INTELIGENCIA ARTIFICIAL, BIG DATA, TECNOVIGILANCIA Y DERECHOS FUNDAMENTALES EN EL PROCESO PENAL

Juan Carlos Ortiz Pradillo
Profesor Titular de Derecho Procesal
Universidad Complutense de Madrid
juancarlosortiz@ucm.es

Copia privada del trabajo "Inteligencia artificial, Big Data, Tecnovigilancia y Derechos Fundamentales en el Proceso Penal", publicado en *El Derecho de la Encrucijada Tecnológica. Estudios sobre Derechos Fundamentales, nuevas tecnologías e inteligencia artificial* (Editores: Cesar Villegas Delgado y Mª del Pilar Martín Ríos), Tirant lo Blanch, Valencia, 2022, pp. 103-127 (ISBN 9788411132947).

RESUMEN:
Para Quevedo, Góngora era un hombre pegado a una nariz. Para las empresas, sobre todo las de sectores relacionados con la Economía digital, así como para las autoridades encargadas de la investigación criminal, somos seres pegados a un sinfín de dispositivos informáticos que constantemente generan, reciben, transmiten y almacenan ingentes cantidades de información personal sobre nuestros hábitos y paraderos. Este uso permanente y globalizado de la tecnología ha obligado a redefinir y dimensionar adecuadamente el alcance de los derechos fundamentales recogidos en el artículo 18 de la Constitución Española. Y en este trabajo pongo de manifiesto la necesidad de reconocer una nueva dimensión del Derecho fundamental a la intimidad y a la protección de los datos personales en el proceso penal que consistiría en el «Derecho a no estar localizado» de manera sistemática, sin la adecuada y previa ponderación judicial de la gravedad del sacrificio de los derechos e intereses afectados.

PALABRAS CLAVE:
Inteligencia Artificial, Tecnovigilancia, Derechos Fundamentales, Geolocalización, Proceso Penal.

ABSTRACT:
As Quevedo wrote, Góngora was a man glued to a nose. For Tech-companies, as well as for law enforcemente agencies and authorities we are beings glued to an endless number of electronic devices that constantly generate, receive, transmit and store huge amounts of personal data about our habits and whereabouts. This permanent and globalized use of technology has forced us to redefine and properly size the scope of the fundamental rights contained in Article 18 of the Spanish Constitution. In this paper, I highlight the need to recognise a new dimension of the fundamental right to privacy and data protection in

criminal proceedings, which could be defined as the 'Right not to be located' in a systematic manner, without prior judicial consideration of the seriousness of the sacrifice of the rights and interests affected.

KEYWORDS:
Artificial Intelligence, Electronic Surveillance, Fundamental Rights, Location Tracking, Criminal Justice.

1. DE LA «GALAXIA *GUTENBERG*» A LA «GALAXIA *SMARTPHONE*»: LA HIPERCONECTIVIDAD DE LA SOCIEDAD DEL SIGLO XXI

La actual Sociedad del siglo XXI ha sido tradicionalmente calificada como la "Sociedad de la Información", vista como la sucesora de la sociedad industrial o postmoderna, y caracterizada por el trascendental papel que juegan las tecnologías de la información y la comunicación en las actividades humanas. También denominada como «Era Digital» o «Era Informática», se trata de destacar con tales denominaciones la trascendental influencia que ha tenido la revolución informática, e Internet en particular, para el desarrollo de la Sociedad de la información y el conocimiento.

En efecto, los avances y descubrimientos científicos en materia tecnológica de las últimas décadas han generado una auténtica revolución —la llamada *cuarta revolución industrial*— en ámbitos tan diversos como las relaciones sociales, laborales, educativas, etc. La miniaturización y la reducción de costes en la fabricación y venta de todo tipo de dispositivos electrónicos ha provocado la universalización del empleo de la informática en todos los ámbitos de nuestras vidas, y lo que más interesa ahora destacar, ha supuesto un exponencial avance en lo referido a los modos de conservar y comunicar la información.

En mi opinión, y si lo comparamos con lo que significó la invención de la imprenta a mediados del siglo XV, en términos de capacidad de difundir el conocimiento, los posteriores instrumentos de comunicación —el telégrafo, el teléfono, la radio o la televisión— resultan avances insignificantes si los comparamos con lo que supuso la aparición de Internet porque precisamente lo que caracteriza nuestro mundo actual es la colosal capacidad de crear, conservar y compartir la información. Por ello, debe recordarse la percepción del visionario Herbert Marshall McLuhan, quien a la par del desarrollo de Internet, acuñó en la década de los sesenta el término «aldea global» para describir esa nueva forma de interacción humana a escala global gracias a los nuevos medios electrónicos de comunicación. Desde su óptica, la historia humana puede ser dividida cuatro fases: la agrícola, la mecánica, la eléctrica y la tecnológica, siendo esta última la de mayor relevancia en términos de desarrollo del saber humano.

Este aumento exponencial en el uso de instrumentos electrónicos que manejamos de forma rutinaria en todas nuestras actividades ha dado lugar a una nueva forma de relación entre el ser humano y las máquinas (y las máquinas entre sí) a través del acopio e intercambio de *bytes* para cualquier actividad. Se habla así del *entorno digital* del individuo —al que dedicaré especial atención más adelante—, compuesto por la información en forma electrónica, magnética o luminosa que, voluntaria o involuntariamente, de forma consciente o inconsciente, genera con su actividad, no importa dónde se encuentren los archivos informáticos que la contengan o los canales de comunicación a través de los cuales discurra[1]. Cada vez que realizamos o recibimos una

[1] La primera alusión a dicho «Derecho al entorno digital» la encontramos en GONZÁLEZ-CUÉLLAR SERRANO, N.: "Garantías constitucionales en la persecución penal en el entorno digital", en VV.AA.,

llamada telefónica, enviamos un correo electrónico, compramos a través del comercio electrónico, navegamos por la Red, utilizamos los motores de búsqueda de información en Internet, accedemos a un foro o red social, o nos descargamos algún archivo en nuestro ordenador, etc., estamos generando una abundante información digital. Basta con *googlearse* (i. e., utilizar los grandes motores de búsqueda de Internet para saber qué se dice de nosotros) para comprobar la inimaginable información actualmente disponible la Red sobre nosotros mismos, y a ello habría que añadir toda la información almacenada en las bases de datos de entidades privadas, organismos públicos, etc.

