jurídico español continúa sin contener previsión suficiente de las diligencias de averiguación y prevención que, con carácter preprocesal, realiza la policía en el ciberespacio (ciberpatrullaje). Esto es consecuencia, a su vez, de la falta de regulación en España de la figura del patrullaje tradicional, únicamente previsto los artículos 282 LECrim, 547 LOPJ y 11 LFFCCS.

El legislador ha intentado poner fin a esta situación de vacío normativo con ocasión de los anteproyectos de LECrim y, especialmente, con el anteproyecto de 2020, pero la realidad es que, hasta que entre en vigor la normativa correspondiente, el ciberpatrullaje, como actividad de prevención e investigación de la policía y de carácter preprocesal, se encuentra en situación de vacío normativo. Existen instrucciones internas y usos empleados de manera reiterada por la policía, pero dichas disposiciones no tienen rango normativo como tal, y tampoco pueden satisfacer una eventual exigencia de previsión legal. Además, la jurisprudencia no contiene llamadas de atención sobre esta circunstancia, por lo que no se aprecia interés judicial en superar el tradicional oscurantismo de que adolecen las diligencias policiales de prevención.

Esta coyuntura dificulta que la protección de los derechos fundamentales de los ciudadanos pueda desarrollarse con plenas garantías.

QUINTA: Las características técnicas del ciberespacio, unidas a la existencia de una cibercriminalidad especializa y altamente cualificada, sitúa a los poderes públicos en la necesidad de perseguir de manera constante una mejor eficiencia y eficacia en sus actuaciones de prevención y averiguación del ciberdelito, incrementando la formación y especialización de los cuerpos de investigación, la capacidad técnica de las herramientas empleadas en las labores de prevención y averiguación de la ciberdelincuencia.

SEXTA: La búsqueda incesante de una mayor eficacia y eficiencia en la investigación y persecución de los delitos está generando una conciencia colectiva de que los derechos fundamentales, las garantías del proceso y, en particular, el instituto de la ilicitud de la prueba, son auténticas trabas prescindibles en nuestro ordenamiento jurídico, cuya relajación se considera conveniente a fin de alcanzar la mayor protección posible frente a la figura de la ciberdelincuencia. En la búsqueda de una necesaria eficiencia y eficacia que defienda el sistema establecido, se relajan garantías procesales consolidadas tras

lustros de investigación científica y construcción social. Esta situación se traslada, igualmente, al ámbito de los poderes investigativos de las fuerzas y cuerpos de seguridad.

Observamos, además, que tal práctica coincide con el parecer de, al menos, parte de la ciudadanía, que, confundida en la creencia de "no tener nada que ocultar", parece haber asumido sin oposición la dialéctica de una "situación de guerra", en la que determinados fines parecen justificar determinados medios, como es sacrificar derechos individuales en aras de una mayor seguridad común.

SÉPTIMA: Al mismo tiempo, en nuestros tribunales viene aplicándose una presunción de conocimientos tecnológicos respecto de los ciudadanos que, en algunas circunstancias, puede resultar alejada de la realidad, al atribuir una serie de conocimientos que, en muchas ocasiones, no coinciden con el realmente poseído por los usuarios, especialmente si tenemos en consideración el desarrollo vertiginoso de nuevas tecnologías y servicios cibernéticos. Esta atribución, a veces sin fundamento objetivo, de conocimientos técnicos, permite interpretar la existencia de consentimientos tácitos que provocan la disminución de determinadas garantías. Por ejemplo, para el tratamiento de sus datos por el mero acceso a determinadas aplicaciones o servicios de intercambio de archivos.

OCTAVA: La inteligencia sobre fuentes abiertas pueden ofrecer resultados muy relevantes en la lucha contra la cibercriminalidad y la protección frente a injerencias extranjeras. Ahora bien, la potencialidad de dichas técnicas provoca que supongan también un grave riesgo para la privacidad de los ciudadanos, pues el acceso y tratamiento de tales datos pueden servir para multitud de fines difíciles de controlar, como trazar perfiles de la ciudadanía, construir sistemas de previsión de riesgo delictivo, etc.

NOVENA: Las herramientas disponibles para realizar actividades de ciberpatrullaje son las mismas que las disponibles para realizar diligencias de investigación tecnológica, sin que existan instrumentos con alcance diferenciado en función de si se realizan actividades de uno u otro tipo, a pesar de que las primeras tendrán lugar con carácter preprocesal y fuera del control judicial. Es paradigmático el caso de los simuladores de antenas de telefonía, pues el mismo dispositivo sirve tanto para obtener la etiqueta identificativa del terminal –actividad enmarcada en el ciberpatrullaje– como para acceder al almacenamiento del mismo e interceptar comunicaciones -diligencia de investigación tecnológica-. No existen limitaciones que se deriven del propio diseño de las herramientas disponibles a tal efecto. En consecuencia, durante el ciberpatrullaje no existe garantía

alguna de que se haga un uso limitado de las capacidades técnicas de las herramientas que se emplean. Además, la competición en el mercado por ofrecer más y mejores prestaciones lleva a que sus desarrolladores incluyan posibilidades de investigación muy superiores a las estrictamente necesarias para la investigación policial.

DÉCIMA: Al contrario de lo que sucede respecto del patrullaje tradicional, "analógico" o material, en el ciberespacio no existe, al menos por el momento, representación o indicativo alguno que señale la existencia de presencia policial en un ámbito concreto del ciberespacio. En consecuencia, los individuos no pueden comprobar *in situ* el modo en que realizan las funciones de prevención del delito y seguridad ciudadana, ni tampoco ser conscientes de la presencia policial en dicho "espacio público", por lo que se resta eficacia preventiva al propio acto de ciberpatrullar, que tendrá un menor efecto disuasorio al ser desconocido por naturaleza.

DECIMOPRIMERA: Aunque, en nuestro ordenamiento jurídico, el principio general es el de la prohibición de las diligencias de investigación tecnológica prospectivas (apartado segundo del artículo 588 *bis* a LECrim), esto es, aquellas que no se dirijan a la averiguación de hechos concretos sobre los que exista una base objetiva y razonable para sospechar de su carácter delictivo, la falta de regulación y de publicidad de las técnicas concretas empleadas en el ciberpatrullaje, comporta que no pueda entenderse garantizado el respeto a dicho principio. Redunda también en este aspecto la falta de regulación específica acerca de algunas diligencias de investigación, como el caso del agente encubierto informático o el de los nidos o redes trampa, en los que se plantean serias dudas sobre la concurrencia de una posible provocación al delito o, incluso, de una tentativa inidónea, en el caso de los "cebos" compuestos por meros programas informáticos, y que se dirigen contra la colectividad indeterminada de personas.

DECIMOSEGUNDA: De igual modo, ante la imposibilidad operativa y jurídica de patrullar el espacio privado y de obtener autorización judicial para cada uno de los usuarios de un servicio, se traslada al usuario el acto de otorgar consentimiento a injerencias en su privacidad por el mero hecho de utilizar el servicio. De esta forma, es la propia compañía prestadora de los servicios la que, además de disponer de los datos de conducta de sus usuarios, asume el esfuerzo de patrullar y analizar los mismos, la actividad cibernética de los usuarios –a lo que estos han prestado su consentimiento de manera tácita al acceder al servicio–, y quien traslada a la policía noticia de aquellas conductas o contenidos potencialmente ilícitos. De esta manera, se puentea el régimen de garantías y

exigencias legalmente establecido para proscribir las investigaciones que no vayan dirigidas a un sujeto específico por razones concretas, la actividad de patrullaje se traslada a los propios prestadores del servicio, y se construye un nuevo consentimiento tácito por parte del usuario.

DECIMOTERCERA: Existen graves dificultades para que los usuarios puedan conocer el verdadero alcance del deber de colaboración de los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información. A ese respecto, existen varios ejemplos en los que la opinión pública ha podido conocer la existencia de programas y colaboraciones entre los prestadores de servicios y las agencias de investigación de diferentes gobiernos. De igual modo, dicha entrega de información no se produce solamente respecto de la policía del Estado del que el usuario es nacional, sino que la propia prestadora del servicio puede facilitar dicha información a la policía de aquél Estado del que ella es nacional, distinto de aquél en el que preste los servicios.

Como consecuencia de ello, aparecen ciertas manifestaciones de desconfianza sobre la diligencia con la que tratan y custodian dichos prestadores de servicios los datos que reciben de sus usuarios cuando estos emplean sus servicios. En tal coyuntura, los propios prestadores de servicios elaboran informes se transparencia con la finalidad de apaciguar las sospechas de su público usuario, pero lo cierto es que no existe garantía alguna de que la información plasmada en dichos informes responda a la realidad.

DECIMOCUARTA: Se aprecian tendencias conducentes a establecer la responsabilidad de los prestadores de servicios e intermediarios de internet por los contenidos de los propios usuarios. Esta atribución supondría, en consecuencia de imponerles la obligación de desplegar una diligencia activa al respecto, lo que a su vez puede emplearse para justificar las facultades de revisión y tratamiento de los datos de los usuarios, convirtiéndose así el ciberespacio en una zona de vigilancia permanente.

DECIMOQUINTA: Al igual que existen herramientas accesibles de forma pública que sirven al ciberpatrullaje y a la ciberinvestigación, también existen herramientas de "ciberprivacidad" que -siendo igualmente accesibles públicamente- dificultan dichas tareas. En ese sentido, del mismo modo que la ciberdelincuencia genera un mercado (el de la ciberseguridad), la cibervigilancia genera otro, el de la ciberprivacidad, en igual crecimiento exponencial. Así, asistimos a la expansión y democratización de diversas

herramientas, entre las que sobresalen el encriptado de los datos en tráfico y reposo y el empleo de redes VPN (a través de soluciones gratuitas, de código abierto, o con precios muy atractivos para el usuario medio).

Esta situación, unida al deber de colaboración de las sociedades prestadoras de servicios de la sociedad de información -de alcance incontrolable-, al imposible de fiscalizar ciberpatrullaje, y una jurisprudencia proclive a reducir la aplicación de la regla de la ilicitud de la prueba en caso de vulneración de derechos fundamentales y a expandir el concepto del "consentimiento tácito" a los usuarios de internet, puede generar que los ciudadanos adopten las herramientas necesarias para restringir los datos que ponen a disposición de las autoridades y empresas prestadoras de servicios, intentando fortalecer su privacidad online y provocando con ello una disminución de la eficacia de las herramientas de ciberinvestigación

DECIMOSEXTA: Con ocasión de la pandemia provocada por la covid-19 ha aparecido la "cara amable" de las técnicas de vigilancia masiva, reavivando desde una óptica diferente el debate social ya existente sobre la conveniencia de que los individuos renuncien a su privacidad a cambio de una mayor seguridad común, planteándose sistemas con posibilidad de rastrear los contactos entre individuos a través de conexiones inalámbricas de sus dispositivos y, probablemente, geolocalización, con una utilidad aún pendiente de determinar.

DECIMOSÉPTIMA: Las circunstancias expuestas confirman lo necesario que resulta reconocer un derecho fundamental a la integridad y a la reserva de los sistemas informáticos como parte del derecho a la intimidad y al desarrollo de la libertad personal. Las garantías establecidas para proteger la esfera privada de las personas del uso público de la informática no son suficientes para que en nuestras sociedades se mantenga la necesaria parcela de intimidad, terreno necesario para el despliegue de la creatividad y el avance de la sociedad.

Es cierto que se prevé un sistema de exigencias proporcionales a la gravedad de la injerencia, pero, en realidad, en multitud de ocasiones las medidas implican una injerencia de mucha mayor gravedad a la públicamente conocida. Y, es más, resulta de gran dificultad poner de manifiesto la existencia de dicho desequilibrio en los casos concretos. Asistimos a supuestos en los que la policía puede realizar dichas averiguaciones *de facto*, sin necesidad de atender a los límites marcados por la legislación procesal y el debido

respeto a los derechos fundamentales, y que el único rastro que pueda advertirse de dichas prácticas dependa de la diligencia o buena voluntad del funcionario policial que las consigne en su informe, diligencia o atestado, más allá de averiguaciones periciales cuya naturaleza escapa a la práctica ordinaria de los tribunales. Nada impide a la Policía Judicial ejecutar la más invasiva de las medidas para, a continuación, solicitar autorización judicial "sobre seguro" –sin revelar la previa intervención ilegítima–.

En ese sentido, el regulador europeo y el legislador español deben extremar las precauciones para impedir que en Europa se establezcan a largo plazo métodos invasivos de extracción de datos y de vigilancia digital. Quizás debería plantearse la conveniencia de un reconocimiento internacional del derecho de los ciudadanos a que su información –recolectada mediante sistemas de cibervigilancia o a través de la colaboración de prestadores de servicios– sea utilizada exclusivamente para los fines que inicialmente ellos mismos hubieran autorizado. Igualmente, se hace necesario establecer mayores garantías en lo relativo a las diligencias de investigación tecnológica, especialmente en cuanto al ciberpatrullaje y al deber de colaboración de terceros. No sólo por una defensa *per se* de los derechos fundamentales, sino porque, en cuanto al ciberpatrullaje, su falta de regulación y control puede comportar la adopción de iniciativas individuales que reduzcan en mucho la capacidad investigadora de la policía, y porque, en cuanto al deber de colaboración de terceros, se puede estar facilitando que dichas entidades recolecten información a través de sus usuarios y las remitan a sus respectivas agencias de seguridad nacionales.

BIBLIOGRAFÍA

ALBALADEJO, F., *Seguridad interior, seguridad exterior ¿dónde quedan las fronteras?*, Fundación Policía Española, fecha de consulta 11 abril 2022, en http://www.dykinson.com/libros/seguridad-interior-seguridad-exterior-donde-quedan-las-fronteras/9788461421992/.

ALEXY, R., "Constitutional Rights, Balancing, and Rationality", *Ratio Juris*, vol. 16, n.º 2, 2003, pp. 131-140.

ALONSO SALGADO, C., "Acerca de la inteligencia artificial en el ámbito penal: especial referencia a la actividad de las fuerzas y cuerpos de seguridad", *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, vol. 7, n.º 1, 2021, Universidad de Sevilla, pp. 25-36.

ÁLVAREZ CONDE, E., "El sistema constitucional español de derechos fundamentales", *Corts: Anuario de derecho parlamentario*, n.º 15, 2004, Cortes Valencianas, pp. 115-146.

ÁLVAREZ SÁNCHEZ DE MOVELLÁN, P., "«Ponderaciones» judiciales en materia de prueba prohibida y garantías para la nueva investigación en el proceso penal", en *Exclusiones probatorias en el entorno de la investigación y prueba electrónica, 2020, págs. 105-140*, Reus, 2020, pp. 105-140.

ANDERSON, N., *The Internet Police: How Crime Went Online, and the Cops Followed*, W. W. Norton & Company, New York, 2013.

ANDREU, J., *Instalación de equipos de red. Configuración (Redes locales)*, Editex, 2011.

