Revista de las Cortes Generales. ISSN: 0213-0130. ISSNe: 2659-9678
N.º 121, Primer semestre (2026): pp. 137-166
https://doi.org/10.33426/rcg/2026/121/1918

LAS DILIGENCIAS DE INVESTIGACIÓN PENAL A TRAVÉS DEL SMARTPHONE: ¿EL CREPÚSCULO DE LA PRIVACIDAD?

CRIMINAL INVESTIGATION PROCEDURES VIA SMARTPHONE: THE TWILIGHT OF PRIVACY?

Antón Fructuoso Freire Montero
Fiscalía Provincial de A Coruña
(Sección de Criminalidad Informática)
Doctor en Derecho
https://orcid.org/0000-0003-3056-1450

Fecha de recepción del artículo: marzo 2026
Fecha de aceptación y versión final: junio 2026

RESUMEN

En el contexto actual, el teléfono inteligente se ha convertido en un instrumento imprescindible en la vida diaria de los ciudadanos: no sólo desempeña un papel crucial para mantener nuestras comunicaciones telemáticas, sino que frecuentemente funciona también como un instrumento de trabajo y constituye un soporte en el que conservamos buena parte de nuestra vida privada. Consciente de esta realidad, hace ya más de una década que el legislador introdujo en la LECrim, a través de la LO 13/2015, varias medidas de investigación que permiten seguir el rastro que genera el empleo del smartphone para lograr la averiguación de delitos. Con el presente trabajo nos proponemos analizar las notas básicas de cada una de estas técnicas, valorando la calidad de las normas que las regulan y calibrando el impacto que su utilización por las autoridades produce en los derechos fundamentales de la persona usuaria del dispositivo, en especial en su privacidad. En realidad, no es descabellado plantearse una cuestión un tanto inquietante: ¿existe aún este bien jurídico, tal y como fue concebido en sus orígenes, en el mundo digital?

Palabras clave: investigación tecnológica, smartphone, privacidad, entorno virtual, calidad de la ley.

ABSTRACT

In the current context, smartphones have become an essential tool in people's daily lives: not only do they play a crucial role in maintaining our telematic communications, but they also frequently serve as a work tool and a medium on which we store a large part of our private lives. Aware of this reality, more than a decade ago, the legislator introduced several investigative measures into the Criminal Procedure Act (LECrim) through Organic Law 13/2015, which allow the trail generated by smartphone use to be tracked in order to investigate crimes. In this paper, we aim to analyse the basic features of each of these techniques, assessing the quality of the regulations governing them and gauging the impact that their use by the authorities has on the fundamental rights of the device user, particularly their privacy. In fact, it is not unreasonable to ask a somewhat disturbing question: does this legal right, as it was originally conceived, still exist in the digital world?

Keywords: technological research, smartphone, privacy, virtual environment, quality of law.

I. Introducción

1. La delincuencia en la sociedad digital

En la escena inicial de la película *2001: Una odisea en el espacio*[1] un grupo de homínidos se encuentran con un monolito, un misterioso objeto negro y rectangular que parece marcar un antes y un después en el curso de su existencia. Curiosamente, también hoy la humanidad tiene ante sí un objeto de similares características que está cambiando nuestras vidas y que constituye un elemento esencial en la dinámica de la sociedad digital. Conviene comenzar este estudio destacando que la «sociedad digital»[2] o «sociedad de la información»[3] es una estructura social que se caracteriza por la capacidad que los ciudadanos poseemos para generar, comunicar, almacenar y procesar una enorme cantidad de información. En particular, es muy notable la incidencia que en este contexto poseen las redes sociales, medios que constituyen un verdadero altavoz para sus miembros, concediéndoles un *púlpito* desde el que difundir sus pensamientos e ideas en el «ágora digital» (Pérez-Latre, 2015, p. 108). Esto implica evidentes efectos benévolos, al otorgar a sus usuarios el estatus de «sujetos colaborativos» (STC 27/2020, de 24 de febrero, FJ 3); no obstante, también provoca problemas alarmantes, como sucede con el imparable aumento de la información falsa –*fake news*–, una realidad que se ve intensificada con el uso de tales aplicaciones. Además, en no pocas ocasiones el uso de redes sociales genera una relación de *dependencia* hacia estos medios, sobre todo en los usuarios más jóvenes (Armenta Deu, 2018, p. 68); de hecho, se ha anunciado recientemente una iniciativa tendente a impedir la participación de personas menores de 16 años en este ámbito[4].

---

[1] En el idioma original, *2001: A Space Odyssey* (Stanley Kubrick, 1968).

[2] La expresión fue empleada originariamente hace tres décadas por Clarke (1994, p. 77).

[3] El término «sociedad de la información» es empleado por Castells (1999, p. 49). El autor, sin embargo, prefiere el término «sociedad informacional» antes que «sociedad de la información», de la misma forma que entiende preferible el uso del término «sociedad industrial» a «sociedad de la industria».

[4] Así lo ha anunciado el presidente del Gobierno en una cumbre celebrada en Dubái el día 3/2/2026. Para conocer con mayor detalle la iniciativa puede consultarse la nota publi-

Por otro lado, debe destacarse el hecho de que la gran mayoría de los integrantes de la sociedad digital vivimos actualmente acompañados por un dispositivo que nos conecta de forma permanente a Internet, y que además está provisto de mecanismos que permiten la captación de imagen y sonido. Ese objeto negro y rectangular al que nos referíamos antes es, lógicamente, el smartphone, un instrumento que se ha ido deslizando de forma silenciosa en nuestra vida diaria, seduciéndonos para ello con el poderoso señuelo de innumerables servicios –aparentemente– gratuitos (Bellver y Montalvo, 2021, p. 3). El uso de esta clase de dispositivos es ya no sólo masivo[5], sino también intensivo: más allá de lo que podría considerarse como un natural aumento del intercambio de información propio de las actuales posibilidades comunicativas, puede entenderse que los actuales parámetros de la telecomunicación humana están superando todas las expectativas. Así, en realidad, en la actualidad seguramente no estemos ante una comunicación potenciada por las TIC, sino ante claros supuestos de *hipercomunicación*.

Entre las dificultades inherentes al proceso de digitalización de la sociedad se encuentran también las referentes al mundo criminal. Con carácter general, puede decirse que las posibilidades operativas de los delincuentes se multiplican en el entorno digital debido a las notas propias de este contexto –anonimato, alcance global, volatilidad de las evidencias delictivas…–. En esta dirección, ya en el año 2021 la FGE[6] informaba sobre un progresivo aumento en el número de investigaciones penales vinculadas a la utilización de las nuevas tecnologías y, más específicamente, de Internet. Así mismo, la jurisprudencia constata la migración de un gran número de delitos del mundo físico al ámbito digital, siendo esta una realidad especialmente

---

cada en https://www.lamoncloa.gob.es/presidente/actividades/paginas/2026/030226-sanchez-cumbre-gobiernos-dubai.aspx.

[5] Por poner un ejemplo, los últimos análisis estadísticos reflejan que un 96,3% de las personas de 16 a 74 años utilizó Internet en los tres últimos meses (0,5 puntos más que en 2024) y que el 92,5% lo usó diariamente (1,0 puntos más que en 2024). *Vid.* al respecto la Encuesta del Instituto Nacional de Estadística del año 2025, sobre Equipamiento y Uso de Tecnologías de la Información y Comunicación (TIC) en los Hogares, publicada el 20/11/2025.

[6] Puede consultarse, en relación con esta problemática, la Instrucción 2/2011, de 11 de octubre, sobre el/la Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las fiscalías (actualización de 2021), punto II.1.

preocupante en relación con determinadas tipologías criminales, en las que el empleo de las redes sociales incrementa el alcance de la actuación del delincuente, como sucede, *v.gr.*, con las estafas informáticas –art. 248.1 letra a) CP– o con el acoso telemático –art. 172 ter.1. 2º CP–. En este contexto, el TS ha declarado que bajo la expresión «lugar de comisión del delito» deben entenderse comprendidos en la actualidad no sólo los lugares físicos, sino también los espacios digitales o virtuales, en los que las personas pueden también subir o volcar contenidos ilícitos[7].