La compra y utilización de todo tipo de dispositivos electrónicos (teléfonos móviles inteligentes ―*smartphones*―, agendas electrónicas, *tablets*, ordenadores portátiles, videoconsolas, reproductores digitales de música y, cada vez más, electrodomésticos domotizados y conectados a Internet, etc.) se ha interiorizado tan rápidamente que resultan ahora indispensables para múltiples facetas con fines laborales, educativos, trámites administrativos y legales, pero sobre todo, para nuestro tiempo de ocio y para nuestras relaciones sociales. Términos como *e-mail, sms, tuit, wasap, post, blog, chat, mp3, usb, gigabite*, etc., se han incorporado a nuestro léxico cotidiano. Y sobre todo, Internet ha modificado por completo los tradicionales canales de comunicación entre las personas: prácticamente se ha abandonado el uso del correo postal a favor del envío de correos electrónicos, la comunicación en tiempo real a través de foros, chats, o servicios de mensajería instantánea. El empleo del telegrama para el envío de mensajes cortos ha caído en desuso, en favor del uso de los e-mails y sms desde ordenadores, agendas electrónicas, *tablets* y teléfonos móviles, y de los "posts" en blogs o redes sociales. Junto con el uso de la telefonía fija alámbrica, cobra cada vez mayor importancia la utilización de la telefonía voIP a través de internet. Programas y herramientas informáticas tipo *Skype, Zoom* y *Whatsapp* causan verdadero furor como nuevas formas de comunicación. La consulta de dudas en los tomos de las grandes enciclopedias ha sido desplazada por el recurso telemático a consultar en la Red. Hay quien opta por consultar sus problemas legales, médicos o sentimentales en foros virtuales y *chatbox* en vez de acudir presencialmente a profesionales cualificados. Y cada día, centenares de miles de personas deciden crearse un "perfil" en alguna de las Redes sociales más conocidas, como por ejemplo, *Facebook, Twitter,* o *Instagram*.

El futuro más inmediato de nuestra Sociedad avanza, en este ámbito, hacia la «hiperconectividad». La computación cuántica, la nanotecnología, el auge del "Internet de las cosas" (IoT) y la conexión 5G auguran un nuevo cambio de paradigma en la Economía y las relaciones humanas basado en la digitalización y la conectividad de todo tipo de objetos, productos y servicios. En poco tiempo habrá billones de dispositivos conectados a la Red. Si la tecnología 2G introdujo los SMS, la 3G impulsó la conexión a Internet y la 4G significó la llegada de la "banda ancha", la tecnología 5G aumentará exponencialmente la velocidad de conexión, reducirá al mínimo la latencia y multiplicará de manera casi ilimitada el número de dispositivos conectados, lo cual redundará en el nuevo modo de comunicar y transmitir información de ese entorno digital al que anteriormente nos referíamos: cualquier objeto podrá estar conectado (con otros objetos y con nosotros) en tiempo real. A través de nuestro *Smartphone* ―en tanto no se generalice un chip hipodérmico recargable― podremos interactuar con cualquier objeto, intercambiando y compartiendo información al instante con los electrodomésticos y demás servicios domotizados de nuestros hogares y nuestros centros laborales, con nuestros automóviles, con el mobiliario público (las farolas de las calles por las que

---

Derecho y Justicia penal en el Siglo XXI. Liber amicorum en homenaje al Profesor Antonio González-Cuéllar García, Colex, Madrid, 2006, p. 1.

paseemos, las marquesinas publicitarias, las señales de tráfico, los controles de peaje de las autopistas, etc.). En definitiva, la fusión entre lo físico, lo biológico y lo tecnológico dará lugar a una nueva Sociedad y, por ende, a nuevas exigencias y desafíos tecnológicos en la investigación criminal.

2. (R)EVOLUCIÓN DIGITAL E INVESTIGACIÓN CRIMINAL EN EL SIGLO XXI: LA «TECNOVIGILANCIA»

Desde los orígenes de los tiempos, siempre han existido crímenes y delitos de todo tipo y, ante ello, la necesidad de esclarecerlos. No en vano, y si atendemos a los textos bíblicos, podría decirse que la primera investigación a los fines de averiguar un hecho delictivo tuvo lugar con el interrogatorio de Dios sobre Caín para resolver lo sucedido[2].

La tecnología también ha estado siempre presente, de una u otra manera, en la búsqueda y recogida de vestigios del delito[3], pues cualquier avance científico (el microscopio, los rayos X, la luz infrarroja o ultravioleta, reactivos químicos, etc.) ha sido paralelamente utilizado, tanto para el desarrollo y progreso de la sociedad civil, como por las autoridades encargadas de la investigación criminal, permitiéndolas resolver los delitos de forma más rápida, eficaz y segura. Así, por ejemplo, al igual que el ser humano se ha servido desde hace siglos de animales para localizar alimentos y vigilar el ganado, las autoridades también han aprovechado las capacidades caninas para tareas de vigilancia y rastreo. Por ello, si la actual Sociedad Digital y la hiperconectividad que la caracteriza ha sido bien recibida por los criminales para desplegar nuevas conductas y servirse de la arquitectura de la Red como vehículo y entorno comisivo, también ha sido aprovechada por las autoridades policiales para aumentar su capacidad investigadora, gracias a lo que yo califico como la *transversalidad* de la prueba electrónica[4]: como quiera que la tecnología está presente en casi cualquier conducta humana, los dispositivos utilizados y la información creada o intercambiada gracias a los mismos constituyen una valiosísima fuente de prueba para investigar y esclarecer cualquier clase de delito, sea o no de los denominados "delitos informáticos".

Es decir, del mismo modo que los criminales han perfeccionado sus técnicas delictivas, las autoridades se han visto en la necesidad de acudir a la ciencia y la tecnología para facilitar las labores de investigación y persecución eficaz de esa delincuencia cada vez más compleja. De la misma manera que hemos pasado de viajar a caballo o en carruaje a utilizar modernas aeronaves que nos permiten alcanzar la órbita exterior terrestre, la policía ha pasado de utilizar linternas y prismáticos a manejar modernas herramientas informáticas y dispositivos electrónicos, tanto en el campo forense (dactiloscopia, balística, acústica, bioquímica, informática), como en el campo operativo, a través de lo que se ha venido a denominar la «vigilancia electrónica o tecnovigilancia[5]».