ARANGÜENA FANEGO, C., "Orden europea de investigación: aspectos generales del nuevo instrumento de obtención de prueba penal transfronteriza", en *Orden europea de investigación y prueba transfronteriza en la Unión Europea, 2019*, Tirant lo Blanch, 2019, pp. 297-326.

ARIAS RODRÍGUEZ, J. M., "El Programa de Estocolmo", *Diario La Ley*, n.º 7812, 2012, Wolters Kluwer, p. 2.

ARMENTA DEU, T., "Prueba ilícita y regla de exclusión: perspectiva subjetiva", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020,* Ediciones Jurídicas Castillo de Luna, 2020, pp. 117-140.

ARRABAL PLATERO, P., "El derecho fundamental al propio entorno virtual y su incidencia en el proceso", en *Era Digital, Sociedad y Derecho*, Tirant lo Blanch, Valencia, 2020.

ARRABAL PLATERO, P., *La prueba tecnológica: aportación, práctica y valoración*, Tirant lo Blanch, Valencia, 2019.

ARREOLA GARCÍA, A., *Ciberseguridad: ¿Por qué es importante para todos?,* Siglo XXI Editores México, 2019.

ASENCIO GALLEGO, J. M., "Los delitos informáticos y las medidas de investigación y obtención de pruebas en el convenio de Budapest sobre la ciberdelincuencia", en *Justicia penal y nuevas formas de delincuencia, 2017*, Servei de Publicacions, 2017.

ASENCIO MELLADO, J. M., "La exclusión de la prueba ilícita en la fase de instrucción como expresión de garantía de los derechos fundamentales", *Diario La Ley,* n.º 8009, 2013, Wolters Kluwer.

ASENCIO MELLADO, J. M., "La prueba ilícita y su triste destino", en *La Administración de Justicia en España y en América, Vol. I*, Editorial Astigi, Sevilla, 2021, pp. 175-197.

ASENCIO MELLADO, J. M., "La prueba y la obra del profesor Gimeno en los tiempos de cambio", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020,* Ediciones Jurídicas Castillo de Luna, 2020, pp. 177-198.

ASENCIO MELLADO, J. M., "La STC 97/2019, de 16 de julio. Descanse en paz la prueba ilícita", *Diario La Ley*, n.º 9499, 2019.

ASENCIO MELLADO, J. M., "Prueba ilícita: declaración y efectos", *Revista General de Derecho Procesal*, n.º 26, 2012, Iustel.

ASENCIO MELLADO, J. M., *Prueba prohibida y prueba preconstituída*, Editorial Trivium, 1989.

ASENCIO MELLADO, J. M.; FERNÁNDEZ LÓPEZ, M., *Justicia penal y nuevas formas de delincuencia*, Servei de Publicacions, 2017.

ASENCIO MELLADO, J. M.; FUENTES SORIANO, O.; CALAZA LÓPEZ, M. S., *Derecho procesal penal*, Tirant lo Blanch, Valencia, 2019.

BACHMAIER WINTER, L., "El exhorto europeo de obtención de pruebas en el proceso penal: estudio y perspectivas de la propuesta de decisión marco", en *El Derecho procesal penal en la Unión Europea: tendencias actuales y perspectivas de futuro, 2006*, Constitución y Leyes, COLEX, 2006, pp. 131-178.

BARRIO ANDRÉS, M., *Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2ª, Wolters Kluwers, Madrid, 2018.

BECK, U., *La sociedad del riesgo: Hacia una nueva modernidad*, Grupo Planeta Spain, 2013.

BELLIDO PENADÉS, R., "Intervención de las comunicaciones orales directas y proceso penal en la jurisprudencia constitucional", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020*, Ediciones Jurídicas Castillo de Luna, 2020, pp. 257-278.

BENFORADO, A., "Body Cams Don't Guarantee Objectivity. They Limit It.", *Slate Magazine*, 2015.

BERLE, I., "The Law and Surveillance", 2020, pp. 113-124.

BERNAL, A. R., "España: Los Cibercrimenes en el Espacio de Libertad, Seguridad y Justicia", *AR: Revista de Derecho Informático*, n.º 103, 2007, Alfa-Redi, p. 4.

BLASI CASAGRAN, C., "El reglamento europeo de Europol: Un nuevo marco jurídico para el intercambio de datos policiales en la UE", *Revista General de Derecho Europeo*, n.º 40, 2016, Iustel, pp. 202-221.

BONACHERA VILLEGAS, R., "El registro de archivos informáticos: una cuestión necesitada

de regulación", *Revista General de Derecho Procesal*, n.º 27, 2012, Iustel.

BONET NAVARRO, J., "Apuntes sobre el concepto, obtención, introducción y fiabilidad de la prueba electrónica", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020*, Ediciones Jurídicas Castillo de Luna, 2020, pp. 279-298.

BUENO DE MATA, "El derecho probatorio ante la cuarta revolución industrial", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020*, Ediciones Jurídicas Castillo de Luna, 2020, pp. 299-314.

BUENO DE MATA, F., "El agente encubierto en internet: mentiras virtuales para alcanzar la justicia", en *Los retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso Gallego de Derecho Procesal (I Internacional), A Coruña, 2 y 3 de junio de 2011, 2012*, 2012, pp. 295-306.

BUENO DE MATA, F., "España", en *La prueba en el proceso: perspectivas nacionales, 2018*, Tirant lo Blanch, 2018, pp. 573-580.

BUENO DE MATA, F., "La validez de los «screenhots» o «pantallazos» como prueba electrónica a tenor de la jurisprudencia del Tribunal Supremo", en *Los desafíos de la justicia en la era post crisis, 2016*, Atelier, 2016, pp. 141-152.

BUENO DE MATA, F., "Peculiaridades probatorias del dron como diligencia de investigación tecnológica", en *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas, 2018*, Tirant lo Blanch, 2018, pp. 169-204.

BUENO DE MATA, F.; BUJOSA VADELL, L.-M.; FORUM DE EXPERTOS Y JÓVENES INVESTIGADORES EN DERECHO Y NUEVAS TECNOLOGÍAS, "Fodertics 5.0", Comares, Albolote, Granada, 2016.

BUENO DE MATA, F.; BUJOSA VADELL, L.-M.; FÓRUM DE EXPERTOS Y JÓVENES INVESTIGADORES EN DERECHO Y NUEVAS TECNOLOGÍAS, "Fodertics 6.0: los nuevos retos del derecho ante la era digital", Comares, Albolote, Granada, 2017.

BUENO DE MATA, F.; FORUM DE EXPERTOS Y JÓVENES INVESTIGADORES EN DERECHO Y NUEVAS TECNOLOGÍAS; "Fodertics, estudios sobre derecho y nuevas tecnologías",

Andavira, Santiago de Compostela, 2012.

BUENO DE MATA, F.; GONZÁLEZ PULIDO, I.; BATRES LEÓN, M. A., *Fodertics 7.0: estudios sobre derecho digital*, Comares, Granada, 2019.

BYUNG-CHUL, H., "La emergencia viral y el mundo de mañana. Byung-Chul Han, el filósofo surcoreano que piensa desde Berlín", *EL PAÍS*, 2020.

CABEZUDO RODRÍGUEZ, N., "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal", *I Jornada del Boletín del Ministerio de Justicia: Las reformas del proceso penal*, vol. 2186, 2016, pp. 7-60.

CALAZA LÓPEZ, S., "Tres verdades (material, formal, virtual) y una sola realidad: la prueba electrónica", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020*, Ediciones Jurídicas Castillo de Luna, 2020, pp. 371-398.

CALAZA LÓPEZ, S., "Fortalecimiento de las garantías procesales y agilización de la justicia", *Revista General de Derecho Procesal*, n.º 41, 2017, Iustel.

CALAZA LÓPEZ, S., "Protección judicial del derecho a la intimidad informática en su doble dimensión de derecho a la autodeterminación informativa y derecho al entorno virtual", en *Nuevos postulados de la cooperación judicial en la Unión Europea: libro homenaje a la Prof.ª Isabel González Cano, 2021*, Tirant lo Blanch, 2021, pp. 1111-1146.

CALAZA LÓPEZ, S., "Proyecciones del derecho de defensa tras la reforma de la LECrim: son todas las que están, pero no están todas las que son", *Actualidad jurídica Aranzadi*, n.º 924, 2016, Aranzadi Thomson Reuters.

CALAZA LÓPEZ, S., "Un nuevo horizonte judicial en materia de derechos constitucionales y principios procesales: Propuestas de reforma en tiempos de crisis", *e-Legal History Review*, n.º 25, 2017, Iustel.

CALAZA LÓPEZ, S., "Una nueva dimensión del derecho de información del investigado/encausado en el proceso penal", *Anuario jurídico Villanueva*, n.º 11, 2017,

Centro Universitario Villanueva, pp. 17-52.

CALVO LÓPEZ, D., "Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (apartados K) a M) del art. 588 ter de la LECrim)", en *Jornadas de Especialistas celebradas en el Centro de Estudios Jurídicos de Madrid*, Madrid, 2017.

CARRILLO DEL TESO, A. E., "El diálogo judicial sobre las «listas Falciani»: los diferentes criterios de su admisión como prueba", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020*, Ediciones Jurídicas Castillo de Luna, 2020, pp. 419-434.

CARRILLO, M.; REVENGA SÁNCHEZ, M.; DÍEZ-PICAZO GIMÉNEZ, I., *El derecho a la privacidad en el nuevo entorno tecnológico*, Centro de Estudios Políticos y Constitucionales (España), 2016.

CASTILLEJO MANZANARES, R., "Alguna de las cuestiones que plantean las diligencias de investigación tecnológica", *Revista de derecho y proceso penal*, n.º 45, 2017, Aranzadi Thomson Reuters, pp. 23-57.

CASTILLEJO MANZANARES, R., "Europol y las investigaciones transfronterizas", *Dereito: Revista xuridica da Universidade de Santiago de Compostela*, vol. 17, n.º 2, 2008, Servicio de Publicaciones = Servizo de Publicacións, pp. 91-104.

CERVERA RODRÍGUEZ, Á., *Cómo elaborar trabajos académicos y científicos: (TFG, TFM, tesis y artículos)*, Alianza, Madrid, 2019.

CHAMBERS-JONES, C., "Policing Cyber Hate, Cyber Threat and Cyber Terrorism", *International Journal of Police Science & Management*, vol. 15, 2013.

CHANDLER, S., "Researchers Use Big Data And AI To Remove Legal Confidentiality", *Forbes*.

CID, I. V. L., "La protección de la intimidad en la era tecnológica: hacia una reconceptualización", *Revista Internacional de Pensamiento Político*, vol. 7, 2012, Universidad Pablo de Olavide, pp. 117-144.

COHEN, S., "¿Quién necesita extraer inteligencia de fuentes abiertas (OSINT)?", *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones*, n.º 84, 2019, Borrmart.

COOPER, I., "A new form of democratic oversight in the EU: The joint parliamentary scrutiny group for Europol", *Perspectives on Federalism*, vol. 10, n.º 3, 2018, Centro Studi sul Federalismo, p. 13.

CÓRDOBA CASTROVERDE, D.; DÍEZ-PICAZO GIMÉNEZ, I., "Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico", en *El derecho a la privacidad en un nuevo entorno tecnológico: XX Jornadas de la Asociación de Letrados del Tribunal Constitucional*, 2016, pp. 99-122.

COTINO HUESO, L., *Derecho constitucional II: Derechos fundamentales*, Universitat de València, 2011.

CRUZ, J., "Carolin Emcke: "La pandemia es una tentación autoritaria que invita a la represión"", *EL PAÍS*, 2020.

CUADRADO SALINAS, C., "Registro informático y prueba digital. Estudio y análisis comparado de la ciberinvestigación criminal en Europa", 2014, La Ley.

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*, n.º 107, 2014, Wolters Kluwer, p. 3.

CUADRADO SALINAS, C. C., "La obtención de pruebas electrónicas transfronteriza: Nuevos retos y nuevas consideraciones desde la perspectiva de la Unión Europea", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum*, Ediciones Jurídicas Castillo de Luna, 2020, pp. 517-534.

DAVARA RODRÍGUEZ, "El Reglamento Europol", *Actualidad administrativa*, n.º 7, 2017, Wolters Kluwer, p. 8.

DAVARA RODRÍGUEZ, M. Á.; DAVARA FERNÁNDEZ DE MARCOS, E.; DAVARA FERNÁNDEZ DE MARCOS, L., *Delitos informáticos*, Editorial Aranzadi, Pamplona, 2017.

DE LA TORRE OLID, F.; GARCÍA RUIZ, F., "Tecnología de geolocalización y seguimiento

al servicio de la investigación policial. Incidencias sobre el Derecho a la intimidad", *Revista Derecho y Criminología*, vol. Anales, n.º 2, 2011.

DEL MORAL GARCÍA, A., "A vueltas con el derecho al silencio del acusado", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum*, Ediciones Jurídicas Castillo de Luna, 2020, pp. 1303-1322.

DEL POZO PÉREZ, M., "España", en *La prueba en el proceso: perspectivas nacionales*, Tirant lo Blanch, 2018, pp. 757-764.

DELGADO MARTÍN, J., "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015", *Diario La Ley*, n.º 8693, 2016, Wolters Kluwer.

DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, 2ª edición actualizada, La Ley, Madrid, 2018.

DELGADO MARTÍN, J., "La prueba digital. Concepto, clases, aportación al proceso y valoración", *Diario La Ley Ciberderecho*, n.º 6, 2017, Wolters Kluwer.

DÍAZ CABIALE, J. A.; MARTÍN MORALES, R., *La garantía constitucional de la inadmisión de la prueba ilícitamente obtenida*, 2001.

DÍAZ CAPPA, J., "Confidencialidad, secreto de las comunicaciones e intimidad en el ámbito de los delitos informáticos", *Diario La Ley*, n.º 7666, 2011, Wolters Kluwer.

DÍAZ GÓMEZ, A., "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest", *Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR)*, n.º 8, 2010, pp. 169-203.

DÍAZ GÓMEZ, A., "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest", *Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR)*, n.º 8, 2010, pp. 169-203.

DÍAZ MARTÍNEZ, M.; LÓPEZ-BARAJAS PEREA, I., *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo Blanch, Valencia, 2018.

DÍEZ-PICAZO GIMÉNEZ, I., "Algunas ideas sobre la prueba ilícitamente obtenida", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum*, Ediciones Jurídicas Castillo de Luna, 2020, pp. 575-590.

DONAIRE VILLA, F. J., "El Tratado de Amsterdam y la Constitución", *Revista española de derecho constitucional*, vol. 18, n.º 54, 1998, Centro de Estudios Políticos y Constitucionales (España), pp. 119-167.

DURÁN SILVA, C., "Los medios de prueba tecnológicos como garantía de la correcta incorporación de las nuevas fuentes de prueba al juicio oral", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum*, Ediciones Jurídicas Castillo de Luna, 2020, pp. 611-624.