Por otra parte, la colaboración que se fragua en las redes sociales, a la que antes nos referíamos, implica también un aumento de los sistemas destinados a la compartición de servicios delictivos, fenómeno comúnmente designado por su expresión anglosajona –«*crime as a service»* (CaaS)–. Como indican los fiscales especialistas en la materia, este modelo genera un nuevo «ecosistema en la red»[8] caracterizado por la coexistencia de un relevante número de grupos u organizaciones criminales especializados en ofertar a ciertos usuarios de Internet una serie de productos específicamente diseñados para la comisión de ciberdelitos. Nos hallamos, dicho llanamente, ante verdaderos supermercados o centros comerciales de servicios delictivos, espacios a los que los sujetos que carecen de específicos conocimientos informáticos pueden acudir para adquirir las herramientas con las que posteriormente recorrer el *iter criminis* deseado.

2. La investigación tecnológica y su impacto en la privacidad

La inquietante situación antes descrita requiere una transformación del ordenamiento jurídico, con el objeto de conseguir que la «senda del Derecho» (Holmes, 1897, p. 1) se adapte al mundo digital. De esta forma, la reacción de los estados frente a esta realidad no sólo consiste en situar las nuevas conductas ilícitas en el Código Penal,

---

[7] Véase la STS 547/2022, de 2 de junio, de la Sala Segunda, FJ 3, en la que se avala la imposición de la prohibición del uso de una red social como una pena accesoria de privación del derecho a acudir a determinados lugares en que se haya cometido el delito, *ex* artículo 48.1 CP.

[8] *Vid.* las conclusiones de las 13ª Jornadas de Especialistas en Criminalidad Informática, celebradas en León del 20 al 22 de noviembre de 2024, punto 8º.

norma que constituye una «Constitución en negativo» (Rodríguez Mourullo, 2003, p. 311), sino que exige también adecuar la investigación penal a las características de la sociedad digital. En particular, resulta esencial contar con normas completas y precisas que regulen los modernos medios de investigación tecnológica.

En nuestro país, el legislador ha realizado notables esfuerzos para acomodar las normas procesales penales a las nuevas formas de investigación. Así sucedió hace ya más de una década con 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, con la que se introdujeron en la ley procesal penal la mayor parte de los medios de investigación tecnológica, sometiendo su uso en todo caso a la observancia del principio de proporcionalidad –artículo 588 bis a) LECrim–. Posteriormente se promulgaron otras normas que poseen una gran incidencia en la investigación tecnológica, como 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, o, más recientemente, el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial.

En este contexto, es conveniente destacar el papel que puede desempeñar el smartphone del sospechoso, habida cuenta de la multifuncionalidad (Varona Jiménez, 2020, p. 242) de tales aparatos, así como la masividad y la intensidad con la que los ciudadanos de a pie utilizamos estos dispositivos. El objeto de este trabajo es, en primer lugar, analizar todas las posibilidades que el Estado posee para investigar a una persona a través de este dispositivo y valorar la calidad de las normas que regulan el uso de estas técnicas. Además, el presente estudio pretende reflexionar sobre la incidencia que tales medios de investigación producen en la privacidad de los individuos. Creemos que esta pretensión no responde a una simple curiosidad académica, sino que constituye una cuestión vital en un régimen democrático. En este sentido, Pérez Luño (2003, p. 317) refiere que el respeto a los derechos de la privacidad es una de las exigencias más acuciantes en las sociedades tecnológicamente avanzadas, provocando esto que

las legislaciones más sensibles a las defensas de las libertades hayan intentado ofrecer una respuesta jurídica eficaz a esta problemática. Es más, la inquietud por el respecto a la privacidad en este contexto parece haber trascendido del ámbito estrictamente jurídico, instalándose en el imaginario colectivo. Así, se ha escrito (Truong, 2020) que «si el siglo XIX ha sido balzaquiano y el XX kafkiano, el siglo XXI va a devenir orwelliano»[9].

II. Las medidas de investigación sobre las comunicaciones telemáticas

1. La intervención de comunicaciones telemáticas

Regulada en los artículos 588 ter a) a 588 ter i) de la LECrim, la intervención de las comunicaciones telemáticas es la única medida de investigación tecnológica que no fue introducida por la LO 13/2015: ya con anterioridad a esta reforma existía en la ley procesal penal una previsión específica sobre la intervención de comunicaciones telefónicas –el antiguo art. 579 de la LECrim–, si bien esta norma no superaba los estándares de calidad de la ley marcados por el Tribunal de Estrasburgo[10].

En esencia, la intervención telemática puede ser definida como aquella diligencia de investigación penal que permite a las autoridades conocer el contenido de las comunicaciones a distancia mantenidas por la persona investigada, así como la captación de los datos de tráfico relativos a estas comunicaciones. Esta medida se caracteriza por practicarse en tiempo real y por no provocar la interrupción de la conversación afectada, pudiendo comprender tanto las comunicaciones telefónicas –fijas y móviles– como el correo electrónico o cualquier otro tipo de comunicaciones a través de internet, *v. gr.,* las producidas en foros o chats cerrados (Cabezudo Rodríguez, 2016, p. 29). Naturalmente, entran dentro de este contexto las comunicaciones mantenidas por el sospechoso mediante su smartphone. Es

---

[9] El autor hace referencia a la novela *1984* de George Orwell, una distopía en la que un Estado autoritario monitoriza casi por completo la vida privada de sus ciudadanos.

[10] Véanse a este respecto las condenas al Estado español contenidas en la STEDH *Valenzuela Contreras vs España,* de 30 de julio de 1998, así como en la STEDH *Prado Bugallo vs España,* de 18 de febrero de 2003.

conveniente destacar además que el ámbito objetivo de aplicación de esta medida se ha diversificado en los últimos tiempos debido al uso de los teléfonos inteligentes: a diferencia de lo que sucedía con las clásicas «escuchas», en las que los investigadores procedían únicamente a captar y analizar las conversaciones orales que el investigado mantenía a través del teléfono «pinchado», a día de hoy la diligencia de intervención de las telecomunicaciones puede abarcar un contenido mucho más amplio, incluyendo las referidas conversaciones orales a distancia, pero englobando también otra clase de elementos, tales como mensajes escritos, audios, imágenes y demás contenido multimedia.

El secreto comunicativo –art. 18.3 CE– es el bien jurídico que principalmente resulta lesionado al poner en práctica esta actividad de indagación estatal. Naturalmente, el derecho al secreto de las comunicaciones –como todos los demás derechos– no es absoluto y puede ser limitado *secundum constitutionem* por las autoridades, si bien esto ha de efectuarse siempre teniendo presente, como indica la jurisprudencia de la Sala Segunda del TS, que es «su restricción es de gran trascendencia en una sociedad libre» (STS 699/2021, de 16 de septiembre de 2021, FJ 2). En este sentido, Jiménez Campo (1987, p. 36) destaca la importancia de que se produzca un adecuado respeto de este bien jurídico por parte de los poderes públicos democráticos, en la medida en que este derecho se relaciona con los llamados «*ius activae civitatis*», actúa en favor de la autodeterminación privada y permite la constitución de un ámbito de autonomía del individuo –y de la sociedad en general– frente al Estado. En efecto, el propio TC ha declarado reiteradamente que este derecho es especialmente valioso por estar conectado con otros bienes jurídicos que son protegidos por la CE, tales como el secreto del sufragio activo, la libertad ideológica, la libertad de empresa, la confidencialidad de la asistencia letrada o el derecho a la intimidad (*ex multis*, STC 123/2002, de 20 de mayo, FJ 5).