---

[2] Génesis 4:8-10. «Y Jehová dijo a Caín: ¿Dónde está Abel tu hermano? Y él respondió: No sé. ¿Soy yo acaso guarda de mi hermano? Y él le dijo: ¿Qué has hecho? La voz de la sangre de tu hermano clama a mí desde la tierra».

[3] ORTIZ-PRADILLO, J. C.: *Problemas procesales de la ciberdelincuencia*, Colex, Madrid, 2013, p. 28.

[4] ORTIZ PRADILLO, J. C.: "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica", en VV.AA.: *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito* (Coord. Julio Pérez Gil), La Ley, Madrid, 2012, pp. 267-310.

[5] LLAMAS FERNÁNDEZ, M., GORDILLO LUQUE, J. M.: "Medios técnicos de vigilancia", en VV.AA.: *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia*, Cuadernos de Derecho Judicial, 2007-II, CGPJ, p. 236. La doctrina norteamericana utiliza los términos

En este sentido, se han venido diferenciando tres periodos o etapas en el ámbito de la investigación policial[6]: La primera —época primitiva—, arbitraria o de inexistencia de una verdadera investigación policial en la forma como en la actualidad se la conoce, hasta finales del siglo XVIII; la segunda fase —etapa intermedia—, de iniciación a la Técnica Policial, que alcanza desde el fin de la anterior, hasta finales del siglo XIX; y la tercera fase —Policía Científica—, que se corresponde con el siglo XX y caracterizada por la especialización y profesionalización de la policía en la aplicación de los conocimientos técnico-científicos a la recogida de pruebas e indicios y a la identificación de los autores o partícipes a través de la elaboración de informes periciales sobre ello. En mi opinión, debemos añadir una cuarta etapa, coincidente con el inicio del nuevo milenio, caracterizada por el uso generalizado de los más avanzados instrumentos tecnológicos por parte de las Fuerzas y Cuerpos de Seguridad del Estado, especialmente en labores de investigación y seguimiento —Tecnovigilancia— y ello a pesar de la falta de una legislación suficiente y moderna sobre la materia.

Así, el *ciberpatrullaje* y la búsqueda de datos abiertos en la Red, el rastreo de ficheros con contenido ilícito, el uso de programas informáticos para la lectura automática de matrículas, rostros o bultos sospechosos, el cotejo instantáneo y cruzado de los datos almacenados en las diversas bases policiales, la videovigilancia mediante cámaras con activación remota, los sistemas de imágenes aéreas, térmicas, de visión nocturna o por satélite, los equipos de reconocimiento biométrico de las huellas, iris, rostros o voz de las personas, bultos sospechosos, la utilización de radiobalizas o sistemas de posicionamiento global (GPS) para conocer la ubicación geográfica exacta de un concreto dispositivo de seguimiento de vehículos, embarcaciones o aeronaves, la utilización de georradares para escrutar y sondear el subsuelo, o el control de pagos online y movimientos bancarios son sólo algunos ejemplos de lo que la tecnología facilita en la actualidad las labores policiales de seguimiento e investigación. Dicho en otras palabras, asistimos a un auténtico cambio de paradigma en la investigación policial, en donde el nuevo "teatro de operaciones" se ha trasladado a la búsqueda, acopio y análisis de toda aquella información en formato electrónico que pueda estar relacionada con el entorno virtual del sujeto investigado, y en donde la Inteligencia artificial, el *(big) Data mining* y el *Machine learning* están llamados a representar un abismal salto cualitativo en el uso policial de la tecnología.

3. (R)EVOLUCIÓN TECNOLÓGICA Y LEGISLACIÓN PROCESAL PENAL: UNA LEY DEL SIGLO XIX PARA UNA DELINCUENCIA DEL SIGLO XXI

Para combatir eficazmente la delincuencia de nuevo cuño en el siglo XXI, sin embargo, siempre hemos contado con una legislación del siglo XIX. A finales del siglo XX (década de los noventa), las principales instituciones internacionales abogaban por promover reformas legislativas para incorporar las posibilidades derivadas del desarrollo

"electronic surveillance", "Internet surveillance" y "online surveillance". Vid. BELLIA, P.: "The future of internet surveillance", *The George Washington Law Review,* August, 2004, 72, p. 1375 y ss.; FREIWALD, S.: "Online Surveillance: Remembering the Lessons of the Wiretap Act", *Alabama Law Review*, Fall, 2004, 56, p. 9 y ss.

[6] CABEZAS, P.: La investigación del crimen a través de los tiempos. Tesis doctoral. Universitat Autònoma de Barcelona, 2010. Accesible en la dirección URL https://www.educacion.gob.es/teseo/imprimirFicheroTesis.do?idFichero=FIHxYNhGkts%3D. Fecha de consulta: 7 de abril de 2021.

tecnológico a la investigación procesal. Por citar un ejemplo concreto, en el apéndice de la Recomendación R (95) 13, del Comité de Ministros del Consejo de Europa, de 11 de septiembre de 1995, relativa a los problemas de la legislación procesal penal conectados a las tecnologías de la información, se advertía sobre la insuficiencia de las leyes de la mayoría de los Estados miembros respecto a la existencia de medidas apropiadas para la búsqueda y aprehensión de las evidencias contenidas en los equipos informáticos, y se defendía la necesidad de adaptar las medidas de investigación recogidas en la legislación procesal penal a la naturaleza específica de las investigaciones referidas a los sistemas informáticos, como por ejemplo, regular de manera clara y diferenciada el registro de equipos informáticos (*searching computer systems*), así como la aprehensión de los datos almacenados en aquéllos (*seizing data stored therein*) o la intervención de los datos transmitidos (*intercepting data in the course of transmission*), y todo ello, bajo condiciones similares a las de los tradicionales poderes de entrada y registro sí regulados. Y en su Recomendación R (2005) 10, de 20 de abril de 2005, sobre "medidas de investigación especial" en relación con delitos graves incluidos los actos de terrorismo, el Consejo de Europa apostó por la utilización de especiales medidas de investigación relacionadas con las Nuevas Tecnologías, por ejemplo, a través de la colaboración con el sector privado, los acuerdos internacionales existentes para la cooperación judicial o policial en relación con el uso de técnicas especiales de investigación, especialmente las necesarias en un contexto internacional, o a través de la firma, ratificación y aplicación de los convenios o instrumentos existentes en el ámbito de la cooperación internacional en materia penal en ámbitos como el intercambio de información, entrega vigilada, investigaciones encubiertas y equipos conjuntos de investigación, las operaciones transfronterizas y la formación, con especial mención al Convenio sobre el Cibercrimen de 23 de noviembre de 2001.