DWYER, J., "Showing the Algorithms Behind New York City Services", *The New York Times*, 2017, fecha de consulta 4 mayo 2020, en https://www.nytimes.com/2017/08/24/nyregion/showing-the-algorithms-behind-new-york-city-services.html.

ECHARRI CASI, F. J., "Prueba ilícita: conexión de antijuridicidad y hallazgos casuales", *Revista del poder judicial*, n.º 69, 2003, Consejo General del Poder Judicial, pp. 261-301.

ECIJA BERNAL, Á., "Ciberespacio, Dark Web y Ciberpolicía", *Diario La Ley*, n.º 8940, 2017, Wolters Kluwer.

ESQUINAS VALVERDE, P., "El tipo de mera posesión de pornografía infantil en el código penal español (art. 189.2): razones para su destipificación", *Revista de Derecho Penal y Criminología*, n.º 18, 2006, Facultad de Derecho, pp. 171-228.

ESTRELLA RUIZ, M., "Entrada y registro, interceptación de comunicaciones postales, telefónicas, etc...", *Cuadernos de derecho judicial*, n.º 12, 1996, Consejo General del Poder Judicial, pp. 351-392.

ETXEBERRIA GURIDI, J. F., "Inteligencia Artificial aplicada a la videovigilancia: tecnologías de reconocimiento facial", en *Justicia algorítmica y neuroderecho: una mirada multidisciplinar*, Tirant lo Blanch, 2021, pp. 443-467.

ETXEBERRIA GURIDI, J. F., "La sentencia del TEDH «S. y Marper c. Reino Unido», de 4 de diciembre de 2008, sobre ficheros de ADN, y su repercusión en la normativa española", en *Derecho y nuevas tecnologías, Vol. 1, 2011 (Primera parte. Nuevas tecnologías, sociedad y derechos fundamentales),* Universidad de Deusto = Deustuko Unibertsitatea, 2011, pp. 393-406.

EXPÓSITO LÓPEZ, L., "Criminalidad organizada y tráfico de drogas: Las transformaciones del sistema jurídico-penal sustantivo y procesal", 2016, UNED. Universidad Nacional de Educación a Distancia (España).

FELIP I SARDÁ, J. M., "La gestión de fuentes abiertas por los servicios de Inteligencia y los equipos de investigación: el estado de la cuestión", *Cuadernos constitucionales de la Cátedra Fadrique Furió Ceriol*, n.º 48, 2004, Departamento de Derecho Constitucional y Ciencia Política y de la Administración, pp. 41-50.

FERNÁNDEZ ENTRALGO, J., "Prueba ilegítimamente obtenida", *Jueces para la democracia*, n.º 7, 1989, Jueces para la Democracia, pp. 21-33.

FERNÁNDEZ LÓPEZ, J. M., "El derecho fundamental a la protección de los datos personales. Obligaciones que derivan para el personal sanitario.".

FLORES PRADA, I., "Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia", *Revista electrónica de ciencia penal y criminología*, n.º 17, 2015, Universidad de Granada.

FREIXES SANJUÁN, T. F., "La igualdad y el futuro de Europa: reflexiones en torno al proceso de constitucionalización", *Artículo 14, una perspectiva de género: Boletín de información y análisis jurídico*, n.º 16, 2004, Instituto Andaluz de la Mujer, pp. 4-21.

FRIEDEN, J.; MURRAY, L., "The Admissibility of Electronic Evidence Under the Federal Rules of Evidence", *Richmond Journal of Law & Technology*, vol. 17, n.º 2, 2011, p. 5.

FRIEDERSDORF, C., "The NYPD Is Using Mobile X-Ray Vans to Spy on Unknown Targets", *The Atlantic*, 2015.

FUENTES SORIANO, O., "La prueba prohibida aportada por particulares: , a la luz de las nuevas tecnologías", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum,* Ediciones Jurídicas Castillo de Luna, 2020, pp. 715-744.

FUENTES SORIANO, O.; ARRABAL PLATERO, P.; ALCARAZ RAMOS, M., *Era Digital, Sociedad y Derecho,* Tirant lo Blanch, Valencia, 2020.

FUENTES SORIANO, O.; DOMENECH FEDERIC, A., *El proceso penal: cuestiones fundamentales,* Tirant lo Blanch, Valencia, 2017.

GALLEGO, E., "Honeynets: Aprendiendo del Atacante", p. 10.

GÁLVEZ MUÑOZ, L. A., *La ineficacia de la prueba obtenida con violación de derechos fundamentales: normas y jurisprudencia (TEDH, TC, TS, TSJ y AP) en los ámbitos penal, civil, contencioso-administrativo y social,* Thomson Reuters Aranzadi, 2003.

GARCÍA BORREGO, J. A., "Análisis de la regulación y jurisprudencia actual de las Diligencias de Investigación en el Proceso Penal y la actuación de la Policía Judicial, en particular; en la intervención de las nuevas modalidades de comunicaciones personales.", 2017, Universidad Católica San Antonio de Murcia, p. 1.

GARCÍA GONZÁLEZ, A., "Desdentado Bonete, Aurelio y Muñoz Ruiz Ana Belén, Control informático, videovigilancia y protección de datos en el trabajo.", *Revista Latinoamericana de Derecho Social,* n.º 19, 2014, Instituto de Investigaciones Jurídicas.

GARCÍA, J., "La inteligencia artificial se viste de policía para atrapar a los malos", *El País,* 2019, Madrid.

GARCÍA, J., "VeriPol, el polígrafo 'inteligente' de la policía, puesto en cuestión por expertos en ética de los algoritmos", *EL PAÍS,* 2021.

GARCÍA TORRES, M. L., "La tramitación electrónica de los procedimientos judiciales", *La ley penal: revista de derecho penal, procesal y penitenciario,* n.º 82, 2011, Wolters Kluwer.

GARCÍA VALDÉS, C., "«No destruirán nuestra libertad» de Javier Gómez Bermúdez", *Anuario de la Facultad de Derecho*, n.º 3, 2010, Servicio de Publicaciones, pp. 557-562.

GASCÓN INCHAUSTI, F., "La eficacia de las pruebas penales obtenidas en el extranjero al amparo del régimen convencional: apogeo y declive del principio de no indagación", en *Orden europea de investigación y prueba transfronteriza en la Unión Europea*, Tirant lo Blanch, 2019, pp. 31-63.

GASCÓN INCHAUSTI, F., "Reconocimiento mutuo de resoluciones de embargo preventivo y aseguramiento de prueba: análisis normativo", en *Reconocimiento mutuo de resoluciones penales en la Unión Europea: análisis teórico-práctico de la Ley 23/2014, de noviembre,* Aranzadi Thomson Reuters, 2015, pp. 323-362.

GEORGE, R.; KLINE, R., *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, Rowman & Littlefield, 2006.

GIMENO SENDRA, J. V., *Derecho Procesal Penal*, fecha de consulta 23 diciembre 2021, en http://www.dykinson.com/libros/derecho-procesal-penal/9788413086293/.

GIMENO SENDRA, J. V., "La Prova preconstituïda de la policia judicial", *Revista catalana de seguretat pública*, n.º 22, 2010, Institut de Seguretat Pública de Catalunya, pp. 35-64.

GIMENO SENDRA, J. V., "Las intervenciones electrónicas y la policía judicial", *Diario La Ley*, n.º 7298, 2009, Wolters Kluwer, p. 1.

GIMENO SENDRA, J. V., "Libertad de expresion, honor e intimidad personal", *Economist & Jurist*, vol. 17, n.º 136, 2010, Global Economist & Jurist, pp. 40-48.

GIRI, S., "Cyber Crime, Cyber threat, Cyber Security Strategies and Cyber Law in Nepal", vol. Volume 9, 2020, pp. 662-672.

GOIZUETA VÉRTIZ, J., "La cooperación policial en el seno de Europol: el principio de disponibilidad y la confidencialidad de la información", *Revista española de derecho constitucional*, vol. 37, n.º 110, 2017, Centro de Estudios Políticos y Constitucionales (España), pp. 75-103.

GÓMEZ COLOMER, J. L., "El aumento del intervencionismo público en la investigación del delito: Una reflexión al hilo del acto de investigación criminal de registro remoto de equipos informáticos (coloquialmente llamado «del gusano informático»)", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum,* Ediciones Jurídicas Castillo de Luna, 2020, pp. 817-852.

GÓMEZ DE LIAÑO FONSECA HERRERO, M., "El uso de dispositivos electrónicos de captación de comunicaciones en operaciones de inflitración", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum,* Ediciones Jurídicas Castillo de Luna, 2020, pp. 853-870.

GONZÁLEZ, G. F.-B., "Europol: los informes de inteligencia como medios de prueba", en *Los nuevos escenarios en las relaciones internacionales: retos, amenazas y oportunidades,* Aranzadi Thomson Reuters, 2019, pp. 319-337, fecha de consulta 6 mayo 2022, en https://dialnet.unirioja.es/servlet/articulo?codigo=8097010.

GONZÁLEZ GRANDA, P., "Internet, ética y prueba de oficio: a propósito de dos recientes dictámenes de la Comisión de Ética Judicial del Consejo General del Poder Judicial", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum,* Ediciones Jurídicas Castillo de Luna, 2020, pp. 907-930.

GONZÁLEZ HURTADO, J. A., "Delincuencia informática: daños informáticos del artículo 264 del Código penal y propuesta de reforma", 2013, Universidad Complutense de Madrid.

GONZÁLEZ NAVARRO, A., "Breves reflexiones críticas sobre la proyección de los principios de oportunidad y dispositivo en el proceso penal", en *Postmodernidad y proceso europeo: la oportunidad como principio informador del proceso judicial,* Dykinson, 2020, pp. 279-297.

GONZÁLEZ NAVARRO, A., "Delito grave y cesión de datos de la comunicación: algunas consideraciones a raíz de la Sentencia del TJUE en el Asunto C-207/16", en *En torno a la prueba y al proceso,* Comares, 2019, pp. 241-254.

GONZÁLEZ NAVARRO, A., "Medios tecnológicos de investigación en el proceso penal alemán: Una visión comparada", en *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas,* Tirant lo Blanch, 2018, pp. 233-282.

GONZÁLEZ NAVARRO, A., "Servicios de inteligencia y orden europea de investigación", en *Orden europea de investigación y prueba transfronteriza en la Unión Europea, 2019*, Tirant lo Blanch, 2019, pp. 225-238.

GONZÁLEZ-CUÉLLAR SERRANO, N., *Proporcionalidad y derechos fundamentales en el proceso penal*, Constitución y Leyes, COLEX, 1990.

GONZÁLEZ-MENESES ROBLES, M., "La función notarial en el medio electrónico", *Anales de la Academia Matritense del Notariado*, n.º 52, 2012, Editoriales de Derecho Reunidas. EDERSA, pp. 47-122.

GROENLEER, M. L. P., "The autonomy of European Union Agencies. A comparative study of institutional development.", 2009, Eburon, fecha de consulta 10 abril 2022, en https://hdl.handle.net/1887/14519.

GUDIN RODRÍGUEZ-MAGARIÑOS, F., "Obtención de los códigos de identidad del teléfono móvil y del abonado (IMEI/IMSI): crónica de un caos normativo".

GUTIÉRREZ, J. L.; JIMÉNEZ, F. S.; SÁNCHEZ, D. H.; MORENO, F. M.; GARCÍA, M. R.; PÉREZ, V. G.; Y OTROS, "Estudio sobre la Cibercriminalidad en España".

HAMED ABDURRAHIM, S.; SAMAD, S. A.; HUDDIN, A. B., "Review on the effects of age, gender, and race demographics on automatic face recognition", *The Visual Computer*, vol. 34, n.º 11, 2018, pp. 1617-1630.

HAR, J., "San Francisco becomes the first US city to ban the use of facial recognition software by police", *Business Insider*.

HARRIS, T., "Cómo un grupo de compañías tecnológicas controlan billones de mentes cada día".

HEILWEIL, R., "Why we don't know as much as we should about police surveillance technology", *Vox*, 2020.

HILL, K., "The Secretive Company That Might End Privacy as We Know It", *The New York Times*, 2020.

JIMÉNEZ CONDE, F.; BELLIDO PENADES, R.; DE LUIS GARCÍA, E., *Justicia: ¿Garantías*

Versus eficiencia?

JIMÉNEZ MEJÍA, D., "La crisis de la noción material de bien jurídico en el derecho penal del riesgo", *Nuevo Foro Penal*, n.º 82, 2014, Universidad EAFIT, pp. 148-176.

JIMÉNEZ SÁNCHEZ, F., "Europol: cooperación y coordinación policial en la Unión Europea", 2015, Universidad Carlos III de Madrid, fecha de consulta 2 mayo 2022, en https://dialnet.unirioja.es/servlet/tesis?codigo=95085.

JIMÉNEZ SEGADO, C.; PUCHOL AIGUABELLA, M., "Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección datos", *Diario La Ley*, n.º 8676, 2016, Wolters Kluwer.

JUELS, A.; SUDAN, M., "A Fuzzy Vault Scheme", *Des Codes Crypt*, vol. 38, 2006, pp. 237-257.

KAPPLER, S. I. Á. DE N., "Los descubrimientos casuales en el marco de una investigación penal: (Con especial referencia a las diligencias de entrada y registro en domicilio).", *Riedpa: Revista Internacional de Estudios de Derecho Procesal y Arbitraje*, n.º 2, 2011, Del Blanco Editores, pp. 1-69.

KHAN, M.; MISHRA, A.; KHAN, M., "Cyber Forensics Evolution and Its Goals", 2020, pp. 16-30.

KLOSEK, J., "The Development of International Police Cooperation within the EU and Between the EU and Third Party States: A Discussion of the Legal Bases of Such Cooperation and the Problems and Promises Resulting Thereof", *American University International Law Review*, vol. 14, 1999, p. 59.

LANDWEHR, C.; BULL, A.; MCDERMOTT, J.; CHOI, W., "A Taxonomy of Computer Program Security Flaws", *ACM Computing Surveys - CSUR*, vol. 26, 1993.

LARSON, E., "Tracking Criminals with Internet Protocol Addresses: Is Law Enforcement Correctly Identifying Perpetrators?", *North Carolina Journal of Law & Technology*, vol. 18, 2017.

LARSON MATTU, J.; OTROS, O.; OTROS, O., "How We Analyzed the COMPAS Recidivism Algorithm", *ProPublica*.

LEBEUF, M.-E., "Organized Crime and Police Cooperation in the European Union: Lessons Learned, an Interview with Professor Cyrille Fijnaut", *Trends in Organized Crime*, vol. 7, n.º 4, 2004, pp. 55-72.

LECHER, C., "Privacy advocate held at gunpoint after license plate reader database mistake, lawsuit alleges", *The Verge*, 2019.