Además, el desarrollo de la intervención telemática determinará frecuentemente una injerencia en la intimidad de la persona investigada –art. 18.1 CE–, puesto que habilita a las autoridades penales a tomar conocimiento del contenido de las comunicaciones telemáticas que mantenga durante un período de tiempo más o menos

prolongado; esto permite a los investigadores tener acceso a una notable cantidad de información que sin duda puede enmarcarse en ese «ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario –según las pautas de nuestra cultura– para mantener una calidad mínima de la vida humana» (STC 231/1988, de 2 de diciembre, FJ 2). Debe destacarse que las pautas comunicativas propias de la sociedad digital provocan que la lesión de la intimidad generada con la práctica de esta medida sea de mayor entidad a la que podría causarse hace no mucho tiempo. Pensemos en la frecuencia con la que utilizamos los medios de comunicación telemática actualmente –señaladamente, el smartphone– y comparémosla, por ejemplo, con lo que sucedía hace tan sólo dos décadas: la cantidad de información personal que recibimos y trasladamos en este contexto es muy superior. En este punto conviene destacar que la puesta en práctica de una intervención telemática puede dar lugar a la captación de un considerable número de conversaciones que, si bien se mantienen a través del dispositivo intervenido, resultan completamente ajenas al hecho criminal, fenómeno que la jurisprudencia ha designado tradicionalmente como «recogida de arrastre» (STS 419/2013, de 14 de mayo, de la Sala Segunda, FJ 1).

Finalmente, una referencia completa a las intervenciones telemáticas no puede hacerse sin mencionar que la medida está aquejada hoy en día de notables dificultades en la práctica, cuestión a la que aludíamos ya en estudios previos (Autor, 2024, pp. 158 y 159). Por un lado, la dimensión global de las comunicaciones causa una enorme lentitud en el desarrollo de la diligencia, debiendo acudirse frecuentemente a mecanismos de cooperación judicial internacional si la plataforma de comunicación empleada por el sospechoso tiene sus servidores radicados en el extranjero[11]. Por otro, la utilidad de la medida mengua en la actualidad ante la posibilidad de que las comunicaciones a distancia sean encriptadas. Debe valorarse en este punto que los canales de comunicación ordinarios o de uso masivo –*v. gr.,* las aplicaciones Telegram o WhatsApp– están dotados de mecanismos que dificultan la intromisión de terceros, como es el caso

[11] Como apunta Rodríguez-Yzquierdo Serrano (2021, p. 135), el problema se agudiza si tenemos en cuenta que la mayor parte de las jurisdicciones de los Estados siguen inmersas en una «poco permeable dimensión territorial».

del cifrado de extremo a extremo de los mensajes; además, existen ciertas plataformas de comunicación específicamente creadas para blindar las comunicaciones y preservar el anonimato de sus usuarios, tales como las redes EncroChat[12] o Sky-ECC. Como veremos más adelante, la existencia de tales dificultades puede provocar que el órgano instructor descarte el empleo de la intervención telemática, en favor de otra técnica de investigación más vanguardista: el registro remoto de equipos informáticos.

2. El análisis de datos derivados de las comunicaciones telemáticas

Como indicábamos en el apartado introductorio de este trabajo, una de las señas de identidad de la sociedad digital es la consagración de los medios de comunicación que se basan en las TIC, sustentados esencialmente en el empleo de Internet. Así, el uso de estas tecnologías está actualmente presente en casi cualquier actividad humana, lo que provoca que las personas nos hallemos continuamente generando o intercambiando información –es decir, datos– a través de la red. Nuevamente, la relación del smartphone con esta dinámica es evidente. En este punto debe subrayarse el papel crucial que juegan las operadoras y empresas del sector de las telecomunicaciones, pues tales entidades privadas conservan de forma sistemática los datos que se derivan de nuestras comunicaciones a distancia, haciéndolo no sólo por motivos de seguridad o técnicos, sino de muy diversa índole (Fernández Rodríguez, 2016, p. 102). Entre otras muchas aplicaciones, tal información podrá ser de gran utilidad para lograr el esclarecimiento de hechos delictivos (Ortiz Pradillo, 2020, p. 4).

En realidad, determinar el grado de influencia que supone la gestión los datos es una cuestión que excede el propósito de este estudio: la capacidad para registrar, analizar y utilizar tales datos adquiere actualmente una relevancia de tal magnitud que puede decirse que la nuestra es una sociedad sometida al imperio o al «poder»

[12] Sobre las medidas de investigación que pueden practicarse para acceder a esta clase de redes, es de mucho interés consultar la sentencia del TJUE (C-670/22) del 30 de abril de 2024, resolución que validó el uso de pruebas de EncroChat obtenidas por Francia, considerándolas compatibles con el Derecho de la Unión Europea siempre que se respetasen determinados criterios de proporcionalidad.

(Casas Baamonde, 2020, p. 11) de los datos, constituyendo estos lo que algunos autores consideran una verdadera «religión» (Harari, 2017, p. 400). Sea como fuere, lo que parece incuestionable es que los datos conforman ya una materia prima esencial del mercado: se ha afirmado elocuentemente en este sentido que los datos constituyen el «oro moderno» (Andrejevic, 2007, p. 81), siendo una mercancía con un valor equiparable al que pudieron tener el oro o el petróleo en anteriores revoluciones económicas. Por otra parte, son varias las voces doctrinales que advierten sobre los peligros de esta dinámica, al generarse un modelo político, económico y social designado por Zuboff (2019) como el «capitalismo de la vigilancia». En particular, resulta inquietante para algunos autores constatar las inmensas facultades de control que las grandes multinacionales tecnológicas ostentan sobre los ciudadanos, surgiendo así un «binomio» (Lasalle, 2021) conformado por unas multitudes digitales, de un lado, y, de otro, un tecnopoder que «depreda» (Bellver y Montalvo, 2021, p. 3) nuestros datos.

En nuestro ordenamiento jurídico las técnicas de investigación penal relativas al análisis de los datos derivados de las comunicaciones a distancia vienen reguladas en los arts. 588 ter j) a 588 ter m) de la LECrim, debiendo consultarse así mismo las previsiones contenidas en la Ley 25/2007, sobre retención de datos de tráfico, y en la normativa de protección de datos personales vigente[13]. Con estos mimbres, el legislador construye un sistema que opera sobre la base del principio de disponibilidad de los datos y que discrimina las garantías necesarias para esa disposición en función de su naturaleza. En concreto, si se trata de datos vinculados a un concreto proceso de comunicación –es decir, de naturaleza dinámica–, su incorporación a la causa exigirá la intercesión judicial, como sucede con los datos obrantes en archivos automatizados de los prestadores de servicios –art. 588 ter j) LECrim– o con los datos asociados a una IP –art. 588 ter k) LECrim–. En caso contrario, es decir, para recabar datos

[13] En este ámbito ha de respetarse con carácter general la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y, con carácter específico, 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.

de naturaleza estática, también llamados «datos de abonado», la autorización del órgano instructor no será necesaria, pudiendo actuar de forma autónoma los agentes de la autoridad: este sería el proceder en la identificación de terminales mediante captación de códigos de identificación, tales como el IMEI o el IMSI, o en la identificación de titulares o terminales o dispositivos de conectividad –art. 588 ter letras l) y m) de la ley procesal penal–. Téngase en cuenta que en ningún caso estas diligencias permitirán a los investigadores conocer el contenido de las comunicaciones, siendo necesario para ello acudir a la medida de intervención telemática más arriba referida.

Por lo que se refiere al impacto iusfundamental de estas técnicas, parece claro que su utilización genera una clara injerencia en el derecho a la protección de datos de carácter personal –art. 18.4 CE–, así como una afectación tangencial del derecho al secreto comunicativo, en la medida en que algunos datos de tráfico se integran dentro del contenido protegido por el artículo 18.3 CE[14]. Además, y pese a lo que *prima facie* pueda parecer, estas diligencias también pueden lesionar la intimidad de la persona investigada –art. 18.1 CE–, especialmente en los casos de investigaciones que son prolongadas o sostenidas en el tiempo, cuando la recopilación de datos de tráfico se realiza con carácter sistemático y permite elaborar un *perfil* del individuo, tal y como han declarado de forma expresa tanto el Tribunal de Estrasburgo (STEDH Podchasov vs Rusia, de 13/2/2024, punto 52) como el Tribunal de Luxemburgo (STJUE Digital Rights Ireland y Seitlinger and others vs Irish Data Protection Commissioner, de 8/4/2014, punto 27). Téngase en cuenta, además, que el Reglamento UE 1689/2024, sobre Inteligencia Artificial, califica como «de alto riesgo» aquellos sistemas de IA tendentes a la elaboración de perfiles de personas físicas –artículo 6.3 del RIA–.