Frente a ello, la regulación española en este campo siempre fue considerada claramente deficiente. A pesar de que el Pacto de Estado para la Reforma de la Justicia, suscrito por los dos grandes partidos políticos en 2001, proponía *la aprobación de una nueva Ley de Enjuiciamiento Criminal (...) con especial atención al establecimiento de los métodos de investigación y procedimentales apropiados para el enjuiciamiento de los delitos de nuevo cuño y la adaptación de la regulación de los medios de prueba, en especial a los últimos avances tecnológicos*, dicha adecuación se hizo de rogar. No fructificaron los intentos de aprobación de una nueva legislación procesal en 2011 y 2013, de modo que tuvo que esperarse hasta la aprobación de 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, para poder afirmar, ahora sí, que las autoridades cuentan con una legislación a la altura de los tiempos para poder emplear con las debidas garantías todo el arsenal investigador que el actual desarrollo tecnológico permite. Y mientras tanto, los tribunales utilizaban el archiconocido art. 579 LECrim como «cajón de sastre» para legitimar nuevas metodologías (interceptación de todo tipo de comunicaciones electrónicas, grabación de conversaciones orales, etc.) a pesar de las condenas por parte del TEDH, que siempre había defendido que *la ley debe ser lo suficientemente clara para señalar a todos las circunstancias y condiciones en que autoriza a los poderes públicos a recurrir a una injerencia así, secreta y posiblemente peligrosa, en el derecho al respeto de la vida privada y de la correspondencia*, llegando a exigir expresamente que *las normas sean claras y detalladas, tanto más cuanto que los procedimientos técnicos utilizables se perfeccionan continuamente*[7].

[7] Vid, por todas, las SSTEDH *Kruslin* y *Huvig c. Francia* de 24 de abril de 1990.

No obstante, ya advertí en su momento que esta continua adaptación judicial a las constantes innovaciones tecnológicas corría el riesgo de no superar, en algún momento, las exigencias de legalidad, claridad y previsibilidad establecidas por el TEDH en el contexto especial de medidas secretas de vigilancia y el tiempo nos ha dado la razón: el Tribunal Constitucional, en su STC 145/2014, de 22 de septiembre, puso *pies en pared* ante esta tendencia del Tribunal Supremo de interpretar hiperbólicamente el anterior art. 579 LECrim, exigiendo una habilitación legal con calidad. Para ser más exactos, el Tribunal Constitucional pidió al legislador *una «ley de singular precisión» que defina las modalidades y extensión del ejercicio del poder otorgado con la suficiente claridad para aportar al individuo una protección adecuada contra la arbitrariedad*[8]. Y con tal objetivo, el legislador reconvirtió a marchas forzadas algunos apartados de un futurible Código Procesal Penal en una norma que ahora se antoja trascendental para el estudio que ocupa este trabajo: la señalada Ley Orgánica 13/2015, en cuya Exposición de Motivos sintetiza de un modo muy didáctico su génesis: «*Por muy meritorio que haya sido el esfuerzo de jueces y tribunales para definir los límites del Estado en la investigación del delito, el abandono a la creación jurisprudencial de lo que ha de ser objeto de regulación legislativa ha propiciado un déficit en la calidad democrática de nuestro sistema procesal, carencia que tanto la dogmática como instancias supranacionales han recordado»*.

4. HIPERCONECTIVIDAD Y ENTORNO DIGITAL DEL INDIVIDUO: EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES COMO LA «CENICIENTA» EN EL PROCESO PENAL

Durante mucho tiempo, la alusión recogida en el art. 18.4 CE sobre la necesidad de que la ley pueda limitar el uso de la informática "para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" pasó tan desapercibida en el ámbito de la investigación criminal, que incluso se debatía si se trataba de un verdadero Derecho Fundamental autónomo o, por el contrario, una manifestación constitucional más del Derecho Fundamental a la intimidad de las personas, en todos sus ámbitos[9].

El Tribunal Constitucional había declarado en 1993 que dicho apartado 4º del 18 CE no sólo constituye "un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad", sino también 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[10]»". Y en el año 2000 declaró abiertamente que "Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del 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

[8] STC 145/2014, de 22 de septiembre.

[9] Sobre el sentido y alcance del art. 18.4 CE, vid. MURILLO DE LA CUEVA, L.: *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990; ORTÍ VALLEJO, A.: *Derecho a la intimidad e informática*, Comares, Granada, 1994; ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M.: *La defensa de la intimidad de los ciudadanos y la tecnología informática,* Aranzadi, Pamplona, 1999; Ídem en "La libertad informática, un nuevo derecho fundamental en nuestra Constitución", *La Ley*, núm. 5230, 2001; pp. 1 y ss.

[10] STC 254/1993, de 20 de julio.

terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley[11]".

El Derecho Fundamental a la Protección de Datos Personales adquiere una enorme relevancia en el proceso penal desde el mismo momento en que la fase de investigación constituye una continuada intromisión en el ámbito de tutela que propicia toda la normativa de protección de datos personales, y tal Derecho Fundamental debería quedar incorporado también entre las garantías del debido proceso[12]. Y, sin embargo, nuestros tribunales de justicia apenas le habían otorgado relevancia a la hora de examinar la adecuación constitucional, a dicho Derecho Fundamental, de las medidas tecnológicas de investigación policial centradas en el acopio de información con fines procesales.