LERMA, E. M.; PUERTA, M. J. R., "Traducción y breve comentario del convenio sobre cibercriminalidad", *Revista de derecho y proceso penal*, n.º 7, 2002, Aranzadi Thomson Reuters, pp. 167-200.

LEVINE, E. S.; TISCH, J.; TASSO, A.; JOY, M., "The New York City Police Department's Domain Awareness System", *INFORMS Journal on Applied Analytics*, vol. 47, n.º 1, 2017, INFORMS, pp. 70-84.

LIBERATORE, M.; ERDELY, R.; KERLE, T.; LEVINE, B. N.; SHIELDS, C., "Forensic investigation of peer-to-peer file sharing networks", *Digital Investigation*, vol. 7, 2010, (The Proceedings of the Tenth Annual DFRWS Conference), pp. S95-S103.

LLOVERAS SOLER, J. M., "Capitalismo de control", *Alternativas económicas*, n.º 80, 2020, SGEL: Sociedad General Española de Librería.

LÓPEZ, A., "La investigación policial en Internet: estructuras de cooperación internacional", *IDP: revista de Internet, derecho y política = revista d'Internet, dret i política*, n.º 5, 2007, Universitat Oberta de Catalunya.

LÓPEZ-BARAJAS PEREA, I., "Eficacia probatoria de las medidas de investigación tecnológica del delito", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum,* Ediciones Jurídicas Castillo de Luna, 2020, pp. 1029-1056.

LUACES GUTIÉRREZ, A. I., "La conformidad en el Anteproyecto de Ley de Medidas de Eficiencia Procesal del Servicio Público de Justicia", en *El impacto de la oportunidad sobre los principios procesales clásicos: Estudios y diálogos,* Iustel, 2021, pp. 289-308.

LUACES GUTIÉRREZ, A. I., "La preinstrucción de la Policía Judicial en los juicios rápidos",

La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía, n.º 4, 2004, Wolters Kluwer, pp. 1541-1548.

LUCENA CID, I. V., "La protección de la intimidad en la era teconlógica: hacia una reconceptualización", *Revista internacional de pensamiento político*, n.º 7, 2012, Laboratorio de Ideas y Prácticas Políticas, pp. 117-144.

MAEZTU, D., "Cartas que reclaman por descargar mediante sistemas P2P. ¿Qué hago? Razones para no pagar.".

MAEZTU, D., "El rastreo de usuarios en internet por la policia. Sentencia del TS 236/2008", fecha de consulta 2 mayo 2020, .

MAEZTU, D., "La identificación por la IP y la reforma de la LPI".

MAFFEI, L., *Alabanza de la lentitud*, Alianza, Madrid, 2016.

MAGHERESCU, D., "Challenges of the forensic science facing new technologies", *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, vol. 7, n.º 1, 2021, Universidad de Sevilla, pp. 48-61.

MANGAS MARTÍN, A., "La reforma institucional en el Tratado de Amsterdam", *Revista de Derecho Comunitario Europeo*, vol. 2, n.º 3, 1998, Centro de Estudios Políticos y Constitucionales (España), pp. 7-40.

MANGAS MARTÍN, A., "Las cooperaciones reforzadas en el Tratado de Niza", en *Tratado de Niza: análisis, comentarios y texto*, 2002, pp. 67-82, fecha de consulta 28 abril 2022, en https://dialnet.unirioja.es/servlet/articulo?codigo=4800496.

MARCHAL ESCALONA, A. N., "Competencia como policía judicial en el proceso penal", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum*, Ediciones Jurídicas Castillo de Luna, 2020, pp. 1163-1180.

MARCHENA GÓMEZ, M., "Grabaciones entre particulares y prueba prohibida", *Revista de derecho y proceso penal*, n.º 52, 2018, Aranzadi Thomson Reuters, pp. 393-400.

MARCHENA GÓMEZ, M., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Ediciones Jurídicas Castillo de Luna, Madrid, 2015.

MARCHENA GÓMEZ, M., "Prueba ilícita y reglas de exclusión: los matices introducidos por la Sala Penal del Tribunal Supremo en la Sentencia 116/2007, 23 de febrero (Caso Falciani)", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum,* Ediciones Jurídicas Castillo de Luna, 2020, pp. 1181-1200.

MARTÍN DE LA ESCALERA, A. M., "El registro de dispositivos de almacenamiento masivo de la información", *Revista del Ministerio Fiscal*.

MARTÍN DIZ, F., "Delincuencia organizada y procesos penales supranacionales: el caso de la Unión Europea", *Pensamiento jurídico*, n.º 21, 2008, Universidad Nacional de Colombia, pp. 191-242.

MARTÍN DIZ, F., "El derecho fundamental a justicia: Revisión integral e integradora del derecho a la tutela judicial efectiva", *Revista de derecho político*, n.º 106, 2019, Universidad Nacional de Educación a Distancia – UNED, pp. 13-42.

MARTÍN DIZ, F., "Herramientas de inteligencia artificial y adecuación en el ámbito del proceso judicial", en *Derecho procesal: retos y transformaciones,* Atelier, 2021, pp. 295-304.

MARTÍN DIZ, F., "Inteligencia artificial y derecho procesal: luces, sombras y cábalas en clave de derechos fundamentales", en *Nuevos postulados de la cooperación judicial en la Unión Europea: libro homenaje a la Prof.ª Isabel González Cano, 2021,* Tirant lo Blanch, 2021, pp. 969-1006.

MARTÍN DIZ, F., "Justicia digital post-covid19: El desafío de las soluciones extrajudiciales electrónicas de litigios y la inteligencia artificial", *Revista de Estudios Jurídicos y Criminológicos*, n.º 2, 2020, Universidad de Cádiz, pp. 41-74.

MARTÍN DIZ, F., "Modelos de aplicación de Inteligencia Artificial en justicia: asistencial o predictiva versus decisoria", en *Justicia algorítmica y neuroderecho: una mirada multidisciplinar,* Tirant lo Blanch, 2021, pp. 65-85, fecha de consulta 30 noviembre 2021.

MARTÍN DIZ, F., "Presunción de inocencia como derecho fundamental en el ámbito de la Unión Europea", *Revista europea de derechos fundamentales*, n.º 18, 2011,

Instituto de Derecho Público, pp. 133-166.

MARTÍN DIZ, F., "Propuesta de un modelo procesal penal europeo para delitos transfronterizos", en *Estudios procesales sobre el espacio europeo de justicia penal*, Aranzadi, 2021, pp. 51-71.

MARTÍN RÍOS, P., "Cuestiones procesales que plantea el empleo de drones y de ortofotografía digital en la investigación de delitos urbanísticos", en *Drones, investigación y medio ambiente,* Atelier, 2021, pp. 111-127.

MARTÍN RÍOS, P., "El alcance del derecho al propio entorno virtual en la valoración de la evidencia digital", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum,* Ediciones Jurídicas Castillo de Luna, 2020, pp. 1259-1270.

MARTÍN RÍOS, P., "El necesario enfoque procesal de la Digital Forensics", en *El sistema jurídico ante la digitalización. Estudios de Derecho Público y Criminología,* Tirant lo Blanch, 2021, pp. 265-286.

MARTÍN RÍOS, P., "El "primer acceso policial" a dispositivos de almacenamiento digital, o de cuando las garantías se supeditan a la búsqueda de la eficiencia", en *Justicia: ¿garantías "versus" eficiencia?,* Tirant lo Blanch, 2019, pp. 839-846.

MARTÍN RÍOS, P., "El uso de las nuevas tecnologías en la lucha contra los delitos urbanísticos", *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, vol. 6, n.º 2, 2020, Universidad de Sevilla, pp. 11-25.

MARTÍN RÍOS, P., "El valor probatorio de información obtenida de un ordenador de uso compartido: a propósito de la STS 287/2017", en *Exclusiones probatorias en el entorno de la investigación y prueba electrónica,* Reus, 2020, pp. 327-338.

MARTÍN RÍOS, P., "La colaboración del investigado/encausado en el registro de dispositivos de almacenamiento masivo de información: ¿un supuesto de autoincriminación?", en *FODERTICS 6.0: los nuevos retos del derecho ante la era digital,* Comares, 2017, pp. 149-161.

MARTÍN RÍOS, P., "La indemnidad del domicilio informático como posible límite a la

digital forensics", en *Giustizia e Costituzione agli albori del XXI Secolo*, Bonomo Editore, Bolonia, Italia, 2017, pp. 1279-1284.

MARTÍN RÍOS, P., "Problemas de admisibilidad de la prueba obtenida de dispositivos de almacenamiento digital", *Revista General de Derecho Procesal*, n.º 51, 2020, Iustel, p. 5.

MARTÍNEZ SANTOS, A., "Terrorismo, proceso penal y derechos fundamentales", *Cuestiones constitucionales*, n.º 29, 2013, Instituto de Investigaciones Jurídicas, UNAM, pp. 459-466.

MASELLAS, R., "El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre – InDret".

MATIA PORTILLA, F. J., "Delito flagrante e inviolabilidad del domicilio (Comentario a la STC 341/1993)", *Revista española de derecho constitucional*, vol. 14, n.º 42, 1994, Centro de Estudios Políticos y Constitucionales (España), pp. 197-217.

MENDIZABAL, R. T.; GUILLÉN, J. F.; PÉREZ, J. C., "La obtención de la prueba electrónica, su acceso al proceso civil y la garantía de derechos en material penal", *Economist & Jurist*, vol. 20, n.º 163, 2012, Global Economist & Jurist, pp. 26-40.

MERCHÁN MURILLO, A., "Cloud computing: soluciones ante un posible conflicto de leyes", *La Ley mercantil*, n.º 48 (junio), 2018, Wolters Kluwer, fecha de consulta 4 abril 2020.

MERKEL, L., *Derechos humanos e investigaciones policiales*, Marcial Pons, Madrid, 2022, Madrid.

MIRÓ LLINARES, F., "Predictive policing: utopia or dystopia? On attitudes towards the use of big data algorithms for law enforcement", *IDP: revista de Internet, derecho y política = revista d'Internet, dret i política*, n.º 30, 2020, Universitat Oberta de Catalunya.

MONSERRAT COLL, FRANCISCO JESÚS, "PED: Red de equipos trama de REdIRIS".

MONTERROSSO CASADO, E.; MUÑOZ VILLARREAL, A.; ÁLVAREZ OLALLA, M. P., *Inteligencia artificial y riesgos cibernéticos: responsabilidades y aseguramiento*,

Tirant lo Blanch, Valencia, 2019.

MONTORO SÁNCHEZ, J. A., "Breve análisis acerca del futuro reglamento comunitario «e-evidence» sobre las órdenes europeas de conservación y entrega de pruebas y evidencias electrónicas a efectos de enjuiciamiento penal", en *Orden europea de investigación y prueba transfronteriza en la Unión Europea*, Tirant lo Blanch, 2019, pp. 169-181.

MORATINOS, G. L., "Modelos algorítmicos, sesgos y discriminación", en *FODERTICS 9.0: Estudios sobre tecnologías disruptivas y justicia*, Comares, 2021, pp. 283-294.

MORENO CATENA, V. M., "El mito de la instrucción dirigida por el juez", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum*, Ediciones Jurídicas Castillo de Luna, 2020, pp. 1339-1364.

MUERZA ESPARZA, J. J., "Sobre la prueba testifical del menor-víctima en el proceso penal de mayores", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum*, Ediciones Jurídicas Castillo de Luna, 2020, pp. 1365-1378.

MUÑOZ CONDE, F., "Prueba prohibida y valoración de las grabaciones audiovisuales en el proceso penal", *Revista penal*, n.º 14, 2004, Tirant lo Blanch, pp. 96-123.

MUÑOZ, R., "Más de 40 millones de teléfonos móviles serán usados para rastrear el coronavirus en toda España", *EL PAÍS*, 2020.

NADAL GÓMEZ, I., "El Régimen de los hallazgos casuales en la Ley 13/2015, de modificación de la ley de Enjuiciamiento criminal", *Revista General de Derecho Procesal*, n.º 40, 2016, Iustel.

NEGRIN MENDOZA, P., "El Ministerio Fiscal como órgano instructor en el Anteproyecto de la Ley de Enjuiciamiento Criminal 2020".

NIEVA FENOLL, J., "El discutido valor probatorio de las diligencias policiales", *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía*, n.º 4, 2007, Wolters Kluwer, pp. 1652-1666.

NIEVA FENOLL, J., *Inteligencia artificial y proceso judicial*, Marcial Pons, Madrid, 2018.

NIEVA FENOLL, J., "La instrucción como falsa "primera instancia" del proceso penal: La instrucción como falsa "primera instancia" del proceso penal", *Revista ítalo-española de Derecho Procesal*, n.º 1, 2019, Marcial Pons, pp. 39-56.

NIEVA FENOLL, J., "La protección de derechos fundamentales en las diligencias policiales de investigación del proceso penal", *La ley penal: revista de derecho penal, procesal y penitenciario*, n.º 50, 2008, Wolters Kluwer, pp. 81-101.

NIEVA FENOLL, J., "Orden europea de investigación: autoridades competentes en el estado emisor y de ejecución, especial consideración del papel del ministerio fiscal", en *Orden europea de investigación y prueba transfronteriza en la Unión Europea*, Tirant lo Blanch, 2019, pp. 437-456.

NIEVA FENOLL, J., "Policía judicial y prueba ilícita. Regla de exclusión y efecto disuasorio: un error de base", *Diario La Ley*, n.º 9068, 2017, Wolters Kluwer.

NIEVA FENOLL, J., "Tecnología y derechos fundamentales en el proceso judicial", en *Nuevos postulados de la cooperación judicial en la Unión Europea: libro homenaje a la Prof.ª Isabel González Cano*, Tirant lo Blanch, 2021, pp. 1007-1033.

NIEVA FENOLL, J., "Inteligencia artificial y proceso judicial: perspectivas tras un alto tecnológico en el camino", en *Revista General de Derecho Procesal*, n.o 57, 2022, Iustel.

NOYA FERREIRO, M. L., "Dificultades probatorias en los delitos de violencia de género", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum*, Ediciones Jurídicas Castillo de Luna, 2020, pp. 1415-1432.

ORTEGA, A.; BALSA-BARREIRO, J.; CEBRIÁN, M., "The limits of surveillance capitalism", 2020.

ORTEGA GIMÉNEZ, A.; GONZÁLEZ MARTÍNEZ, J. A., "Protección de datos, secreto de las comunicaciones, utilización del correo electrónico por los trabajadores y control empresarial", *Diario La Ley*, n.º 7188, 2009, Wolters Kluwer, p. 1.

ORTIZ PRADILLO, J. C., "Cibercrimen y conflictos de jurisdicción penal: una cuestión por

resolver", en *Temas actuales en la persecución de los hechos delictivos,* 2012, pp. 501-539.