En esta línea, la potencialidad lesiva que subyace en el empleo de esta clase de medidas se comprende mejor si se contempla desde la óptica de la teoría del «*mosaico de la privacidad*». Esta tesis propugna que las injerencias estatales en la privacidad de los ciudadanos

[14] Reparemos en que, por ejemplo, algunas de las medidas cuyo estudio nos ocupa permitirán conocer o inferir la identidad de los interlocutores en una comunicación telemática, siendo este uno de los aspectos incluidos en el ámbito protector del secreto comunicativo (STC 230/2007, de 5 de noviembre, FJ 2).

pueden venir constituidas, bien por un acto aislado del Estado (a), o bien por una secuencia de actos, cada uno de los cuales ostenta una menor intensidad lesiva individualmente considerados, pero que se engloban en una investigación más compleja y prolongada en el tiempo (b). En este último caso, podría entenderse que cada uno de los actos individuales de investigación se relacionan entre sí como las teselas de un mosaico: para valorar la afectación de la privacidad del individuo habrá de observarse el resultado conjunto de todos los actos o datos recabados, es decir, habrá de contemplarse el mosaico en su integridad (Bellovin *et al*., 2014, p. 570).

III. La captación y grabación de comunicaciones orales directas

En primer lugar, hemos de señalar que, si bien la vía ordinaria para la práctica de esta diligencia es la instalación de micrófonos ambientales específicamente diseñados para tal fin, también en este caso existe una conexión con el smartphone. En efecto, la posibilidad de emplear el teléfono móvil de la persona investigada como dispositivo de captación de sus conversaciones orales directas es una técnica expresamente admitida por la jurisprudencia de la Sala Segunda (STS 373/2016, de 3 de mayo, FJ 1.6) que puede resultar extraordinariamente útil, teniendo en cuenta la *hipercomunicación* a la que nos referíamos en la introducción de este trabajo: en este sentido, el hecho de que la gran mayoría de ciudadanos portemos con nosotros un teléfono con conexión a Internet supone que vayamos acompañados constantemente de micrófonos en potencia. No obstante, la articulación técnica de la escucha –es decir, la activación remota y subrepticia del smartphone para iniciar y finalizar la grabación del sonido ambiente– exigirá con toda seguridad tener que inocular un virus en el dispositivo para tomar el control de este, lo que implicará que sea necesario aplicar para ello –también– el registro remoto de equipos informáticos, medida a la que más adelante nos referiremos.

Regulada en los artículos 588 quater letras a) a d) de la LECrim, la captación de comunicaciones orales directas es una diligencia íntimamente vinculada a la investigación de delitos de cierta complejidad, en particular a los delitos perpetrados por organizaciones

y grupos criminales, tal y como expresamente afirma la FGE[15]. Así, las escuchas ambientales constituyen un instrumento indispensable para combatir eficazmente la actividad de redes criminales que actúan desde hace años en nuestro país, a diferencia de lo que sucede en ocasiones con otras medidas de investigación más clásicas[16] que han quedado «obsoletas» (Casanova Martí, 2016). Tales organizaciones, dedicadas tanto a la comisión de delitos contra el patrimonio como a perpetrar delitos contra bienes personales –piénsese en las bandas dedicadas al tráfico de estupefacientes o a la elaboración y difusión de pornografía infantil–, suelen contar además con un gran número de integrantes y sofisticados medios técnicos para evadir el control de las autoridades.

En relación con la afectación de derechos que provoca esta diligencia, resulta evidente que con su práctica se lesiona gravemente el derecho a la intimidad –art. 18.1 CE– del investigado; de hecho, el elevado impacto que las escuchas ambientales pueden provocar en la privacidad de los ciudadanos es una reflexión que supera desde hace tiempo el ámbito estrictamente jurídico y que se refleja en conocidas obras cinematográficas[17]. En nuestra opinión, en el caso de captación de comunicaciones orales directas se produce una injerencia más intensa que en las intervenciones telemáticas, pues también la expectativa de privacidad en esta clase de conversaciones es notablemente superior: la sospecha de posibles injerencias externas en las conversaciones mantenidas a través de medios telemáticos es razonable, a diferencia de lo que sucede –en condiciones norma-

[15] En esta línea la Circular FGE 3/2019, dispone en su punto 1: «la técnica de investigación consistente en grabar a través de micrófonos ambientales ha sido empleada en ocasiones en los últimos años, sobre todo, en el caso de investigaciones especialmente complejas».

[16] Así, *v. gr.*, Nieva Fenoll (2016) se muestra escéptico sobre la efectividad de las intervenciones telefónicas en relación con los delitos más complejos: «La experiencia ha demostrado que esa agresión contra la privacidad sirve de muy poco a efectos investigadores. Actualmente existen canales seguros de comunicación que prestan perfecto y fácil servicio a cualquier usuario. En consecuencia, las intervenciones de comunicaciones ya sólo podrían ser útiles para perseguir a delincuentes comunes bastante descuidados en sus comunicaciones, lo que no sólo es desproporcionado, sino completamente absurdo».

[17] Así sucede, por ejemplo, en los filmes *The conversation* (Francis Ford Coppola, 1974) o *Das Leben der Anderen* –en español: *La vida de los otros*– (Florian Henckel von Donnersmarck, 2006).

les– en las conversaciones entre presentes. Así mismo, las escuchas ambientales pueden afectar al derecho al secreto comunicativo, habiendo declarado el TC que el derecho consagrado en el art. 18.3 de la CE ofrece cobertura también a las comunicaciones interpersonales mantenidas sin la intervención de medios o artificios técnicos (*vid*. STC 99/2021, de 10 de mayo, FJ 7).

Un comentario específico merece el supuesto en el que las escuchas tienen lugar en el interior de un domicilio, pues entonces el nivel de impacto en los derechos fundamentales se multiplica: no sólo se menoscaba la inviolabilidad domiciliaria –art. 18.2 CE–, sino que se afecta con mayor profundidad el derecho a la intimidad personal y familiar. Por tal motivo la jurisprudencia de la Sala Segunda (*inter alia*, STS 718/2020, de 28 de diciembre, FJ 7) predica una aplicación ultra-restrictiva de esta diligencia en el ámbito doméstico. La lesión puede ser aún de mayor entidad si se autoriza la captación de imágenes de forma conjunta con el sonido, posibilidad permitida de forma expresa por la norma procesal –art. 588 quater a) apartado 3 LECrim–. En este punto conviene tener presente la tesis de origen germano[18] que propugna la existencia determinadas parcelas de la intimidad humana que no pueden ser invadidas por las autoridades estatales en el curso de la investigación de delitos –*ámbitos de inmunidad*– por hallarse directamente conectadas con la dignidad humana, valor que inspira la totalidad de la CE (Hernández Gil, 1982, pp. 418 a 421). En la práctica, observar esta teoría implicaría que, en determinadas estancias del domicilio, en las que se ejerce una intimidad extrema –*v. gr*., el aseo o el dormitorio–, no cabría realizar las escuchas ambientales; téngase en cuenta que esta regla sería de gran relevancia si se utiliza un smartphone como dispositivo de captación, pues este es un instrumento que las personas frecuentemente portamos con nosotros cuando nos trasladamos a tales espacios.

[18] Esta es la tesis que subyace en la sentencia del Tribunal Constitucional Federal Alemán de 3 de marzo de 2004, mediante la cual el Alto Tribunal declara parcialmente inconstitucional una ley que permitía las escuchas ambientales en el domicilio del investigado. Los magistrados acogen en ella la denominada «teoría de los dos niveles», que consiste en diferenciar dos grados o niveles en la intimidad: un ámbito privado, en primer lugar, y un ámbito intangible o intocable de la vida privada, en el núcleo de este derecho.