Cuando se trata de obtener datos personales en poder de terceros, y dada la legitimidad del fin perseguido por las autoridades policiales y judiciales encargadas de una investigación delictiva, se venía defendiendo la suficiencia de la habilitación general a favor de los Cuerpos y Fuerzas de seguridad prevista en el artículo 22.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal —en vigor transitoriamente, también en virtud de lo dispuesto por la L.O 3/2018, hasta la entrada en vigor de la reciente 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, que ha incorporado nuevas garantías y mayores salvaguardas en la obtención, tratamiento y cesión de dichos datos en el ámbito de la investigación criminal—.

Cuando se trata de obtener información personal almacenada en dispositivos informáticos en poder del propio investigado, se venía considerando que no había propiamente una afectación al *Habeas Data*, de modo que el gran dilema constitucional y procesal se centraba en la necesidad o no de reserva jurisdiccional para la ejecución de la concreta medida de investigación, en función de si la medida afectaba, de manera grave, a la «intimidad» (en donde el art. 18.1 CE no exige exclusividad jurisdiccional), o bien a las «comunicaciones» (cuyo art. 18.3 CE sí impone tal reserva), pues si bien rige como regla general la exigencia constitucional de monopolio jurisdiccional en la limitación de derechos fundamentales, el Tribunal Constitucional siempre había matizado que «no existe en la Constitución reserva absoluta de previa resolución judicial respecto del derecho a la intimidad personal (…) y hemos admitido de forma excepcional que en determinados casos y con la suficiente y precisa habilitación legal sea posible que la policía judicial realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas[13]».

En una Sociedad en la que los dispositivos informáticos (y toda la ingente cantidad de información creada, comunicada y almacenada en los mismos) se han convertido casi en un apéndice más de la anatomía humana y en una prolongación digital de nuestra memoria, la protección frente a injerencias en dicha información debería residenciarse en el Derecho Fundamental a la protección de los datos personales del art. 18.4 CE, y sin embargo, comprobamos como dicho Derecho Fundamental ha sido, tradicionalmente, el menos protegido y ponderado de todos los reconocidos y tutelados por el art. 18 CE, no existiendo un marco jurídico mínimamente suficiente que establezca las condiciones, bajo qué presupuestos y con qué limitaciones pueden aprehenderse, recopilarse, o tratarse

[11] STC 292/2000, de 30 de noviembre.

[12] En este punto, véanse las propuestas de PÉREZ GIL, J.: "Investigación penal y nuevas tecnologías: algunos de los retos pendientes", *Revista Jurídica de Castilla y León*, n.º 7, octubre 2005, p. 226 y ss.

[13] SSTC 70/2002, de 13 de abril y 123/2002, de 20 de mayo.

datos personales de un individuo —almacenados, además, para fines muy diferentes— cuando se trata de vincular tales actuaciones a la prevención o la investigación y represión de la delincuencia[14].

Por fortuna, esta infravaloración del art. 18.4 CE ha sido superada. Ante el crecimiento exponencial de las telecomunicaciones, el surgimiento de nuevas tipologías de datos creados y transmitidos a través de las mismas (datos de conexión, de tráfico, metadatos,…) y las nuevas capacidades de recolección y análisis masivo y automatizado de información de carácter personal, se ha puesto de manifiesto la insuficiencia de dicha jurisprudencia diferenciadora entre art. 18.1 y 18.3 CE a la hora de proteger adecuadamente los derechos fundamentales de los ciudadanos en la nueva Era Digital y la necesidad de potenciar la protección de sus datos personales. De ahí que, en materia de tutela de toda esa información digital que diariamente creamos, modificamos, almacenamos o almacenan otros respecto de nuestra vida (datos personales, económicos, sanitarios, ideológicos, de conexiones, comunicaciones, localizaciones, etc.) se ha ido abriendo camino una corriente jurisprudencial reconocedora de un nuevo Derecho Fundamental relacionado con la protección de los datos personales: el Derecho Fundamental a la protección del «entorno virtual» del individuo. En palabras del Tribunal Supremo, *existe un "derecho al propio entorno virtual" en el que convergen aquellos otros derechos relacionados con la utilización de las nuevas tecnologías, que deberá tomarse en consideración a la hora de examinar las medidas que supongan un sacrificio sobre los mismos*[15].

5. HIPERCONECTIVIDAD, TECNOVIGILANCIA Y GEOLOCALIZACIÓN: EL LABERINTO DEL MINOTAURO Y EL CAPITALISMO DE LA VIGILANCIA

Según cuenta la mitología griega, Ariadna entregó a Teseo un ovillo de hilo de oro para que lo desenrollara según se adentraba en el laberinto del Minotauro, de modo que luego pudiera volver tras sus pasos y encontrar la salida. Hoy en día, más que en Teseo, nos hemos convertido en la versión moderna de Hansel y Gretel[16]: constantemente vamos dejando *migas de pan* en múltiples formatos digitales, a partir de las diversas

[14] ETXEBERRIA GURIDI, J. F.: "Principio se disponibilidad y protección de Datos Personales: a la búsqueda del necesario equilibrio en el Espacio Judicial Penal Europeo", *EGUZKILORE*, nº.23, 2009, p. 359.

[15] STS núm. 342/2013, de 17 de abril. En dicha sentencia se llega a proponer que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Con carácter previo, el Tribunal Constitucional alemán reconoció en su Sentencia 370/07, de 27 de febrero de 2008, un nuevo Derecho Fundamental, incardinado dentro del Derecho a la Autodeterminación informativa, al cual denominó *Derecho Fundamental a la garantía de la confidencialidad e integridad de los equipos informáticos* (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*). Como estudios sobre dicho nuevo derecho fundamental, vid. ORTIZ PRADILLO, J. C.: "El registro 'online' de equipos informáticos como medida de investigación contra el terrorismo (Online Durchsuchung)", en VV.AA., *Terrorismo y Estado De Derecho* (Dir. José Ramón Serrano-Piedecasas), Iustel, Madrid, 2010, pp. 457-478; y 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,* vol. 26, 2011, pp. 67-92.