ORTIZ PRADILLO, J. C., "Comunicaciones,tecnologías y proceso penal: Viejos delitos, nuevas necesidade", en *Justicia penal y nuevas formas de delincuencia,* Servei de Publicacions, 2017, pp. 15-28.

ORTIZ PRADILLO, J. C., "Desafíos legales de las diligencias de investigación tecnológica", en *El proceso penal: Cuestiones fundamentales,* Tirant lo Blanch, 2017, pp. 279-291.

ORTIZ PRADILLO, J. C., "El impacto de la tecnología en la investigación penal y en los derechos fundamentales", en *Problemas actuales de la justicia penal*, Colex, Madrid, 2013, pp. 317-343.

ORTIZ PRADILLO, J. C., "El registro «on line» de equipos informáticos como medida de investigación contra el terrorismo (online durchsuchung)", en *Terrorismo y estado de derecho, I*ustel, 2010, pp. 457-478.

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*, n.º 52, 2020, Iustel.

ORTIZ PRADILLO, J. C., "«Hacking» legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática", *Revista de derecho y proceso penal*, n.º 26, 2011, Aranzadi Thomson Reuters, pp. 67-92.

ORTIZ PRADILLO, J. C., "Informática y derechos fundamentales: hacia un derecho fundamental a la confidencialidad e integridad de los equipos informáticos", en *El derecho en la sociedad telemática: estudios en homenaje a Valentín Carrascosa López,* Andavira, 2012, pp. 57-86.

ORTIZ PRADILLO, J. C., "Investigación policial sobre dispositivos y control judicial en la reforma de la justicia penal", en *Legalidad y defensa: garantías constitucionales del derecho y la justicia penal*Ediciones Jurídicas Castillo de Luna, 2015, pp. 283-310.

ORTIZ PRADILLO, J. C., *La investigación del delito en la era digital: los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación*, 2013.

ORTIZ PRADILLO, J. C., "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica", en *El proceso penal en la sociedad de la información: las nuevas tecnologías para investigar probar el delito,* La Ley (España), 2012, pp. 267-310.

ORTIZ PRADILLO, J. C., *Problemas procesales de la ciberdelincuencia*, Colex, Majadahonda (Madrid), 2013.

PANTALEÓN, F., "Arrendamiento de local de negocio y suspensión legal de actividades empresariales", *Almacén de Derecho*.

PASTOR, J., "Apple, Google, coronavirus y privacidad: una tormenta perfecta que plantea si es peor el remedio que la enfermedad", *Xataka*, 2020, fecha de consulta 14 abril 2020, en https://www.xataka.com/medicina-y-salud/apple-google-coronavirus-privacidad-tormenta-perfecta-que-plantea-peor-remedio-que-enfermedad.

PÉREZ COLOMÉ, J., "Marbella, el mayor laboratorio de videovigilancia de España", *El País*, 2019, Madrid, fecha de consulta 3 mayo 2020, en https://elpais.com/tecnologia/2019/11/21/actualidad/1574348695_231540.html.

PÉREZ COLOMÉ, J., "Palantir, misterioso proveedor del Pentágono y la CIA, ofrece a España sus servicios contra el coronavirus", *EL PAÍS*, 2020.

PÉREZ DAUDÍ, V., "La prueba electrónica: naturaleza jurídica e impugnación", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum*, Ediciones Jurídicas Castillo de Luna, 2020, pp. 1557-1576.

PÉREZ DE LOS COBOS ORIHUELA, F., *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de derecho comparado : Consejo de Europa : estudio*, 2018.

PÉREZ FRANCESCH, J. L., "El tratado de Lisboa: cooperación policial y judicial entre la europeización y las reservas estatales", en *Diálogos y desafíos euro-latinoamericanos: ensayos sobre cooperación derecho, educación y comunicación,* Ediciones

Uninorte, 2010, pp. 80-111, fecha de consulta 28 abril 2022, en https://dialnet.unirioja.es/servlet/articulo?codigo=4409625.

PAVÓN PÉREZ, J. A., "La labor del Consejo en Europa en la lucha contra la cibercriminalidad: El protocolo adicional al convenio nº 185 sobre cibercriminalidad relativo a la incriminación de actos de naturaleza racista y xenófobos cometidos a través de los sistemas informáticos", *Anuario de la Facultad de Derecho. Universidad de Extremadura*, n.º 21, 2003, Servicio de Publicaciones, pp. 187-204.

PÉREZ ROMERO, J. M., "Obtención eficaz de la prueba transfronteriza en la Unión Europea", 2020, UNED. Universidad Nacional de Educación a Distancia, p. 1, fecha de consulta 7 mayo 2022, en https://dialnet.unirioja.es/servlet/tesis?codigo=283874.

PERRON, W., "Aspectos universales y sistémicos del derecho de la prueba en el proceso penal", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum*, Ediciones Jurídicas Castillo de Luna, 2020, pp. 1593-1604.

PINTO PALACIOS, F., *La prueba en la era digital*, La Ley Wolters Kluwer, Madrid, 2017.

PONS GAMON, V., "Ciberterrorismo: amenaza a la seguridad. Respuesta operativa y legislativa, nacional e internacional", 2018, UNED. Universidad Nacional de Educación a Distancia (España), p. 1.

POOL, R. L. D.; CUSTERS, B. H. M., "The police hack back: legitimacy, necessity and privacy implicationis of the next step in fighting cybercrime", *European Journal of Crime, Criminal Law and Criminal Justice*, vol. 25, n.º 2, 2017, Martinus Nijhoff Publishers, pp. 123-144.

POSTEL, J., "DoD standard Internet Protocol".

POSTEL, J., "Internet Protocol".

Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la Agencia de la Unión Europea para la cooperación y la formación en funciones coercitivas (Europol) y por el que se derogan las Decisiones 2009/371/JAI y 2005/681/JAI, 2013, fecha de consulta 4 mayo 2022, en

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52013PC0173.

QUEVEDO GONZÁLEZ, J., *Investigación y prueba del ciberdelito*, Sepín, Madrid, 2017.

QUEVEDO GONZÁLEZ, J. M., "Investigación y prueba del ciberdelito", 2017, Universitat de Barcelona, fecha de consulta 7 mayo 2022, en https://dialnet.unirioja.es/servlet/tesis?codigo=230669.

RAMÓN ARECES, F., "Más transparencia sobre el uso de los algoritmos", *Revista de Occidente*, n.º 479, 2021, Pertenece a ARCE, pp. 137-140.

RAMONET, I., *El imperio de la vigilancia*, Clave intelectual, Madrid, 2015.

RATCLIFFE, J., *Intelligence-led policing*, Australian Institute of Criminology, Canberra, 2003.

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*, n.º 52, 2019, pp. 179-204.

RAYÓN BALLESTEROS, M. C.; GÓMEZ HERNÁNDEZ, J. A., "Cibercrimen: particularidades en su investigación y enjuiciamiento", *Anuario jurídico y económico escurialense*, n.º 47, 2014, Real Centro Universitario Escorial-María Cristina, pp. 209-234.

Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo, vol. 135, 2016, fecha de consulta 4 mayo 2022, en http://data.europa.eu/eli/reg/2016/794/oj/spa.

REMOTTI CARBONELL, J. C., *Constitución y medidas contra el terrorismo. La suspensión individual de derechos y garantías*, Colex, A Coruña, 1999, fecha de consulta 15 marzo 2022, en https://dialnet.unirioja.es/servlet/articulo?codigo=8127711.

REMOTTI CARBONELL, J. C., "El proceso de formación del espacio de libertad, seguridad

y justicia en la Unión Europea. La lucha contra la delincuencia, cooperación policial y judicial y garantías del debido proceso en el ámbito penal", en *Garantías del proceso debido y Unión Europea: implicaciones para los ordenamientos internos*, Centro de Estudios Políticos y Constitucionales (España), 2020, pp. 21-70, fecha de consulta 28 febrero 2022, en https://dialnet.unirioja.es/servlet/articulo?codigo=7765253.

REMOTTI CARBONELL, J. C., "Las medidas contra el terrorismo en el marco del Tratado de Prüm", *Revista de derecho constitucional europeo*, n.º 7, 2007, Instituto Andaluz de Administración Pública, pp. 181-206.

Resumen del Dictamen del Supervisor Europeo de Protección de Datos sobre las dos Propuestas de Decisiones del Consejo por las que se autoriza a los Estados miembros a firmar y ratificar, en interés de la Unión Europea, el Protocolo adicional segundo al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas, fecha de consulta 4 mayo 2022, en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv%3AOJ.C_.2022.182.01.0015.01.SPA&toc=OJ%3AC%3A2022%3A182%3ATOC.

REVENGA SÁNCHEZ, M., "El derecho a la intimidad: un derecho en demolición (y necesitado de reconstrucción)", en *El derecho a la privacidad en un nuevo entorno tecnológico: XX Jornadas de la Asociación de Letrados del Tribunal Constitucional*, 2016, pp. 71-98.

RICE, S., "Eyes In The Sky: The Public Has Privacy Concerns About Drones", *Forbes*.

RICHARD GONZÁLEZ, M., "Conductas susceptibles de ser intervenidas por medidas de investigación electrónica: presupuestos para su autorización", *Diario La Ley*, n.º 8808, 2016, Wolters Kluwer.

RICHARD GONZÁLEZ, M., "La investigación y prueba de hechos y dispositivos electrónicos", *Revista General de Derecho Procesal*, n.º 43, 2017, Iustel.

RICHARDSON, R.; SCHULTZ, J.; CRAWFORD, K., "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice", 2019.

RICHELSON, J., *The U.S. Intelligence Community*, Hachette UK, 2015.

RIPOLL NAVARRO, R.; TERRÁDEZ SALOM, D.; BELLIDO BARRIONUEVO, M., *La Unión Europea Organización y Funcionamiento*, Tirant lo Blanch, Valencia, 2015.

RIVES SEVA, A. P., *La prueba en el proceso penal. Doctrina de la Sala Segunda del Tribunal Supremo.*

ROBINSON, N.; DISLEY, E.; POTOGLOU, D.; REDING, A.; CULLEY, D. M.; PENNY, M.; Y OTROS, "Feasibility Study for a European Cybercrime Centre", 2012, RAND Corporation.

RODRÍGUEZ ÁLVAREZ, A., "Proceso penal y redes sociales: aportación por las partes de la información contenida en ellas", en *El proceso penal: Cuestiones fundamentales*, Tirant lo Blanch, 2016, pp. 339-348.

RODRÍGUEZ ÁLVAREZ, A., "Redes sociales y proceso penal: una radiografía", en *El nuevo proceso penal sin Código Procesal Penal*, Atelier, 2019, pp. 321-346.

RODRÍGUEZ LAINZ, J. L., "Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas", *Diario La Ley*, n.º 7086, 2009, Wolters Kluwer.

RODRÍGUEZ LAINZ, J. L., *El secreto de las telecomunicaciones y su interceptación legal*, Sepín.

RODRÍGUEZ LAINZ, J. L., "GPS y balizas policiales", *Diario La Ley*, n.º 8416, 2014, Wolters Kluwer.

RODRÍGUEZ LAINZ, J. L., "Intervención de las comunicaciones a través de servicios de la sociedad de la información", *El Blog Jurídico de Sepín*.

RODRÍGUEZ LAINZ, J. L., "La STJUE de 2 de marzo de 2021 (Caso Prokuratur): ¿Una simple secuela de la Sentencia del Caso la Quadraute du Net sobre conservación de datos relativos a las comunicaciones electrónicas?", *Diario La Ley*, n.º 9835, 2021, Wolters Kluwer.

RODRÍGUEZ LAINZ, J. L., "Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre conservación de datos relativos a las

comunicaciones", *Diario La Ley*, n.º 8308, 2014, Wolters Kluwer.

RODRÍGUEZ LAINZ, J. L., "Sobre la naturaleza formal del derecho al secreto de las comunicaciones: dimensión constitucional e histórica", *Diario La Ley*, n.º 7647, 2011, Wolters Kluwer.

RODRÍGUEZ PADRÓN, C., "El anteproyecto de Ley de Enjuiciamiento Criminal: implicaciones orgánicas", *Diario La Ley*, n.º 9826, 2021, Wolters Kluwer.

RODRÍGUEZ RODRÍGUEZ, Y., "Inteligencia de fuentes abiertas (osint): Características, debilidades y engaño", *Análisis GESI*, n.º 11, 2019, Departamento de Ciencia Política y de la Administración.

ROMERO PAREJA, A., "Intervención de las comunicaciones", *Diario La Ley*, n.º 7816, 2012, Wolters Kluwer.

ROSALES LEAL, M. Á., "Captación y grabación de comunicaciones orales directas", *Revista de derecho constitucional europeo*, n.º 30, 2018, Instituto Andaluz de Administración Pública.

RUBIO, I., "Reconocimiento facial: la tecnología que lo sabe todo", *El País*, 2019, Madrid, fecha de consulta 4 mayo 2020, en https://elpais.com/tecnologia/2019/05/21/actualidad/1558455279_966010.html.

RUBIO VIÑUELA, Y.; BREZO FERNÁNDEZ, F., "La utilización de herramientas de monitorización de usuarios como base para el perfilado de identidades en fuentes abiertas: OSRFramework", en *Actas de las primeras Jornadas Nacionales de Investigación en Ciberseguridad: León, 14, 15, 16 de septiembre de 2015. I JNIC2015*, Servicio de Publicaciones, 2015, pp. 32-38.

RUMMELL, N., "Groups Demand to See Criteria for NYPD Gang Database".

SAN JUAN GUILLÉN, C., "Criminología ambiental: un área en expansión", *Ars Iuris Salmanticensis: AIS : revista europea e iberoamericana de pensamiento y análisis de derecho, ciencia política y criminología*, vol. 1, n.º 1, 2013, Ediciones Universidad de Salamanca, pp. 33-38.

SAN MIGUEL CASO, C., "La aplicación de la Inteligencia Artificial en el proceso: ¿un

nuevo reto para las garantías procesales?", *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, vol. 7, n.º 1, 2021, Universidad de Sevilla, pp. 286-303.

SÁNCHEZ GUARIDO, A.; MEDINA, A. M., "El TJUE reabre el debate entre privacidad o seguridad nacional", *Diario La Ley*, n.º 9743, 2020, Wolters Kluwer.

SILVA SÁNCHEZ, J. M., "La responsabilidad penal de las personas jurídicas en el convenio del consejo de Europa sobre cibercriminalidad", *Cuadernos de derecho judicial*, n.º 9, 2002, Consejo General del Poder Judicial, pp. 113-142.

SÁNCHEZ MELGAR, J., "La nueva regulación de las medidas de investigación tecnológica. Estudio de su Parte General", *Práctica penal: cuaderno jurídico*, n.º 82, 2016, Sepin Editorial Jurídica, pp. 20-32.

SÁNCHEZ RUBIO, A., *La Prueba científica en la justicia penal*, Tirant lo Blanch, Valencia, 2019.