IV. El uso de medios técnicos de seguimiento y localización

Desde la óptica del investigador penal, es de gran interés la idea de poder situar a un sospechoso en un lugar y momento determinado, normalmente, en el lugar y momento de la comisión del hecho delictivo; se trata, en palabras de la Sala Segunda, de conocer las «coordinadas espacio-temporales» en las que se movió la persona investigada (STS 291/2021, de 7 de abril, FJ 4). Esta información, si bien difícilmente supondrá una prueba directa del hecho en cuestión, sí es capaz de constituir un poderoso indicio incriminatorio que podría utilizarse contra el acusado para evitar las consecuencias del principio de presunción de inocencia, pues el conocimiento del lugar exacto en el que puede hallarse una persona puede resultar absolutamente decisivo para el esclarecimiento del hecho imputado (STS 141/2020, de la Sala Segunda, de 13 de mayo, FJ 2). Por este motivo, la LO 13/2015 establece una serie de normas que regulan la utilización de esta clase de técnicas por las autoridades, en los artículos 588 quinquies b) y c) de la LECrim.

Con carácter inicial, debe advertirse que en la expresión empleada por el legislador en este contexto «utilización de dispositivos o medios técnicos de seguimiento y localización» se comprenden dos técnicas nítidamente diferenciadas; por lo tanto, es posible afirmar que existen dos «modalidades básicas» (Delgado Martín, 2023, p. 86) dentro de esta medida de investigación, siendo esta una dualidad contemplada incluso por la jurisprudencia del TEDH que se pronuncia expresamente sobre la materia (STEDH Ben Faiza vs Francia, de 8 de febrero de 2018, punto 53). Siguiendo a la FGE[19], dentro del concepto amplio de «geolocalización» se engloba la (i) utilización de dispositivos técnicos basados en sistemas de posicionamiento global (GPS, GLONASS, etc.), comúnmente conocidos como «balizas», o bien (ii) el uso de los datos electrónicos asociados a sistemas de comunicación telefónica. Lógicamente, al estudiar la geolocalización que se realiza a través del smartphone de la persona investigada, centraremos la atención en el segundo supuesto. En punto cabe destacar que tal técnica

[19] *Vid.* 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, punto 3.3.

no será útil para la investigación de los delitos premeditados, pues cualquier criminal medianamente astuto, conociendo las posibilidades de seguimiento que se derivan de su terminal telefónico, evitará portarlo consigo en el momento de perpetrar el hecho delictivo.

Indudablemente, cuando se somete a un individuo a una medida de seguimiento y localización se ocasiona una nítida injerencia en su derecho a la intimidad, tal y como ha sido reconocido de forma reiterada por la jurisprudencia del Tribunal de Estrasburgo (STEDH Uzun vs Alemania, de 2 de septiembre de 2010, punto 52). Al fin y al cabo, el poder hallarse en un lugar ignoto es quizás una de las vertientes más básicas y primitivas del derecho a la privacidad; de hecho, existe una percepción benévola sobre la capacidad de permanecer ilocalizable que trasciende también el ámbito jurídico y subyace en múltiples creaciones artísticas[20]. En este punto, resulta esencial considerar la duración de la medida de localización para valorar la entidad de la injerencia en la privacidad del sujeto pasivo: reparemos en que, dado el «vínculo de proximidad» (Batuecas Caletrío, 2015, p. 49) que existe entre un dispositivo de telefonía y su usuario, el seguimiento de una persona mediante esta técnica permitirá normalmente averiguar todos los desplazamientos que realiza durante un periodo prolongado de tiempo; de esta forma, esta diligencia ofrece a los investigadores penales un conocimiento bastante preciso de sus hábitos y costumbres, con la problemática de la posible formación de un *perfil* del individuo a la que aludíamos anteriormente.

No obstante, entendemos que la medida de geolocalización alcanza un nivel medio de injerencia en la privacidad, por varios motivos. En primer lugar, debe considerarse que esta actuación puede ser menos invasiva que otras diligencias de investigación que incluyen inmisiones visuales o acústicas. Además, debe valorarse que la utilización de esta diligencia únicamente determinará el posicionamiento del terminal que sea posicionado a través de los datos asociados, por lo que no siempre se estará conociendo la posición real del sospechoso. Finalmente, en esta ponderación debe manejarse también la doctrina

[20] La aspiración de situarse fuera de la civilización, desconectado de la sociedad, caracteriza a los protagonistas de abundantes obras literarias (*v.gr. Il barone rampante*, Italo Calvino, 1957) o cinematográficas (por ejemplo, *Jeremiah Johnson*, Sydney Pollack, 1972).

de la expectativa razonable de privacidad: la intimidad no resultaría afectada cuando de forma intencional o consciente el investigado participa en actividades que, por las circunstancias que las rodean, claramente pueden ser objeto de un registro o información pública –*v.gr*., un acto político–. Este nivel medio de injerencia nos permite defender una modificación legal para hacer posible el uso de esta medida de forma autónoma por el Ministerio Fiscal y sin necesidad de recabar la autorización del instructor, siendo que la propia FGE[21] ya se ha pronunciado anteriormente en esta línea. En apoyo de esta reforma puede alegarse que esta técnica suele ser empleada en las fases más incipientes de la instrucción, concibiéndose como un medio para obtener los indicios necesarios con los que solicitar después la práctica de otras medidas de investigación más invasivas que sí exigirán en todo caso la habilitación judicial, como la intervención de comunicaciones telemáticas o el registro de dispositivos informáticos.

V. El registro de dispositivos de almacenamiento masivo de información

Los arts. 588 sexies letra a) a 588 sexies letra c) LECrim regulan el registro de dispositivos de almacenamiento masivo de información. Se trata esta de una diligencia de investigación esencial en la sociedad digital, pues la proliferación en el uso de los dispositivos electrónicos provoca que, en paralelo, haya aumentado el interés de las autoridades penales por acceder a los datos que en ellos se contienen (Escudero García-Calderón, 2022, p. 376). Obviamente, el smartphone constituye actualmente el objeto sobre el que principalmente se aplica esta medida, ya que es el instrumento en el que se contiene la mayor parte de nuestra información personal, bien sea porque la generamos o creamos nosotros mismos con nuestro dispositivo, bien sea porque la conservamos en él tras haberla recibido a través de las múltiples «autopistas de la información»[22] que nos

[21] *Vid*. Memoria de la FGE correspondiente al año 2016, Capítulo VI –«Propuestas de reformas legislativas», págs. 846 y 847.

[22] La expresión era ya utilizada en el preámbulo de la Recomendación número (R) 99 (5), adoptada por el Comité de Ministros de los Estados miembros del Consejo de Europa sobre la protección de la intimidad en Internet, de fecha 23/2/1999.

conectan. Además, es preciso resaltar que la hipercomunicación y el uso intensivo del smartphone, circunstancias a las que hacíamos alusión al inicio de este trabajo, provocan que en la actualidad el examen de nuestro teléfono pueda describir con gran precisión nuestra personalidad. En este sentido, ha de considerarse que hoy en día el empleo de los dispositivos informáticos es de tal intensidad que comprende ya no sólo un uso consciente y voluntario, sino también un uso inconsciente que deja un «rastro oculto» para el propio titular del dispositivo (Sánchez Medrano, 2022, p. 85).

Existen algunas notas que singularizan la medida y que merecen ser destacadas. En primer lugar, podemos referir que se trata de una medida (i) de carácter estático: el registro permitirá a los investigadores conocer el contenido del dispositivo en el momento en que este es aprehendido, pero no los archivos que posteriormente pudiesen almacenarse en él; se diferencia, por tanto, del carácter dinámico que posee el registro remoto de equipos informáticos. En esta línea, es útil acudir a una metáfora gráfica: si el dispositivo del investigado fuese una habitación, el registro de dispositivos sería equiparable a tomar una foto de esa habitación. En segundo lugar, y como consecuencia de lo anterior, la medida (ii) no es susceptible de prolongarse en el tiempo –se agota en sí misma–, con independencia de que siempre será necesario un determinado espacio temporal para su ejecución material. Finalmente, esta diligencia (iii) no requiere necesariamente que rija el secreto previsto de forma genérica para toda medida de investigación tecnológica en el art. 588 bis d) LECrim, pues el carácter estático del registro implica que el secreto no sea imprescindible para garantizar la eficacia de la medida: al no prolongarse en el tiempo, únicamente será preciso que el investigado desconozca la medida antes de que el dispositivo sea intervenido por los agentes de la autoridad[23].