[16] ORTIZ PRADILLO, J. C.: "Desafíos legales de las diligencias de investigación tecnológica", en VV.AA., *El Proceso Penal. Cuestiones fundamentales*, (Coord. Olga Fuentes Soriano), Tirant lo Blanch, Valencia, 2017, pp. 303-316.

interacciones que llevamos a cabo (comunicaciones a través de nuestros teléfonos móviles y otros dispositivos, navegación web, compras online y uso de medios electrónicos de pago, tránsito por lugares videovigilados, etc.). Además, gracias a una alta capacidad de digitalización y cruce de datos, toda esa información a la que nos referimos puede relacionarse con una ubicación geográfica[17]. En la navegación web, cada vez son más habituales los servicios basados en localización (LBS —*Location Based Services*— o LDIS —*Location Dependent Information Services*—) que se ofrecen a los usuarios de dispositivos electrónicos y que proporcionan un valor añadido relacionado con el contexto en el que se encuentran los usuarios[18]. Ese valor añadido suele corresponderse con la entrega de información geográfica y el geoprocesamiento de los usuarios móviles con base en su posicionamiento actual, a veces facilitada por el cliente (vía GPS, Wi-Fi, dirección IP, etc.), a veces por el servidor (ej. servicio de posicionamiento suministrado por el operador de la red). En este sentido, al entrar a un restaurante y hacer una foto —y a veces sin ni siquiera tomar esa foto— *Google* nos ofrece la posibilidad de hacer una reseña en la Red sobre la calidad de dicho establecimiento; si viajamos al extranjero y abrimos nuestro perfil de *Twitter* o *Facebook*, es muy probable que nos aparezca publicidad y noticias en el idioma del país en el que nos encontramos; y si abrimos cualquier aplicación de la denominada "Economía colaborativa" (*Airbnb, Wallapop, Uber, MyTaxi,* etc.), en nuestro dispositivo nos aparecerán ofertas que se encuentran en un radio geográfico muy próximo a nuestra ubicación.

En la actual Sociedad Tecnológica a la que me estoy refiriendo, y debido al uso exponencial que hacemos de nuestros diversos dispositivos informáticos, dichos instrumentos no deben ser considerados propiamente como simples instrumentos de comunicación, sino como incansables creadores de información referida a quienes los utilizan, de modo que las autoridades encargadas de una investigación criminal podrán servirse de las vastas posibilidades que ofrecen las nuevas capacidades de recopilación y análisis de información («tecnovigilancia») a la hora de determinar la identidad de un sujeto, su ubicación en un momento concreto y en un lugar determinado o sus movimientos pasados, presentes o futuros (lo que, en adelante, denominaremos «geolocalización»).

En efecto, el sueño de cualquier investigador sería localizar ese ovillo de hilo de oro que, recogiéndolo como si fuera el sedal de una caña de pescar, le permitiera identificar, localizar y aprehender al autor de un hecho delictivo. Hoy en día, y con motivo de la investigación de un hecho sucedido en el pasado en un lugar concreto, ya no sólo se atiende a buscar vestigios físicos en la escena del crimen o a recabar testimonios de posibles testigos presenciales de los hechos, sino también rastros digitales dejados por los posibles partícipes (v. gr., datos de conexión de sus teléfonos móviles con puntos de acceso wi-fi o antenas BTS que dan cobertura a esa zona) o almacenados en instrumentos electrónicos (cámaras de videovigilancia de entidades públicas o privadas). Y con tal finalidad, comprobamos como las capacidades policiales de localización, aprehensión y análisis de los datos personales de los ciudadanos para su posterior utilización en el Proceso Penal se han visto favorecidas por un nuevo modelo de Economía mundial que se ha calificado como «el capitalismo de la vigilancia[19]». Frente al capitalismo de la era

[17] DÍAZ DÍAZ, E., "La "huella histórica" de la geolocalización personal", publicado el 8 de marzo de 2017 en la página web http://tecnologia.elderecho.com/tecnologia/internet_y_tecnologia/Derecho_Geoespacial-privacidad-seguridad-geoinformacion-datos-servicios_geograficos-abogados_11_1063930005.html.

[18] PAYERAS CAPELLÀ, M. M. et al.: "Privacidad en servicios turísticos basados en geolocalización", *Revista de Derecho, Empresa y Sociedad (REDS)*, núm. 5 julio-diciembre 2014. p.78.

[19] ZUBOFF, S.: *The Age Of Surveillance Capitalism*. PublicAffairs, New York, 2019.

industrial, centrado en la explotación de las materias primas naturales y que utilizaba a las personas como mano de obra, la materia prima en el capitalismo de vigilancia son las propias personas (fuentes de información); sus datos obtenidos a partir de la vigilancia del comportamiento de las personas para predecir sus comportamientos futuros, que posteriormente son monetizados a través de su venta a terceros.

En la película *Sneakers* (1992, traducida en España como *Los Fisgones*), cuyo argumento trata de un grupo de expertos informáticos que, por encargo de una agencia secreta, roban un dispositivo capaz de decodificar cualquier sistema, hay un diálogo entre *Marty* Bishop (Robert Redford) y *Cosmo* (Ben Kingsley) en el que este último le dice: «El mundo ya no está manejado por armas, ni energía, ni dinero, sino por unos y ceros, pequeños pedazos de datos. Todo es solo electrones (…). Hay una guerra allá afuera, viejo amigo. Una guerra mundial y no se trata de quién tiene más balas. Se trata de quién controla la información. Lo que vemos y escuchamos, cómo trabajamos, lo que pensamos... ¡se trata de la información!».

Esa recopilación, almacenamiento, segmentación y clasificación de todo tipo de datos, unida a las actuales obligaciones legales de conservación de determinados datos y a las potentes herramientas de análisis y procesamiento de dicha información, permiten a las empresas —y, por ende, a las autoridades— la creación de los denominados «perfiles de personalidad» de los ciudadanos. Las primeras los utilizarán para predecir comportamientos y tendencias que les permitan anticiparse al mercado y obtener un beneficio económico en su labor empresarial, y las segundas los recopilarán para conocer sus movimientos y ubicaciones pasadas, presentes y futuras con una precisión abrumadora.

Hay quien relaciona esta nueva forma de investigación policial con la película *Minority Report* (2002), basada en un relato corto de 1956 de Philip K. Dick titulado *El informe de la minoría*, pero resulta que, mucho tiempo atrás, en 1941, Miguel Fenech escribía lo siguiente: «el liberalismo no establece leyes que afecten al fuero interno porque no le parece justo intervenir en la esfera íntima del hombre; el Estado totalitario no las establece porque carece de medios técnicos de vigilar su cumplimiento. Si se inventase un aparato que permitiera leer los pensamientos y descifrar las intenciones, el Estado totalitario desarrollaría en el acto una vivísima legislación interna[20]».