SÁNCHEZ SISCART, J. M., "A vueltas con el secreto de las comunicaciones: Algunos supuestos críticos en la jurisprudencia de la Sala 2.ª del Tribunal Supremo", *Diario La Ley*, n.º 7338, 2010, Wolters Kluwer.

SANCHÍS CRESPO, C., "La prueba en soporte electrónico", en *Las tecnologías de la información y la comunicación en la administración de justicia: análisis sistemático de la Ley 18/2011, de 5 de julio*, Thomson Reuters Aranzadi, 2012, pp. 707-734.

SANJURJO RÍOS, E. I., "Proceso penal y volatilidad/mutabilidad de las fuentes de pruebas electrónicas: sobre la conveniencia y el modo de asegurarlas eficazmente", en *Exclusiones probatorias en el entorno de la investigación y prueba electrónica, 2020*, Reus, 2020, pp. 195-224.

SANZ HERMIDA, Á. M. [A], "Presunción de inocencia y prisión provisional a la luz de la Directiva (UE) 2016/343", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum*, Ediciones Jurídicas Castillo de Luna, 2020, pp. 1841-1860.

SHAIK, A.; BORGAONKAR, R.; ASOKAN, N.; NIEMI, V.; SEIFERT, J.-P., "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems",

arXiv:1510.07563 [cs], 2015, fecha de consulta 19 enero 2021, en http://arxiv.org/abs/1510.07563.

STANLEY, JAY, "The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy", 2019, fecha de consulta 4 mayo 2020, en https://www.aclu.org/sites/default/files/field_document/061119-robot_surveillance.pdf.

TAYLOR, E.; HOFFMANN, S., "EU–US Relations on Internet Governance", fecha de consulta 14 abril 2020, en https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-14-EU-US-Relations-Internet-Governance2.pdf.

TÉLLEZ CARVAJAL, E., "Derechos humanos, ética y transparencia algorítmica", *IUS ET SCIENTIA*, vol. 7, n.º 1, 2021, pp. 370-386.

URIARTE VALIENTE, L. M., "Nuevas técnicas de investigación restrictivas de derechos fundamentales", fecha de consulta 8 abril 2020, en https://docplayer.es/56647100-Nuevas-tecnicas-de-investigacion-restrictivas-de-derechos-fundamentales-luis-m-uriarte-valiente-fiscal.html.

VALIÑO CES, A., "Una lectura crítica en relación al agente encubierto informático tras la Ley Orgánica 13/2015", *Diario La Ley*, n.º 8731, 2016, Wolters Kluwer, p. 3.

VALLÉS CAUSADA, L., "La investigación criminal basada en datos conservados de las comunicaciones electrónicas - Blog de Criminología - Iter Criminis", 2018.

VALLÉS CAUSADA, L., "La polícia judicial en la obtención de inteligencia sobre comunicaciones electrónicas para el proceso penal", 2012, UNED. Universidad Nacional de Educación a Distancia (España).

VÁZQUEZ SECO, L., "Retención obligatoria de datos de tráfico de las comunicaciones telefónicas y/o electrónicas. Análisis de la sentencia del Tribunal de Justicia de la Unión Europea de 8 de abril de 2014 en los asuntos acumulados C-293/2012 y C-594/2012 (Digital Rights Ireliand y Seitlinger y otros)".

VEALE, M.; EDWARDS, L., "Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling", *Computer Law & Security Review*, vol. 34, n.º 2, 2018, pp. 398-404.

VEBLEN, T.; MELLIZO, C., *Teoría de la clase ociosa*, Alianza, 2004.

VEGA, G., "La UE plantea prohibir hasta cinco años el reconocimiento facial en lugares públicos", *El País*, 2020, Madrid.

VEGAS TORRES, J., "Obtención de pruebas en ordenadores personales y derechos fundamentales en el ámbito de la empresa", 2011, Cátedra de Investigación Financiera y Forense KPMG-URJC.

VEGAS TORRES, J., "Sobre el alcance del secreto de las comunicaciones", en *Una filosofía del derecho en acción: homenaje al profesor Andrés Ollero*Dirección de Estudios, Análisis y Publicaciones. Departamento de Publicaciones, 2015, pp. 1609-1626.

VEGAS TORRES, J., "Sobre la licitud de las pruebas obtenidas por las empresas mediante el control de las comunicaciones electrónicas de los trabajadores", en *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020,* Ediciones Jurídicas Castillo de Luna, 2020, pp. 1963-1982.

VELASCO NÚÑEZ, E., "ADSL y troyanos: intervención de sus datos y telecomunicaciones en la investigación penal", *La ley penal: revista de derecho penal, procesal y penitenciario*, n.º 82, 2011, Wolters Kluwer.

VELASCO NÚÑEZ, E., "Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos", en *Investigación Tecnológica y Derechos Fundamentales*, Aranzadi, Navarra, 2017.

VELASCO NÚÑEZ, E., "Crimen organizado, internet y nuevas tecnologías", en *Los retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso Gallego de Derecho Procesal (I Internacional), A Coruña, 2 y 3 de junio de 2011*, 2012, pp. 245-282.

VELASCO NÚÑEZ, E., *Delincuencia informática: tipos delictivos e investigación : con jurisprudencia tras la reforma procesal y penal de 2015*, Tirant lo Blanch, Valencia, 2019.

VELASCO NÚÑEZ, E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*.

VELASCO NÚÑEZ, E., "Derecho a la imagen: tratamiento procesal penal", *Diario La Ley*, n.º 8596, 2015, Wolters Kluwer.

VELASCO NÚÑEZ, E., "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica", *Diario La Ley*, n.º 8183, 2013, Wolters Kluwer.

VELASCO NÚÑEZ, E., "La investigación de delitos cometidos a través de Internet y otras nuevas tecnologías: cuestiones procesales", 2010, Universidade da Coruña.

VELASCO NÚÑEZ, E., "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías - El Derecho - Fiscal, Penal, Sector Jurídico", *El Derecho*.

VIDAL-FOLCH, X., "Europol, más que Interpol, menos que el FBI", *El País*, 1996, Madrid, fecha de consulta 2 mayo 2022, en https://elpais.com/diario/1996/07/14/internacional/837295206_850215.html.

WILLIAMS, M.; EDWARDS, A.; HOUSLEY, W.; BURNAP, P.; RANA, O.; AVIS, N.; Y OTROS, "Policing Cyber-Neighbourhoods: Tension Monitoring and Social Media Networks", *Policing and Society*, vol. 23, 2013, pp. 1-21.

WINSTON, A., "Vague Rules Let ICE Deport Undocumented Immigrants as Gang Members", *The Intercept*.

YADAV, S., "Cyber Forensics: Its Importance, Cyber Forensics Techniques, and Tools", 2020, pp. 1-15.

ZARAGOZA TEJADA, J. I., "La investigación de la dirección IP tras la Reforma operada por Ley 13/2015", *Revista Aranzadi Doctrinal*, n.º 2, 2017, Thomson Reuters Aranzadi.

GUTIÉRREZ ZARZA, M. A., "La incorporación al proceso penal de la información facilitada por las autoridades administrativas o policiales de otros Estados miembros, por Europol y Eurojust", en *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios*, Aranzadi Thomson Reuters, 2017, pp. 175-199, fecha de consulta 6 mayo 2022, en https://dialnet.unirioja.es/servlet/articulo?codigo=6161416.

ZUBOFF, S., *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, PublicAffairs, Estados Unidos, 2019.

WEBGRAFÍA

"3G-GSM Tactical Interception & Target Location", fecha de consulta 5 mayo 2020, en https://info.publicintelligence.net/Gamma-GSM.pdf.

"2019_NewYorkPolicyTechnology.pdf", fecha de consulta 2 mayo 2020, en https://www.brennancenter.org/sites/default/files/2019-10/2019_NewYorkPolicyTechnology.pdf.

"A Tech Fix For Illegal Government Snooping?", *NPR.org*, fecha de consulta 19 marzo 2020, en https://www.npr.org/templates/story/story.php?storyId=106479613.

"About 3GPP Home", fecha de consulta 15 abril 2020, en https://www.3gpp.org/about-3gpp/about-3gpp.

"Acerca de Europol", *Europol*, fecha de consulta 1 mayo 2020, en https://www.europol.europa.eu/es/about-europol.

"Acuerdo del 23 de febrero de 2010, sobre la necesidad de autorización judicial para la cesión de datos de las operadoras de comunicaciones", fecha de consulta 16 enero 2021, en https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunal-Supremo/Jurisprudencia-/Acuerdos-de-Sala/Acuerdo-del-23-de-febrero-de-2010--sobre-la-necesidad-de-autorizacion-judicial-para-la-cesion-de-datos-de-las-operadoras-de-comunicaciones.

"Acuerdos fundacionales", fecha de consulta 26 marzo 2022, en https://european-union.europa.eu/principles-countries-history/principles-and-values/founding-agreements_es.

"AFRINIC - Regional Internet Registry for Africa", *AFRINIC - Regional Internet Registry for Africa*, fecha de consulta 14 abril 2020, en https://www.afrinic.net/.

"AI Global Surveillance (AIGS) Index", .

"American Registry for Internet Numbers", fecha de consulta 14 abril 2020, en https://www.arin.net/.

"APNIC", fecha de consulta 14 abril 2020, en https://www.apnic.net/.

"ARPANET | Real Academia de Ingeniería", fecha de consulta 20 abril 2020, en http://diccionario.raing.es/es/lema/arpanet.

"Así funciona el reconocimiento facial y por qué debería preocuparte", *ELMUNDO*, 2020, fecha de consulta 3 mayo 2020, en https://www.elmundo.es/tecnologia/2020/02/24/5e4fb4c3fc6c83821f8b4642.html.

"Aspectos juridicos de la direccion de residencias", .

"Autopsy Training", fecha de consulta 21 abril 2020, en https://training.autopsy.com/courses/take/autopsy-basics-8-hours/lessons/9545972-video.

"Beginner's Guides - ICANN", fecha de consulta 14 abril 2020, en https://www.icann.org/resources/pages/beginners-guides-2012-03-06-en.

"Byung-Chul Han sobre coronavirus, la emergencia viral y el Estado policial digital: por qué la revolución será humana", *lavaca*, 2020, fecha de consulta 25 marzo 2020, en https://www.lavaca.org/notas/byung-chul-han-sobre-coronavirus-la-emergencia-viral-y-el-estado-policial-digital-por-que-la-revolucion-sera-humana/.

"Child Safety", *Apple*, fecha de consulta 17 agosto 2021, en https://www.apple.com/child-safety/.

"Ciberseguridad: cómo combate la UE las amenazas cibernéticas", fecha de consulta 16 marzo 2022, en https://www.consilium.europa.eu/es/policies/cybersecurity/.

"Circulares e Instrucciones de la Administración", *El Derecho*, fecha de consulta 4 mayo 2020, en https://elderecho.com/son-impugnables-las-circulares-e-instrucciones-de-la-administracion.

"¿Cómo te localiza la ciberpolicía?", fecha de consulta 2 mayo 2020, en https://www.youtube.com/watch?v=2Mfim7b8Zlw.

"¿Cómo vigila la policía los delitos en internet? Silvia Barrera, de la UIT de @policia, responde", fecha de consulta 2 mayo 2020, en https://www.youtube.com/watch?v=ijjBiSu57SE.

"Consejos de un cazador de hackers para que tu smartphone esté protegido", fecha de consulta 2 mayo 2020, en https://www.youtube.com/watch?v=eVJCOsvFXg0.

COPE, N., "Intelligence led policing or policing led intelligence", *Dialnet*, n.º 2, 2004, fecha de consulta 7 mayo 2022, en https://dialnet.unirioja.es/servlet/articulo?codigo=828455.

"Cortica - Autonomous AI", fecha de consulta 21 julio 2021, en https://www.cortica.com/.

"Court: Public Deserves to Know How NYPD Uses Predictive Policing Software", *Brennan Center for Justice*, fecha de consulta 4 mayo 2020, en https://www.brennancenter.org/our-work/analysis-opinion/court-public-deserves-know-how-nypd-uses-predictive-policing-software.

"Criminal justice access to data in the cloud: challenges", fecha de consulta 9 marzo 2020, en https://rm.coe.int/1680304b59.

"Criminología ambiental: breve historia de su evolución", *Cuadernos de Criminología*, 2017, fecha de consulta 11 noviembre 2021, en https://cuadernosdecriminologia.blogspot.com/2017/09/criminologia-ambiental-breve-historia.html.

"Del 1G al 5G: así funcionan las redes móviles y todo lo qué cambia tras cada salto de generación", *Xataka Móvil*, 2020, fecha de consulta 14 abril 2020, en https://www.xatakamovil.com/conectividad/1g-al-5g-asi-funcionan-redes-moviles-todo-que-cambia-cada-salto-generacion.

"Del derecho y las normas", fecha de consulta 13 abril 2020, en https://www.derechoynormas.com/search/label/Conservacion%20datos.

"Derecho de supresión («al olvido»): buscadores de internet", *AEPD*, fecha de consulta 25 abril 2020, en https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido.

"Dictamen 3/2012 sobre la evolución de las tecnologías biométricas", fecha de consulta 3 mayo 2020, en https://www.aepd.es/sites/default/files/2019-12/wp193_es.pdf.

"E.212 : The international identification plan for public networks and subscriptions",

fecha de consulta 15 abril 2020, en https://www.itu.int/rec/T-REC-E.212.

"EDRM Model", fecha de consulta 6 abril 2020, en https://www.edrm.net/resources/frameworks-and-standards/edrm-model/.

"El anteproyecto de Ley de Enjuiciamiento Criminal: implicaciones orgánicas", fecha de consulta 11 julio 2021, en https://diariolaley.laleynext.es/dll/2021/04/09/el-anteproyecto-de-ley-de-enjuiciamiento-criminal-implicaciones-organicas.

"El Centro Europeo de Ciberdelincuencia (EC3) se inaugura el 11 de enero", *European Commission - European Commission*, fecha de consulta 5 enero 2021, en https://ec.europa.eu/commission/presscorner/detail/es/IP_13_13.

"El «delito grave» en relación a la obligación de conservación de datos, según la L 25/2007", *El Derecho*, fecha de consulta 29 marzo 2020, en https://eldere-cho.com/el-delito-grave-en-relacion-a-la-obligacion-de-conservacion-de-datos-segun-la-l-252007-y-las-reformas-penales-recientes.

"El dilema de las redes (2020) - FilmAffinity", fecha de consulta 29 septiembre 2020, en https://www.filmaffinity.com/es/film640069.html.

"El fiscal investigador: ¿un verdadero riesgo para las garantías?", *Tienda Wolters Kluwer*, fecha de consulta 20 abril 2020, en https://tienda.wolterskluwer.es/p/el-fiscal-investigador-un-verdadero-riesgo-para-las-garantias.