Por otra parte, debe subrayarse el impacto iusfundamental de esta diligencia de investigación, siendo necesario aclarar que se

[23] Esta reflexión, no obstante, ha de tomarse *cum grano salis*: aunque la naturaleza de una concreta diligencia no precise de la declaración de secreto, el instructor debe considerar si la investigación del hecho delictivo puede requerir posteriormente la práctica de otras medidas que sí lo necesitan; en tales supuestos, el conocimiento por parte del afectado de que está siendo objeto del escrutinio estatal puede ponerlo sobre aviso y restar eficacia a otras futuras diligencias.

trata de una actuación en la que es imposible conocer *ex ante* y con precisión los concretos bienes jurídicos que resultarán concernidos. En cualquier caso, el registro de dispositivos afecta de manera nítida al derecho a la intimidad –art. 18.1 CE– y al derecho a la autodeterminación informativa –art. 18.4 CE– de su titular, siendo entendido así por el Tribunal de Estrasburgo (STEDH Mukhtarli vs Azerbaijan y Georgia, de 5 de septiembre 2024, puntos 222 a 224) y por el Tribunal de Luxemburgo (STJUE de 4 de octubre de 2024, recaída en el asunto C-548/2021, punto 26); en la misma dirección, la jurisprudencia de la Sala Segunda ha declarado que el acceso a la memoria de un dispositivo es susceptible de revelar «los más recónditos entresijos de intimidad de su titular» (ATS de 30 de octubre de 2024, FJ 3). Una especial lesión de este derecho se producirá al registrar el smartphone del investigado, un objeto con el que los ciudadanos llevamos actualmente «buena parte de nuestra vida privada a cuestas», como acertadamente ha reflexionado el TS de los EE. UU. (STS Riley v. California, 573 U.S. 373 –2014–, punto III).

Cuando un dispositivo informático guarda en su interior datos que pueden afectar a procesos comunicativos –es decir, mensajes almacenados–, se plantea la posibilidad de que la diligencia objeto de estudio provoque una injerencia en el derecho al secreto de las comunicaciones –art. 18.3 CE–. En este sentido, el Tribunal de Estrasburgo (STEDH Robathin vs Austria, de 3 de julio de 2012, punto 39) ha declarado que el registro sobre «datos electrónicos» es susceptible de lesionar el derecho al secreto de la correspondencia del artículo 8 CEDH. El *punctum dolens* en este ámbito reside no obstante en fijar cuál es el momento en el que finaliza el proceso comunicativo constitucionalmente protegido. Aunque existen varias posturas doctrinales, la jurisprudencia constitucional (STC 173/2011, de 7 de noviembre, FJ 3) ha estimado que este momento se produce cuando el destinatario del mensaje toma conocimiento de su contenido. En este punto, y ante la notable dificultad de constatar el conocimiento efectivo por el receptor, esta teoría asimila el conocimiento con la apertura del mensaje; por el contrario, la comunicación recibida pero no abierta es entendida una comunicación en curso y, en consecuencia, se halla amparada por el derecho fundamental al secreto de las comunicaciones.

Finalmente, el registro de dispositivos colisiona también con el derecho al entorno virtual del investigado. Este moderno bien jurídico fue elaborado por la sentencia del TC alemán de fecha 21/2/2008 sobre la idea de que es posible una «privacidad electrónica» –*elektronische Privatsphäre*–, siendo posteriormente acogido este concepto por nuestro TC[24]. Se trata de un derecho omnicomprensivo, en el que se da un «tratamiento unitario» (STS 105/2025 de la Sala Segunda, de 10 de febrero, FJ 5) a la gran diversidad de datos que pueden contenerse en un dispositivo informático, lo que provoca que en este contexto se vean concernidos o «entremezclados» (Pérez Estrada, 2019, p. 1311) varios de los derechos protegidos por el artículo 18 CE.

Finalmente, conviene resaltar que la ejecución de esta medida requerirá en ocasiones la colaboración de las grandes empresas tecnológicas que fabricaron los dispositivos objeto del registro, compañías que incluyen sofisticadas medidas de seguridad para proteger los datos digitales –el «oro moderno», como antes referíamos– que sus clientes guardan en ellos; así, del mismo modo que en el pasado se valoraba que las cajas fuertes fuesen resistentes para guardar las monedas y las joyas de sus propietarios, en la actualidad los usuarios también buscan que sus dispositivos informáticos sean herméticos. Esta realidad tiene también sus implicaciones para la investigación penal, pues muchas veces la información necesaria para esclarecer un delito se halla en el interior de dispositivos que se hallan blindados frente al acceso no consentido de terceros, incluyendo el Estado; las grandes empresas tecnológicas se erigen por tanto en actores protagónicos también en relación con actividades del ámbito público, ostentando un enorme

[24] *Vid*. la STC 173/2011, de 7 de noviembre, FJ 3, resolución que, por ser de gran interés para este estudio, merece ser reproducida *in extenso*: «Es evidente que cuando su titular 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 más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda de que 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…».

poder que lleva a algunos autores a hablar de «tecnofeudalismo» (Varoufakis, 2024). En nuestra opinión, el deber de colaboración previsto para estas entidades en el art. 588 sexies letra c) apartado 5 LECrim debe ser interpretado en un sentido amplio, pudiendo exigirse cualquier actividad necesaria para llegar hasta los datos almacenados, incluyendo la creación de programas específicos al efecto –*back doors* o puertas traseras–.

VI. El registro remoto de equipos informáticos

El registro remoto de equipos informáticos, regulado en los artículos 588 septies letras a) a c) LECrim, es la medida más vanguardista y, probablemente, la más útil e invasiva de toda la investigación tecnológica; a través de ella, el Estado puede desplegar una vigilancia remota[25] sobre los dispositivos electrónicos o equipos informáticos del sospechoso, logrando la completa observación o «monitorización» (Richard González, 2016, p. 19) de su entorno virtual. Esta medida de investigación puede llevarse a cabo a través de dos vías: bien utilizando el usuario y la contraseña del titular del equipo registrado –es decir, suplantando de forma legítima su identidad–, bien inoculando un software malicioso –*malware*– en el equipo, con el objeto de colonizarlo y controlarlo de forma remota. Como sucedía con el registro de dispositivos referido en el apartado anterior, el smartphone es actualmente el objeto de aplicación preferente en este contexto.

Aunque esta diligencia posee múltiples notas en común con el registro estático, tiene a su vez notables particularidades. En primer término, (a) no exige imperativamente que se produzca una aprehensión física del equipo que va a examinarse. En segundo lugar, (b) el registro remoto posee una naturaleza dinámica, siendo susceptible de prolongarse o extenderse en el tiempo, por lo que no solamente se permite el examen de los datos presentes almacenados en el equipo informático, sino que pueden también accederse a los datos de futuro; utilizando la metáfora del almacén a la que aludíamos más arriba, el registro remoto equivaldría a colocar una cámara en el interior de la estancia y grabar un vídeo durante determinado tiempo, captando

[25] En la expresión anglosajona original, «*remote surveillance*» (Tropina, 2016, p. 100).

todos los movimientos que se producen en ella. En tercer lugar, y como consecuencia de la nota anterior, (c) esta medida sí exigirá que se mantenga el secreto de la investigación, debiendo practicarse con carácter subrepticio. Finalmente, debemos destacar que (d) el nivel de injerencia alcanzado es mucho más elevado que en el registro estático, al permitir al Estado observar el flujo de datos –*data flow*– que se produce en entorno virtual del investigado. Es por ello por lo que puede decirse que el registro remoto «excede» (González Pulido, 2023, p. 268) del registro tradicional o estático.

Atendiendo a estas notas características, el análisis del registro remoto de equipos informáticos conduce a valorar su posible utilización como una vía alternativa para lograr la intervención de las comunicaciones telemáticas, permitiendo de este modo salvar las principales dificultades que en el contexto actual sufre la clásica intervención y a las que nos referíamos *ut supra* –en particular, la encriptación y la lentitud en su desarrollo cuando es preciso acudir a mecanismos de cooperación judicial internacional–. No obstante, con esta solución, que probablemente no se hallaba en la *mens legislatoris* (Bachmaier Winter, 2017, p. 15), se provoca en el patrimonio jurídico de la persona investigada un impacto mucho mayor que con la genuina intervención.