Hoy ya es posible afirmar que existe esa capacidad de predecir, o al menos reconstruir, los movimientos y los pensamientos de las personas. De una parte, la tecnología facilita la labor estatal de averiguar la identidad o la ubicación de un determinado sujeto, simplemente recolectando esas migas de pan que todos vamos diseminando consciente o inconscientemente con nuestras interacciones digitales. La «Inteligencia de Fuentes Abiertas (OSINT, *Open Source Intelligence*[21])» consiste precisamente en eso; en recopilar y analizar toda esa información disponible en múltiples formatos (metadatos, imágenes, videos, etc.) en fuentes accesibles a cualquier persona. Y de otra parte, las grandes empresas tecnológicas pueden poner en manos del Estado más y mayor información sobre los ciudadanos que las propias Administraciones y Registros Públicos, de modo que el Estado ya no necesita llevar a cabo ingentes esfuerzos por crear bases de datos, sino limitarse a conseguir la colaboración de tales empresas en la

[20] FENECH, M.: *El juez y el Nuevo Estado*. Bosch, Barcelona, 1940, p. 162, citado por MAROTO CALATAYUD, M.: "Las redes sociales en internet como instrumento de control penal: tendencias y límites", en VV.AA. *Derecho y Redes Sociales* (eds: Artemi Rallo Lombarte y Ricard Martínez Martínez). Civitas, Madrid, 2013, pp. 427-484.

[21] Y específicamente referido a la recolección y análisis de la información arrojada a través de las Redes Sociales, se habla de «*Social Media Intelligence* (SOCMINT)».

recolección y conservación de la información que posteriormente será utilizada en la persecución de conductas criminales para conocer la identidad o el paradero de un sujeto.

Señalaré un ejemplo concreto: un modo de "geolocalizar" a un individuo consiste en el empleo de instrumentos y dispositivos de localización y seguimiento —balizas, drones, datos de localización que emita su propio terminal móvil— para conocer los movimientos de un individuo en tiempo real. Pero también se puede llegar a reconstruir su actividad pasada a través de la recolección de datos personales almacenados por entidades privadas con otros fines y del examen inteligente de las comunicaciones y conexiones efectuadas por los dispositivos electrónicos de dicha persona, y conocer así con gran precisión los lugares visitados, las rutas utilizadas, las personas con las que contactó, sus hábitos y rutinas, etc. De conformidad con los principios de licitud, lealtad y finalidad, la policía podría recabar los datos en poder de terceros referidos a la matrícula del vehículo empleado (por ej., de las bases de datos de las cámaras de la DGT; de las empresas de alquiler de vehículos[22]; de las concesionarias de Autopistas de Peaje; o de las empresas concesionarias de Parkings y Servicios de Estacionamiento Regulado en superficie); los referidos a viajes y pernoctaciones del sujeto investigado (por ej., los datos de hospedaje remitidos a las autoridades policiales a través de los canales telemáticos de entrega de los Libros-registros y partes de entrada de viajeros o los datos PNR[23] remitidos por parte de las compañías aéreas y otras entidades obligadas). También cabría acudir al examen pericial de los propios dispositivos de navegación del sospechoso o de su teléfono móvil en busca de datos electrónicos acreditativos de las distintas interacciones de dicho terminal que faciliten a las autoridades conocer las ubicaciones y rutas seguidas por ese terminal[24]. Y, por supuesto, también podrán acudir a las operadoras de servicios de acceso a la telefonía móvil e internet para que cedan los datos de tráfico y de localización del terminal empleado por el investigado conservados en virtud de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Parafraseando el título de una conocida película, la indagación sobre el entorno digital de los ciudadanos permite a las autoridades «saber lo que hicisteis el último verano», y dónde estuvisteis, vuestros movimientos, con quién contactasteis, etc., lo cual puede resultar igual o incluso más importante para la averiguación de un delito que su localización en tiempo real, así como también más invasiva. No en vano, la instrucción judicial consiste precisamente en eso: la reconstrucción de las circunstancias en las que se produjeron unos hechos delictivos en el pasado para determinar cuándo sucedieron, dónde se produjeron y quiénes los ejecutaron, de modo que la geolocalización en tiempo real permite conocer el paradero del sospechoso, mientras que la geolocalización histórica

[22] Como ejemplo de datos de los geolocalizadores instalados por las compañías de alquiler de vehículos empleados para la averiguación de hechos delictivos, vid. SAP Valladolid, secc. 4ª, 174/2020, de 30 de octubre y SAP Almería, secc. 3ª, 816/2019, de 30 de junio de 2020).

[23] Las siglas PNR significan «Passenger Name Record» —Registro de Nombres de Pasajeros— y se refieren a informaciones que determinadas empresas y compañías aéreas deben remitir a los Estados, en virtud de lo establecido en la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave. En España, dicha Directiva ha sido incorporada a través de la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves.

[24] Como, por ejemplo, los ficheros almacenados en la tarjeta SIM o los datos de conectividad wi-fi de puntos de acceso a los que se hubiera conectado dicho terminal.

permite conocer, entre otras circunstancias, si el sospechoso se encontraba o no en el lugar de los hechos en el momento de su comisión o si interaccionó con la víctima o con otros partícipes del hecho.

6. EL «DERECHO FUNDAMENTAL A NO ESTAR GEOLOCALIZADO» COMO NUEVA DIMENSIÓN DE LA INTIMIDAD Y LA PROTECCIÓN DE DATOS PERSONALES EN EL PROCESO PENAL

La consecuencia de dicha evolución tecnológica y su aplicabilidad en el terreno de la investigación criminal es la enorme afectación a los derechos referidos a la personalidad de los ciudadanos (intimidad, inviolabilidad domiciliaria y de las comunicaciones y protección de datos personales). La recopilación y análisis inteligente de las interacciones o movimientos de una persona de un modo continuado en el tiempo o la reconstrucción sistemática de sus actos y desplazamientos realizados en el pasado representa una injerencia grave en tales derechos fundamentales, más si cabe cuando para ello se emplean técnicas de vigilancia encubierta, masiva y automatizada[25].