"El Tribunal Supremo anula el informe ilícito de una detective que sirvió para declarar procedente el despido de un trabajador", fecha de consulta 2 junio 2020, en http://www.legaltoday.com/actualidad/noticias/el-tribunal-supremo-anula-el-informe-ilicito-de-una-detective-que-sirvio-para-declarar-procedente-el-despido-de-un-trabajador.

"Electronic discovery", *Wikipedia*, 2020, fecha de consulta 10 abril 2020, en https://en.wikipedia.org/w/index.php?title=Electronic_discovery&oldid=946713667.

"ELISA", fecha de consulta 4 mayo 2020, en https://www.ccn-cert.cni.es/soluciones-seguridad/elisa.html.

"EnCase", *Wikipedia*, 2020, fecha de consulta 10 abril 2020, en https://en.wikipedia.org/w/index.php?title=EnCase&oldid=949275036.

"EU Policy Cycle - EMPACT", *Europol*, fecha de consulta 7 marzo 2020, en https://www.europol.europa.eu/empact.

"EU Terrorism Situation & Trend Report (Te-Sat)", *Europol*, fecha de consulta 6 mayo 2022, en https://www.europol.europa.eu/publications-events/main-reports/tesat-report.

"EUR-Lex - l14005a - ES - EUR-Lex", fecha de consulta 3 mayo 2022, en https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=LEGISSUM%3Al14005a.

"European Counter Terrorism Centre - ECTC", *Europol*, fecha de consulta 4 mayo 2022, en https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc.

"European Cybercrime Centre - EC3", *Europol*, fecha de consulta 4 mayo 2022, en https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

"European Migrant Smuggling Centre - EMSC", *Europol*, fecha de consulta 4 mayo 2022, en https://www.europol.europa.eu/about-europol/european-serious-and-organised-crime-centre-esocc/european-migrant-smuggling-centre-emsc.

"Europol in Brief (Annual Review)", *Europol*, fecha de consulta 6 mayo 2022, en https://www.europol.europa.eu/publications-events/other-reports/europol-in-brief.

"Europol Information System (EIS)", *Europol*, fecha de consulta 6 mayo 2022, en https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-information-system.

"Europol Information System (EIS) Leaflet", *Europol*, fecha de consulta 6 mayo 2022, en https://www.europol.europa.eu/publications-events/publications/europol-information-system-eis-leaflet.

"Europol Platform for Experts (EPE)", *Europol*, fecha de consulta 6 mayo 2022, en https://www.europol.europa.eu/operations-services-and-innovation/services-

support/information-exchange/europol-platform-for-experts.

"Facial Recognition » Avigilon", 2020, fecha de consulta 3 mayo 2020, en https://www.avigilon.com/products/ai-video-analytics/facial-recognition.

"Facial recognition technology: fundamental rights considerations in the context of law enforcement", *European Union Agency for Fundamental Rights*, 2019, fecha de consulta 30 noviembre 2021, en https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law.

"FLIR Skywatch options", fecha de consulta 5 mayo 2020, en https://www.flir.com/globalassets/imported-assets/document/skywatch-options.pdf.

"Full list", *Treaty Office*, fecha de consulta 7 mayo 2022, en https://www.coe.int/en/web/conventions/full-list.

"Full list", *Treaty Office*, fecha de consulta 7 mayo 2022, en https://www.coe.int/en/web/conventions/full-list.

"GDT - Grupo de Delitos Telemáticos", fecha de consulta 1 mayo 2020, en https://www.gdt.guardiacivil.es/webgdt/home_alerta.php.

"Government Monitoring of Social Media: Legal and Policy Challenges", *Brennan Center for Justice*, fecha de consulta 4 mayo 2020, en https://www.brennancenter.org/our-work/research-reports/government-monitoring-social-media-legal-and-policy-challenges.

"GTD Search Results", fecha de consulta 27 marzo 2022, en https://www.start.umd.edu/gtd/search/Results.aspx?page=1&casualties_type=b&casualties_max=&start_yearonly=1970&end_yearonly=1976&dtp2=all&region=8&charttype=line&chart=overtime&ob=GTDID&od=desc&expanded=yes#results-table.

"How do the biggest internet companies make money?", *The Internet Health Report 2019*, 2019, fecha de consulta 11 mayo 2020, en https://internethealthreport.org/2019/how-the-biggest-internet-companies-make-money/.

"How hard is it to «de-anonymize» cellphone data?", *MIT News*, fecha de consulta 19

marzo 2020, en https://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data.

"INE base / Nivel y condiciones de vida (IPC) /Condiciones de vida /Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares / Últimos datos", *INE*, fecha de consulta 24 abril 2020, en https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176741&menu=ultiDatos&idp=1254735976608.

"Informe explicativo de Convenio sobre la Ciberdelincuencia", fecha de consulta 25 abril 2020, en https://rm.coe.int/16802fa403.

"Inicio", *Eurocop | Software de Gestión Policial*, fecha de consulta 21 julio 2021, en https://www.eurocop.com/.

"In-Q-Tel", *Wikipedia*, 2020, fecha de consulta 19 marzo 2020, en https://en.wikipedia.org/w/index.php?title=In-Q-Tel&oldid=946318783.

"Inteligencia Artificial: Un algoritmo puede anticiparse a los actos delictivos", *La Vanguardia*, 2019, fecha de consulta 15 septiembre 2020, en https://www.lavanguardia.com/tecnologia/20190318/461013536935/inteligencia-artifical-vigilancia-predictiva-policia.html.

"Inteligencia artificial y aplicación de la ley: desafíos y oportunidades", fecha de consulta 21 julio 2021, en https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Inteligencia-artificial-y-aplicacion-de-la-ley-desafios-y-oportunidades.

"Interior recurre a la tecnología de inteligencia artificial para mejorar la valoración policial de riesgo en casos de violencia de género", *Noticias Jurídicas*, noticias.juridicas.com, fecha de consulta 21 julio 2021, en https://noticias.juridicas.com/actualidad/noticias/15848-interior-recurre-a-la-tecnologia-de-inteligencia-artificial-para-mejorar-la-valoracion-policial-de-riesgo-en-casos-de-violencia-de-genero/.

"Internet Assigned Numbers Authority", 2017, fecha de consulta 14 abril 2020, en https://web.archive.org/web/20170920185613/http://www.iana.org/.

"Internet Protocol, Version 6 (IPv6) Specification", fecha de consulta 14 abril 2020, en https://tools.ietf.org/html/rfc2460.

"Investigatory Powers Act 2016", *Wikipedia*, 2020, fecha de consulta 10 abril 2020, en https://en.wikipedia.org/w/index.php?title=Investigatory_Powers_Act_2016&oldid=942893147.

"Joint Cybercrime Action Taskforce (J-CAT)", *Europol*, fecha de consulta 4 mayo 2022, en https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce.

JURÍDICAS, N., "Hacia una cooperación judicial en la Unión Europea: el reconocimiento mutuo de resoluciones judiciales en el ámbito penal · Noticias Jurídicas", *Noticias Jurídicas*, noticias.juridicas.com, fecha de consulta 4 junio 2022, en https://noticias.juridicas.com/conocimiento/articulos-doctrinales/11954-hacia-una-cooperacion-judicial-en-la-union-europea:-el-reconocimiento-mutuo-de-resoluciones-judiciales-en-el-ambito-penal/.

"Justicia inicia el proceso para la aprobación de una nueva Ley de Enjuiciamiento Criminal con la creación de la comisión que elaborará el anteproyecto", fecha de consulta 22 abril 2020, en http://www.legaltoday.com/actualidad/noticias/justicia-inicia-el-proceso-para-la-aprobacion-de-una-nueva-ley-de-enjuiciamiento-criminal-con-la-creacion-de-la-comision-que-elaborara-el-anteproyecto.

"K-anonymity", *Wikipedia*, 2020, fecha de consulta 19 marzo 2020, en https://en.wikipedia.org/w/index.php?title=K-anonymity&oldid=944270840.

"La doble cara del reconocimiento facial: entre las ventajas de su uso y el impacto en nuestra privacidad", fecha de consulta 3 mayo 2020, en http://www.legaltoday.com/blogs/nuevas-tecnologias/blog-prodat/la-doble-cara-del-reconocimiento-facial-entre-las-ventajas-de-su-uso-y-el-impacto-en-nuestra-privacidad.

"La policía británica quiere usar IA para predecir delitos antes de que ocurran", *La Vanguardia*, 2018, fecha de consulta 21 julio 2021, en https://www.lavanguardia.com/tecnologia/20181202/453268636098/policia-britanica-uso-inteligencia-artificial-delitos-crimenes-delincuencia.html.

"La solicitud de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación en el marco de la instrucción: reflexión sobre la Ley 25/2007 - El Derecho - Derecho Tic, Penal, Sector Jurídico", *El Derecho*, fecha de consulta 29 marzo 2020, en https://elderecho.com/la-solicitud-de-datos-relativos-a-las-comunicaciones-electronicas-y-a-las-redes-publicas-de-comunicacion-en-el-marco-de-la-instruccion-reflexion-sobre-la-ley-252007.

"LACNIC Inicio", fecha de consulta 14 abril 2020, en https://www.lacnic.net/.

"Law Enforcement | PredPol Law Enforcement Intelligence Led Policing Software | PredPol Law Enforcement Intelligence Led Policing Software", *PredPol*, fecha de consulta 21 julio 2021, en https://www.predpol.com/law-enforcement/.

"Libro blanco sobre la inteligencia artificial", 2020, fecha de consulta 5 mayo 2020, en https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf.

"Linux.com :: «Know Your Enemy»: Everything you need to know about honeypots", 2008, fecha de consulta 4 mayo 2020, en https://web.archive.org/web/20080202010804/http://www.linux.com/articles/39244.

"Microsoft Corp. v. United States", *Wikipedia*, 2020, fecha de consulta 4 abril 2020, en https://en.wikipedia.org/w/index.php?title=Microsoft_Corp._v._United_States&oldid=948795680.

"Müller and Bostrom AI Progress Poll", *AI Impacts*, 2014, fecha de consulta 7 mayo 2020, en https://aiimpacts.org/muller-and-bostrom-ai-progress-poll/.

"New York City Police Department Surveillance Technology", *Brennan Center for Justice*, fecha de consulta 4 mayo 2020, en https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology.

"Not even Singapore has been able to avoid a lockdown", *The Economist*, fecha de consulta 14 abril 2020, en https://www.economist.com/asia/2020/04/11/not-even-singapore-has-been-able-to-avoid-a-lockdown.

"Noticia ENAC - Portal ENAC", fecha de consulta 21 abril 2020, en https://www.enac.es/publicada-nueva-iso17025.

"Nueva arma policial: un «GPS» para buscar pedófilos", *La Razón*, 2011, fecha de consulta 2 mayo 2020, en https://www.larazon.es/historico/6205-nueva-arma-policial-un-gps-para-buscar-pedofilos-ILLA_RAZON_363956/.

"Nulidad de la prueba por la intromisión virtual en domicilio. Una breve reflexión sobre la observación policial ilícita de la intimidad personal y familiar", fecha de consulta 24 abril 2020, en https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAkNDIwsLI7Wy1KLizPw8WyMDQzMDM0MLkEBmWqVLfnJIZUGqbVpiTnEqANGdvcM1AAAAWKE.

"NYPD Detective Guide Skywatch (05-26-16).pdf", fecha de consulta 5 mayo 2020, en https://www.docdroid.net/OliJ4Z6/nypd-detective-guide-05-26-16-pdf.

"Office of the Director of National Intelligence", 2006, fecha de consulta 19 marzo 2020, en https://web.archive.org/web/20060623072458/http://dni.gov/press_releases/20051108_release.htm.

"Página oficial de la DGP-Comisaría General de Policía Judicial", fecha de consulta 1 mayo 2020, en https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html.

"Passcodes are protected by Fifth Amendment, says court", *Naked Security*, 2018, fecha de consulta 13 abril 2020, en https://nakedsecurity.sophos.com/2018/11/01/passcodes-are-protected-by-fifth-amendment-says-court/.

"PhotoDNA Cloud Service | Microsoft", fecha de consulta 5 mayo 2020, en https://www.microsoft.com/en-us/photodna/cloudservice.

"PhotoDNA, el sistema que chiva a las policías y redes sociales de todo el mundo quién comparte pornografía infantil", *La Vanguardia*, 2017, fecha de consulta 2 mayo 2020, en https://www.lavanguardia.com/sucesos/20170307/42577580221/photodna-sistema-pornografia-infantil.html.

"Police Computer Hacking Powers and Civil Liberties", fecha de consulta 24 octubre 2020, en http://www.civilrightsmovement.co.uk/police-computer-hacking-powers-civil-liberties.html.

"Predictive policing", *Liberty*, fecha de consulta 20 agosto 2021, en https://www.libertyhumanrights.org.uk/fundamental/predictive-policing/.

"Predictive Policing Goes to Court", *Brennan Center for Justice*, fecha de consulta 4 mayo 2020, en https://www.brennancenter.org/our-work/analysis-opinion/predictive-policing-goes-court.

"PredPol amplifies racially biased policing", *HRDAG - Human Rights Data Analysis Group*, fecha de consulta 21 julio 2021, en http://hrdag.org/pressroom/predpol-amplifies-racially-biased-policing/.

"Privacy Audit & Assessment of ShotSpotter, Inc.'s GunshotDetection Technology", fecha de consulta 5 mayo 2020, en https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5d40c3693d74b7000160dfbc/1564525424759/Privacy+Audit+and+Assessment+of+Shotspotter+Flex.pdf.

"Privacy Policy - FaceApp", fecha de consulta 5 mayo 2020, en https://www.faceapp.com/privacy-en.html.

"Prosecuted for your password", fecha de consulta 10 abril 2020, en https://www.saunders.co.uk/news/prosecuted-for-your-password.html.

"¿Puede predecirse un crimen antes de suceder con un algoritmo?", *La Vanguardia*, 2019, fecha de consulta 21 julio 2021, en https://www.lavanguardia.com/tecnologia/20190318/461013536935/inteligencia-artifical-vigilancia-predictiva-policia.html.

"¿Qué es INTERPOL?", fecha de consulta 1 mayo 2020, en https://www.interpol.int/es/Quienes-somos/Que-es-INTERPOL.

"Razones para la transición - IPv6", 2016, fecha de consulta 14 abril 2020, en https://web.archive.org/web/20161104001553/http://www.ipv6.es/es-ES/transicion/quees/Paginas/10razones.aspx.

"Richard Serra «Television Delivers People» (1973)", fecha de consulta 10 mayo 2020, en https://www.youtube.com/watch?ab_channel=KunstSpektrum&v=LvZY-waQlJsg.

"RIPE Network Coordination Centre", fecha de consulta 14 abril 2020, en https://www.ripe.net/.

"R/nottheonion - Google tracked his bike ride past a burglarized home. That made him a suspect.", *reddit*, fecha de consulta 10 marzo 2020, en https://www.reddit.com/r/nottheonion/comments/fgbqy1/google_tracked_his_bike_ride_past_a_burglarized/.