En el ámbito del registro remoto también es posible efectuar algunas consideraciones *de lege ferenda*. En particular, entendemos que la principal modificación legal que debería realizarse en este caso es relativa a la configuración subjetiva de la diligencia. Esta proposición requiere un comentario común sobre las dos medidas de investigación tecnológica que provocan una mayor injerencia en la privacidad: las escuchas ambientales y el registro remoto. En aplicación conjunta –lo cual es legalmente posible–, pueden atribuir al Estado una facultad de control prácticamente omnímodo, permitiendo monitorizar el entorno físico –incluyendo la captación de imagen y sonido, y pudiendo alcanzar el domicilio– y el entorno digital de la persona investigada. La situación se agrava si consideramos la posibilidad de utilizar el smartphone como medio para la aplicación de estas técnicas, como estudiamos en este trabajo. Ante tal panorama, conviene no olvidar el riesgo que entrañan los Estados totalitarios, regímenes que intervendrían por completo la esfera íntima de las

personas si contasen con los medios técnicos necesarios para hacerlo (Fenech Navarro, 1940, p. 162) y que, con independencia de su color, se caracterizan por intentar eliminar cualquier barrera entre la vida pública y la vida privada de sus ciudadanos (Vincent, 1989, p. 192).

Estas consideraciones nos permiten afirmar que el principal defecto de la reforma operada por la LO 13/2015 se halla en depositar el ejercicio de esta enorme facultad de control –en primera instancia– en una única persona. No se ha optado por introducir aquí la prudente dinámica de principio acusatorio, regla que sí impera en otros ámbitos como en la imposición de penas, o en la adopción de la medida cautelar más grave existente en nuestro proceso penal: la prisión provisional. Creemos que cualquiera de estas medidas –las escuchas ambientales o el registro remoto– no deberían poder ser acordadas de oficio por el instructor, debiendo exigirse siempre la petición de una de las partes personadas en la causa. Más inquietante aún resulta valorar el posible –quizás ya probable– uso de estas técnicas por entes privados, dadas las características que pueden ostentar tales actuaciones: existencia de fines diversos a la investigación delictiva, no aplicación de los principios rectores del artículo 588 bis a) LECrim, opacidad, ausencia de cualquier mecanismo de control... Es esta una materia trascendental que ha de preocupar a un Estado vinculado por la doctrina de las obligaciones positivas[26] pero que, lógicamente, deberá ser objeto de otro estudio.

VII. Conclusiones

El smartphone es probablemente el instrumento más característico o representativo de la sociedad digital, constituyendo un descubrimiento que ha transformado por completo nuestra vida diaria de forma similar a lo que en épocas pretéritas sucedió con otros avances capitales para la humanidad, tales como el fuego o la electricidad. Su utilización se produce de forma casi unánime por los ciudadanos, por lo que podríamos decir que, en este sentido, posee un carácter democrático; además, la mayor parte de las personas llevamos a cabo un uso intensivo de este objeto, circunstancia que nos aboca a

[26] Pueden consultarse sobre este aspecto, *ex multis*, las SSTEDH K.U. vs Finlandia (2009) o López Ribalda vs España (2018).

estar –quizás ya a *existir*– en una situación de conexión permanente. No obstante, el teléfono inteligente trasciende su finalidad original y es hoy en día mucho más que un medio de comunicación telemática: no sólo lleva incorporadas una o varias cámaras y un micrófono apto para grabar el sonido ambiente, sino que también permite la geolocalización constante de quien lo porta consigo y contiene una ingente cantidad de información personal, funcionando como una suerte de almacén de la vida privada de su dueño.

Esta realidad es aprovechada por el Estado para desarrollar a través de este instrumento buena parte de las modernas técnicas de averiguación delictiva: intervención de comunicaciones telemáticas y análisis de datos asociados, escuchas ambientales, geolocalización, registro de dispositivos, registro remoto de equipos informáticos… El teléfono inteligente se convierte así en un instrumento común en la dinámica de varias medidas de indagación tecnológica, funcionando como una auténtica *navaja suiza* para el investigador penal. Naturalmente, no toda la investigación tecnológica se relaciona con el smartphone, pero sí podemos afirmar que este objeto tiene actualmente un papel protagónico en este contexto.

La LO 13/2015 es la norma mediante la que se introducen en nuestra ley procesal penal las medidas de investigación tecnológica, suponiendo un paso esencial para que el Derecho –que, como un árbol, es un «instrumento vivo»[27]– ofrezca soluciones útiles en el contexto digital. Tras más de una década de vigencia, podemos efectuar una valoración claramente positiva: frente a la censurable situación de anomia anterior, en la actualidad las autoridades pueden actuar con base en auténticas normas jurídicas, las cuales, como indicaba Passerin (2001, p. 102), no son más que «criterios vinculantes de regularidad». No obstante, sí existen algunos aspectos mejorables en esta normativa. Dejando a un lado algunas cuestiones que el legislador no pudo razonablemente prever en el momento de redactar la norma –Villar Palasí (1975, p. 73) hablaba en estos casos de «lagunas secundarias»–, el principal defecto de esta LO se encuentra a nuestro parecer en la configuración subjetiva de las medidas más invasivas: la captación de comunicaciones orales directas y el registro remoto

[27] Así se expresa elocuentemente el Tribunal de Estrasburgo, *vid.* STEDH Tyrer vs Reino Unido, de 25 de abril de 1978, punto 31.

de equipos informáticos. Tales diligencias permiten monitorizar, respectivamente, el entorno físico y digital de la persona investigada, permitiendo al Estado sondear completamente nuestra vida privada. Es por ello por lo que creemos que sería conveniente introducir en este ámbito la máxima del principio acusatorio, evitando que puedan ser acordadas de oficio por el instructor. En cualquier caso, resulta esencial que su aplicación esté inspirada por el principio de proporcionalidad, cuestión que sí ha sido contemplada debidamente por el legislador en el artículo 588 bis a) de la LECrim.

El panorama antes descrito puede hacernos pensar que el uso del smartphone implica para su usuario una drástica reducción de la privacidad: no sólo permite que, a través de tal instrumento, el estado lleve a cabo un intenso control en el seno de la instrucción penal, sino que también es factible que tal injerencia se realice por entes privados y con fines diversos a la averiguación delictiva. No obstante, esta reflexión sobre una aparente limitación de nuestra intimidad ha de matizarse. En primer lugar, porque debe considerarse que el smartphone se porta siempre voluntariamente, por lo que podría decirse que esa restricción es más bien un *suicidio de la privacidad*. En segundo lugar, creemos que no está tan claro que poseer y utilizar este objeto disminuya nuestra vida privada, al menos si la conceptuamos en un sentido amplio. Pensemos, por ejemplo, en la cantidad de información personal –historias, imágenes, sonidos– que hoy en día podemos guardar con nosotros, y comparémosla con la que podían conservar nuestros antecesores.

Sobre estas reflexiones, puede afirmarse que el uso del smartphone no trae consigo una disminución de la privacidad sino más bien una redefinición de este derecho, el cual es siempre «tributario del espacio y del tiempo» (Carrillo, 2006, p. 27). En cualquier caso, sí es imprescindible que los ciudadanos seamos conscientes de las vulnerabilidades inherentes al uso de los medios digitales y que adoptemos las cautelas oportunas. Se trata de adaptarnos a una nueva realidad, como si nos mudásemos, pasando de vivir en una casa iluminada por un pequeño tragaluz a habitar otra dotada de grandes ventanales. Al fin y al cabo, y contrariamente a lo que muchas veces se cree, el «crepúsculo» es también el momento en el que sale el Sol y nace un nuevo día.

Bibliografía

Andrejevic, M. (2007). Spy: Surveillance and Power in the Interactive Era. University Press of Kansas.

Autor (2024). (Título omitido para garantizar el anonimato en la evaluación).

Batuecas Caletrío, A. (2015). Intimidad personal, protección de datos personales y geolocalización. Derecho privado y Constitución, (29), pp. 47-82. https://www.cepc.gob.es/publicaciones/revistas/derecho-privado-y-constitucion/numero29-enerodiciembre-2015/intimidad-personal-proteccion-de-datos-personales-ygeolocalizacion-0.

Bellovin, S.M., Hutchins, R.M., Jebara, T. y Zimmeck, S. (2014). When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning, New York University Journal of Law & Liberty, 8:555, pp. 555-628. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2320019.

Bellver Capella, V. y Montalvo Jäaskeläinen, F. (2021). El diseño del entorno digital como presupuesto de los Derechos Digitales. Diario La Ley, (49), pp. 1-14. https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAG.

Bachmaier Winter, L. (2017). Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015. Boletín del Ministerio de Justicia, (2195), pp. 1-36. https://revistas.mjusticia.gob.es/index.php/BMJ/article/view/2827.

Cabezudo Rodríguez, N. (2016). Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal. Boletín del Ministerio de Justicia, (2186), pp. 7-60. https://revistas.mjusticia.gob.es/index.php/BMJ/issue/view/1015.

Carrillo, M. (2006). Los ámbitos del derecho a la intimidad en la sociedad de la comunicación. En VV.AA., El derecho a la privacidad en un nuevo entorno tecnológico, (pp. 11-70). Centro de Estudios Políticos y Constitucionales.

Casanova Martí, R. (2016). La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos. Diario La Ley, (8674).

Casas Baamonde, M.E. (2020). El derecho a la protección de datos de carácter personal en la sociedad digital. Fundación Ramón Areces. https://www.fundacionareces.es/recursos/doc/portal/2018/03/20/el-derecho-a-laproteccion-de-datos-personales.pdf.

Castells, M. (1999). La Era de la Información. Economía, Sociedad y Cultura: La sociedad Red. Siglo XXI.

Clarke, R. (1994). The digital person and its application to data surveillance. Information Society.

Consejo de Europa (1999). Recomendación número (R) 99 (5), adoptada por el Comité de Ministros de los Estados miembros del Consejo de Europa sobre la protección de la intimidad en Internet.

Delgado Martín, J. (2023). Dispositivos de localización y seguimiento en la investigación penal, Logos Guardia Civil: Revista Científica del Centro Universitario de la Guardia Civil, (0), pp. 83-105. https://revistacugc.es/article/view/5493.

Escudero García-Calderón, B. (2022). La investigación penal ante las nuevas tecnologías: reflexiones acerca de la «carga desproporcionada» y la «facilitación de información» en el registro de dispositivos de almacenamiento masivo de datos. Anuario de derecho penal y ciencias penales, LXXV, pp. 375-419). https://www.boe.es/biblioteca_juridica/anuarios_derecho/articulo.php?id=ANU-P-.

Fenech Navarro, M. (1940). El juez y el Nuevo Estado. Bosch.

Fernández Rodríguez, J.J. (2016). Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente. Revista Española de Derecho Constitucional, (108), pp. 93-122. http://dx.doi.org/10.18042/cepc/redc.108.03.

Fiscalía General del Estado (2011). Instrucción 2/2011, de 11 de octubre, sobre el/la Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las fiscalías (actualización de 2021). https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-I-2011-00002.pdf.

– (2016). Memoria de la FGE correspondiente al año 2016.

– (2019). 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. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4243.

– (2024). Conclusiones de las 13ª Jornadas de Especialistas en Criminalidad Informática, celebradas en León del 20 al 22 de noviembre de 2024.

González Pulido, I. (2023). Presente y futuro de las medidas de investigación tecnológica en el ciberespacio a nivel internacional. Revista Eletrônica de Direito Processual, 24, (1), pp. 254-292. https://www.epublicacoes.uerj.br/redp/article/view/72246/44610Copyright.

Harari, Y.N. (2017). Homo Deus: breve historia del mañana. Penguin Random House, Barcelona.

Hernández Gil, A. (1982). El cambio político español y la Constitución. Planeta.

Holmes, O.W. (1897). The Path of the Law, Harvard Law Review, (457).

Instituto Nacional de Estadística (2025). Encuesta del Instituto Nacional de Estadística del año 2025, sobre Equipamiento y Uso de Tecnologías de la Información y Comunicación (TIC) en los Hogares. https://www.ine.es/dyngs/Prensa/TICH2025.htm.

Jiménez Campo, J. (1987). La garantía constitucional del secreto de las comunicaciones. Revista Española de Derecho Constitucional, (20), pp. 35-82.

Lasalle, J.M. (2021). Ciberleviatán. Ethic.es. https://ethic.es/2021/09/ciberleviatan/.

Nieva-Fenoll, J. (2016). La recuperación de la privacidad de las comunicaciones. Noticias jurídicas. http://noticias.juridicas.com/conocimiento/articulos-doctrinales/11095-.

Ortiz Pradillo, J.C. (2020). Europa: auge y caída de las investigaciones penales basadas en la conservación de datos de comunicaciones electrónicas, Revista General de Derecho Procesal, (52). https://docta.ucm.es/entities/publication/8da61cec-61f4-47be-998d-6fa0ecc36b52.

Passerin D´Entreves, A. (2001). La noción de Estado. Ariel.

Pérez-Latre, F.J. (2015). La tercera revolución digital: Tecnologías con rostro humano y evaluación antropológica. Revista de Comunicación, (14), pp. 100-113. https://revistadecomunicacion.com/article/view/2707/2219.

Pérez Estrada, M.J. (2019). La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información. Revista Brasileira de Direito Processual Penal, 5, pp. 1297-1330. https://revista.ibraspp.com.br/RBDPP/article/view/253.

Pérez Luño, A.E. (2003). Derechos humanos, Estado de Derecho y Constitución.

Richard González, M. (2017). Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido. Wolters Kluwer.

Rodríguez-Yzquierdo Serrano, M. (2021). La extraterritorialidad en las comunicaciones digitales y las empresas tecnológicas ante el derecho a su secreto: reflexión en torno al caso Microsoft corp. vs. United States. Asuntos Constitucionales, (0), pp. 131-140. https://www.asuntosconstitucionales.com/index.php/numero-0-enerojunio-.

Rodríguez Mourullo, C. (2003). Delito, pena y constitución. Revista Jurídica de la Universidad Autónoma de Madrid, (8), pp. 311-329. https://revistas.uam.es/revistajuridica/article/view/6217.

Sánchez Medrano, F. (2022). El registro de dispositivos de almacenamiento masivo de información. Revista Derecho & Proceso, (1), pp. 83-103. https://revistaderechoyproceso.colex.es/wp-content/uploads/2022/07/1.5ok.pdf.

Tropina, T., Sieber, U. y Von Zur Mühlen, N. (2016). Access to Telcommunication Data in Criminal Justice. A comparative Analysis of European Legal Orders. Duncker and Humblot.

Truong, N. (2020). Comment George Orwell est devenu un penseur visionnaire et iconique du XXIe siècle, Le Monde.

Varona Jiménez, A. (2020). Aspectos relevantes de la interceptación de las comunicaciones telefónicas en el proceso penal español. Ius Inkarri: Revista de la Facultad de Derecho y Ciencia Política, (9), pp. 237-258. https://revistas.urp.edu.pe/index.php/Inkarri/article/view/3687.

Varoufakis, Y. (2024). Somos humildes siervos de los señores de la nube: bienvenidos al tecnofeudalismo. El País. https://elpais.com/ideas/2024-02-11/somos-humildes-siervos-de-los-senores-de-la-nube-bienvenidos-al-tecnofeudalismo.html.

Villar Palasí, J.L. (1975). La interpretación y los apotegmas jurídico-lógicos. Tecnos.

Vincent, G. y Prost, A. (1989). Historia de la vida privada. Tomo V: De la Primera Guerra Mundial hasta nuestros días. Taurus.

Vitalis, A. (1981). Informatique, pouvoir et libertés. Económica.

Zuboff, S. (2019). The Age Of Surveillance Capitalism, New York: Public Affairs.