"SAIJ - Recomendación de la Conferencia de los Ministros de Justicia de los Países Iberoamericanos (COMJIB) relativa a la tipificación y sanción de la Ciberdelincuencia", fecha de consulta 10 octubre 2020, en http://www.saij.gob.ar/0-internacional-recomendacion-conferencia-ministros-justicia-paises-iberoamericanos-comjib-relativa-tipificacion-sancion-ciberdelincuencia-lnt0006702-2014-05-28/123456789-0abc-defg-g20-76000tcanyel?&o=24&f=Total%7CFecha%7CEstado%20de%20Vigencia/Vigente%2C%20de%20alcance%20general%7CTema%5B5%2C1%5D%7COrganismo%5B5%2C1%5D%7CAutor%5B5%2C1%5D%7CJurisdicci%F3n/Internacional%7CTribunal%5B5%2C1%5D%7CPublicaci%F3n%5B5%2C1%5D%7CColecci%F3n%20tem%E1tica%5B5%2C1%5D%7CTipo%20de%20Documento/Legislaci%F3n/Ley&t=295.

"SANS Institute: Reading Room - Malicious Code", fecha de consulta 5 abril 2020, en https://www.sans.org/reading-room/whitepapers/malicious/paper/953.

"Secure Information Exchange Network Application (SIENA)", *Europol*, fecha de consulta 6 mayo 2022, en https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena.

"Serious and Organised Crime Threat Assessment (SOCTA)", *Europol*, fecha de consulta 6 mayo 2022, en https://www.europol.europa.eu/publications-events/main-reports/socta-report.

"Service members, civilians learn to harness power of «Open Source» information", *www.army.mil*, fecha de consulta 19 marzo 2020, en https://www.army.mil/article/94007/service_members_civilians_learn_to_harness_power_of_open_source_information.

"Sistema HJ - Resolución: SENTENCIA 180/1991", fecha de consulta 14 abril 2020, en http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/1819#complete_resolucion.

"Specification # 23.003", fecha de consulta 15 abril 2020, en https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729.

"Spot the Surveillance: A VR Experience for Keeping an Eye on Big Brother", *Electronic Frontier Foundation*, 2018, fecha de consulta 11 mayo 2020, en https://www.eff.org/pages/descubra-la-vigilancia-una-experiencia-de-realidad-virtual-para-no-perder-de-vista-al-gran.

"Spot the surveillance with virtual reality", *The Internet Health Report 2019*, 2019, fecha de consulta 11 mayo 2020, en https://internethealthreport.org/2019/spot-the-surveillance-with-virtual-reality/.

"Spotlight: The Dangers of Gang Databases and Gang Policing", *The Appeal*, fecha de consulta 4 mayo 2020, en https://theappeal.org/spotlight-the-dangers-of-gang-databases-and-gang-policing/.

"Static camera analytic profiles", 2014, fecha de consulta 4 mayo 2020, en www.ibm.com/support/knowledgecenter/en/ss88xh_2.0.0/iva/ref_analyticp.html.

"Street-Level Surveillance", *Electronic Frontier Foundation*, fecha de consulta 11 mayo 2020, en https://www.eff.org/issues/street-level-surveillance.

"Tecnología, la nueva tentación que acecha a la libertad", *abc*, 2020, fecha de consulta 3 mayo 2020, en https://www.abc.es/cultura/abci-tecnologia-nueva-tentacion-acecha-libertad-202004190256_noticia.html.

"Terrorism Act 2000", Statute Law Database, fecha de consulta 10 abril 2020, en https://www.legislation.gov.uk/ukpga/2000/11/schedule/7.

"Textos aprobados - La inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales - Miércoles 6 de octubre de 2021", fecha de consulta 23 noviembre 2021, en https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_ES.html.

"The Commission on Crime Prevention and Criminal Justice", *Naciones Unidas : Oficina de las Naciones Unidas contra la Droga y el Delito*, fecha de consulta 26 julio 2021, en //www.unodc.org/unodc/es/commissions/CCPCJ/index.html.

"The Data Retention and Acquisition Regulations 2018", Queen's Printer of Acts of Parliament, fecha de consulta 10 abril 2020, en http://www.legislation.gov.uk/uksi/2018/1123/made/data.htm.

"The Economic Impact of Cybercrime and Cyber Espionage", fecha de consulta 7 marzo 2020, en https://www.csis.org/analysis/economic-impact-cybercrime-and-cyber-espionage.

"The EU's horizontal regulatory framework for illegal content removal in the DSM | Hearings | Events | IMCO | 8ª legislatura (2014 - 2019) | Committees | European Parliament", fecha de consulta 5 mayo 2020, en https://www.europarl.europa.eu/committees/en/product-details/20180613CHE04321.

"The Honeynet Project – Honeypot research", fecha de consulta 4 mayo 2020, en //www.honeynet.org/.

"The NSA Continues to Violate Americans' Internet Privacy Rights", *American Civil Liberties Union*, fecha de consulta 2 mayo 2020, en https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy.

"The Public Oversight of Surveillance Technology (POST) Act: A Resource Page", *Brennan Center for Justice*, fecha de consulta 4 mayo 2020, en https://www.brennancenter.org/our-work/research-reports/public-oversight-surveillance-technology-post-act-resource-page.

"The Wildly Unregulated Practice of Undercover Cops Friending People on Facebook", *The Root*, fecha de consulta 4 mayo 2020, en https://www.theroot.com/the-wildly-unregulated-practice-of-undercover-cops-frie-1828731563.

"Tracking down hi-tech crime", 2006, fecha de consulta 4 mayo 2020, en http://news.bbc.co.uk/2/hi/technology/5414502.stm.

"Trapping hackers in the honeypot", 2006, fecha de consulta 4 mayo 2020, en http://news.bbc.co.uk/2/hi/technology/6035455.stm.

"UAS Drone Program | City of Chula Vista", fecha de consulta 21 julio 2021, en https://www.chulavistaca.gov/departments/police-department/programs/uas-drone-program.

"Un espacio de libertad, seguridad y justicia: aspectos generales | Fichas temáticas sobre la Unión Europea | Parlamento Europeo", fecha de consulta 25 marzo 2022, en https://www.europarl.europa.eu/factsheets/es/sheet/150/un-espacio-de-libertad-seguridad-y-justicia-aspectos-generales.

"Una nueva encuesta revela las inquietudes de los ciudadanos de la UE ante la ciberdelincuencia", fecha de consulta 7 marzo 2020, en https://ec.europa.eu/commission/presscorner/detail/es/IP_13_1130.

"US Patent for Vehicle for deploying a mobile surveillance module Patent (Patent # 9,669,690 issued June 6, 2017) - Justia Patents Search", fecha de consulta 5 mayo 2020, en https://patents.justia.com/patent/9669690.

"U.S. top court rules that Microsoft email privacy dispute is moot", *Reuters*, 2018, fecha de consulta 5 abril 2020, en https://www.reuters.com/article/us-usa-court-microsoft-idUSKBN1HO23S.

"U.S. v. Hasbajrami - Brief of Amici Curiae ACLU and EFF in Support of Defendant-Appellant and Reversal", *American Civil Liberties Union*, fecha de consulta 2 mayo 2020, en https://www.aclu.org/legal-document/us-v-hasbajrami-brief-amici-curiae-aclu-and-eff-support-defendant-appellant-and.

"Van den Eynde | Prueba electrónica (II): Desmitificando mitos", fecha de consulta 10

abril 2020, en https://eynde.es/es/prueba-electronica-mitos/.

"Van den Eynde | Prueba Electrónica (III): Cloud, Troyanos, Herramientas forenses, etc.", fecha de consulta 6 abril 2020, en https://eynde.es/es/prueba-electronica-cloud-troyanos/.

"Van den Eynde | Retos relacionados con la prueba electrónica (parte I)", fecha de consulta 6 abril 2020, en https://eynde.es/es/prueba-electronica-1/.

"Where are the Eyes?", fecha de consulta 3 mayo 2020, en https://eyes.daylightingsociety.org/.

OTRAS FUENTES

Acción Común 95/73/JAI, de 10 de marzo de 1995, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea relativo a la Unidad de Drogas de Europol, DOCE núm. L 62 de 20 de marzo de 1995.

Acción común 96/747/JAI de 29 de noviembre de 1996 adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea, relativa a la creación y mantenimiento de un Directorio de competencias, conocimientos y técnicas especializados en materia de lucha contra la delincuencia organizada internacional con el fin de facilitar la cooperación entre los Estados miembros de la Unión Europea para garantizar el cumplimiento de la ley, DOCE núm. L 342 de 31 de diciembre de 1996.

Acción Común de 10 de marzo de 1995, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea relativo a la Unidad de Drogas de Europol (DOCE núm. L 62 de 20 de marzo de 1995.

Acción Común de 16 de diciembre de 1996, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea relativo a la Unidad de Drogas de Europol. DOCE núm. L 342 de 31 de diciembre de 1996.

Acta Única Europea, DOCE núm. L 169, de 29 de junio de 1987.

Acuerdo entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 14 de junio de 1985, DOUE núm. L 239, de 22 de septiembre de 2000.

Acuerdo ministerial para el establecimiento de la Unidad de drogas de Europol, celebrado en Copenhague, el 2 de junio de 1993. DOCE núm. DO L 62 de 20.3.1995.

Boletín Oficial República Argentina - Ministerio De Seguridad - Resolución 144/2020, , en https://www.boletinoficial.gob.ar/detalleAviso/primera/230060.

Budapest Convention, *Cybercrime*, en https://www.coe.int/en/web/cybercrime/the-

budapest-convention.

Circular 1/2013, de 11 de enero, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas, en https://www.boe.es/buscar/doc.php?coleccion=fiscalia&id=FIS-C-2013-00001&tn=2.

Circular 1/2013, de 11 de enero, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas, en https://www.boe.es/buscar/doc.php?coleccion=fiscalia&id=FIS–C–2013–00001&tn=2.

Circular 1/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal, en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4240.

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

Circular 3/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4242.

Circular 4/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4243.

Circular 5/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre registro de dispositivos y equipos informáticos, en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4244.

Convenio basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía (Convenio Europol), hecho en Bruselas el 26 de julio de 1995, DOCE núm. C 316, de 27 de noviembre de 1995.

Convenio relativo a la determinación del Estado responsable del examen de las solicitudes de asilo presentadas en los Estados miembros de las Comunidades Europeas

(97/C 254/01), DOCE núm. L 254 de 19 de agosto de 1997.

Decisión 2005/511/JAI del consejo de 12 de julio de 2005 relativa a la protección del euro contra la falsificación mediante la designación de Europol como organismo central para la lucha contra la falsificación del euro, DOCE núm. L 185, de 16 de julio de 2005.

Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, DOCE núm. L 210 de 6 de agosto de 2008.

Decisión 2008/616/JAI del Consejo, de 23 de junio de 2008, relativa a la ejecución de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, DOCE núm. L 210 de 6 de agosto de 2008.

Decisión 2009/371/JAI del Consejo, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol) DOUE núm. L 121 de 15 de mayo de 2009.

Decisión del Consejo, de 25 de febrero de 2010, por la que se crea el Comité permanente de cooperación operativa en materia de seguridad interior, DOUE núm. L 52 de 3 de marzo de 2010.

Decisión del consejo, de 3 de diciembre de 1998, por la que se encomienda a Europol la lucha contra los delitos cometidos o que puedan cometerse en el marco de actividades terroristas que atenten contra la vida, la integridad física, la libertad o los bienes de las personas, DOCE núm. C 26 de 4 de junio de 1999.

Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo, DOCE núm. L 330 de 9 de diciembre de 2008, pp. 21/23. Decisión marco del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo, DOCE núm. L 164 de 22 de junio de 2022.

Decisión marco 2009/905/JAI del Consejo, de 30 de noviembre de 2009, sobre acreditación de prestadores de servicios forenses que llevan a cabo actividades de

laboratorio, DOCE núm. L 322 de 9 de diciembre de 2009.

Decisión Marco del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros, DOCE núm. L 190 de 18 de julio de 2002, disponible en que establecía un nuevo sistema para emitir y gestionar una orden de detención europea.

Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se crea la agencia de la Unión Europea para la formación y la cooperación de los servicios con funciones coercitivas (Europol) y se derogan las Decisiones 2009/371/JAI y 2005/681/JAI, DOUE núm. C 38 de 8 de febrero de 2014.

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 infrac-ciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, DOUE núm. L 119, 4.5.2016.

Documento FIS-C-2013-00001, en https://www.boe.es/buscar/doc.php?coleccion=fiscalia&id=FIS-C-2013-00001&tn=2.

El Tratado de Ámsterdam por el que se modifica el Tratado de la Unión Europea, DOCE núm. C 340 de 10 de noviembre de 1997.

European Convention on Mutual Assistance in Criminal Matters (ETS No. 030), disponible en https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=030. Ratificado por España mediante Instrumento de Ratificación de 14 de julio de 1982 del Convenio Europeo de Asistencia Judicial en Materia Penal, hecho en Estrasburgo el 20 de abril de 1959, BOE núm. 223, de 17 de septiembre de 1982.

Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221.

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, en https://www.boe.es/buscar/act.php?id=BOE-A-2021-8806&p=20210527&tn=1#a1.

Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional", en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-6347.

Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional, en https://www.boe.es/diario_boe/txt.php?id=BOE–A–2019–6347.

Reglamento (CE) nº 343/2003 del Consejo, de 18 de febrero de 2003, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de asilo presentada en uno de los Estados miembros por un nacional de un tercer país, Documento l33153, DOUE núm. L 50 de 25 de febrero de 2003.

Reglamento (UE) 2015/2219 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre la Agencia de la Unión Europea para la formación policial (CEPOL) y por el que se sustituye y deroga la Decisión 2005/681/JAI del Consejo, DOUE núm. L 319 de 4.12.2015.

Reglamento (UE) n ° 603/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013 , relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) n ° 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, y por el que se modifica el Reglamento (UE) n ° 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia, DOUE núm. L 180 de 29.6.2013.

Reglamento (UE) n ° 604/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, DOUE núm. L 180, de 29 de septiembre de 2013.

The Hague Programme: strengthening freedom, security and justice in the European Union, 2005, en https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52005XG0303%2801%29.

Tratado de la Unión Europea, DOUE núm. C 191 de 29 de julio de 1992.

Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea, firmado en Lisboa el 13 de diciembre de 2007, DOUE núm. C 306, de 17 de diciembre de 2007.

Tratado de Niza por el que se modifican el Tratado de la Unión Europea, los Tratados Constitutivos de las Comunidades Europeas y determinados actos conexos, DOCE núm. C 80 de 10.3.2001.

Versión consolidada del Tratado de Funcionamiento de la Unión Europea, DOUE núm. C 326 de 26 de octubre de 2012.