Por todo ello, si el Tribunal Constitucional ha aseverado que el titular de un ordenador personal "cuando navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico (…), 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., que (…) si se analizan en su conjunto, no cabe duda 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[26]", considero que la misma conclusión puede hacerse si lo que se lleva a cabo es un seguimiento continuado o una reconstrucción sistematizada de los movimientos e interacciones de un individuo con la finalidad de geolocalizarlo en una coordenadas concretas en un determinado momento.

Hasta épocas recientes, la posibilidad de conocer la ubicación espacio-temporal de un determinado sujeto y sus desplazamientos (geolocalización) se había considerado tradicionalmente por parte de los tribunales como una legítima diligencia policial de investigación que no requería de autorización judicial por no interferir *gravemente* en ningún Derecho Fundamental. A pesar de que nuestro ordenamiento jurídico no contenía una mínima regulación legal sobre las vigilancias discretas, ni visuales, ni a través de dispositivos de seguimiento adheridos a objetos usados o a disposición de la persona investigada, el Tribunal Supremo había elaborado un cuerpo jurisprudencial habilitador del empleo policial de radiotransmisores (denominadas "balizas de seguimiento GPS"), para la localización de embarcaciones, vehículos o aeronaves porque se entendía que no vulneraban el derecho fundamental al secreto de las comunicaciones ni suponían una injerencia excesiva sobre el derecho fundamental a la intimidad a los efectos de exigir un

[25] Tal y como gráficamente describe VELASCO NÚÑEZ, E.: *Delitos tecnológicos: definición, investigación y prueba en el proceso penal.* Sepin, Madrid, 2016, p. 24, dicha actuación aporta "una potencial enorme cantidad de información sensible que puede ir desde sus preferencias religiosas —frecuenta una mezquita—, sexuales —frecuenta un bar gay, un club de alterne, el domicilio de un amante—, políticas —presencia en un determinado mitin o manifestación—, de salud —prácticas de aborto, tratamiento de VIH—, vida personal y familiar, rutas —donde puede ser hasta secuestrado—, aficiones y datos que lleven, obviamente, hasta resolver y descubrir también delitos".

[26] STC 173/2011, de 7 de noviembre.

control jurisdiccional previo y una ponderación sobre dicha afectación constitucional[27]. De los argumentos esgrimidos por el Tribunal Supremo, el más criticable era aquel según el cual no existía una injerencia grave en la intimidad porque "*podría haber afectación a la intimidad del investigado si esa localización permitiera conocer el lugar exacto en el que el comunicante se encontraba, pero cuando (...) esa ubicación sólo puede concretarse con una aproximación de varios cientos de metros, que es la zona cubierta por la BTS o estación repetidora que capta la señal, en modo alguno puede considerarse afectado, al menos de forma relevante, el derecho a la intimidad del sometido a la práctica de la diligencia*[28]. Y digo que resultaba criticable, porque hacer depender la exigencia de autorización judicial (por afectar de manera "relevante" a dicho Derecho Fundamental) del grado de precisión con que se determine la localización geográfica de una persona a través de instrumentos electrónicos, no hacía sino añadir mayor confusión e inseguridad jurídica a esta materia, pues sólo era cuestión de tiempo que la tecnología utilizada evolucionase para poder localizar, de manera exacta y casi sin margen de error, la posición geográfica de una persona, para que tal doctrina del Tribunal Supremo fuera superada[29]. Además, resultaba llamativo que dicha actuación policial en espacios públicos fuera legitimada por entenderse que apenas incidía de modo leve en la intimidad de una persona, y al mismo tiempo fuera proscrita cuando la geolocalización la llevaba a cabo un detective privado en investigaciones relacionadas con bajas laborales fraudulentas porque tal actividad afectaba *a una de las manifestaciones de su derecho a la intimidad: el derecho a que los demás no sepan dónde está en cada momento y cuáles son sus movimientos; o dicho en otros términos, el derecho a no estar localizado de manera continua por medios electrónicos colocados en sus bienes contra su voluntad*[30].

En la actualidad, y dado el avance tecnológico, no sólo se puede geolocalizar y rastrear a un individuo en tiempo real, sino que, como hemos comprobado, también se puede llegar a reconstruir su actividad pasada, y conocer así con gran precisión sus ubicaciones e interacciones, esto es, se pueden crear auténticos «perfiles de comportamientos». Aunque el TEDH afirmara en su Sentencia de 2 de septiembre de 2010 (caso *Uzun*) que el uso de una baliza policial GPS suponía una menor afectación sobre la intimidad del investigado que un seguimiento policial permanente, no es lo mismo efectuar un seguimiento puntual y concreto que toda una reconstrucción de movimientos o una vigilancia sistemática y automatizada de la actividad de un individuo.

Un ejemplo de la repercusión del avance tecnológico sobre la intimidad y la vida privada de las personas en este ámbito referente a la geolocalización, lo encontramos en

---

[27] Véanse, entre otras, las SSTS núm. 562/2007, de 22 de junio; 523/2008, de 11 de julio; 906/2008, de 19 de diciembre; STS 798/2013, de 5 de noviembre y 610/2016, de 7 de julio. Como análisis de dicha jurisprudencia, vid. ORTIZ PRADILLO, J. C.: "El impacto de la tecnología en la investigación penal y en los derechos fundamentales", en VV.AA., *Problemas actuales de la justicia penal* (Dir. Nicolás González-Cuéllar Serrano), ed. Colex, Madrid, 2013, p. 339.

[28] STS núm. 906/2008, de 19 de diciembre.

[29] En el mismo sentido, PÉREZ GIL, J.: "Los datos sobre localización geográfica en la investigación penal", en VV.AA., *Protección de Datos y Proceso Penal* (coord. Ernesto Pedraz Penalva), La Ley, Madrid, 2013, p. 314.

[30] Vid., por todas, la STS, sala de lo social, de 21 de junio de 2012 (Núm. Recurso 2194/2011), confirmatoria de la STSJ del País Vasco, de 10 de mayo de 2011 (núm. Rec. 644/2011). La STS, sala de lo civil, núm. 278/2021, de 10 de mayo, también ha refrendado que la utilización por parte de detectives privados de dispositivos de localización y seguimiento *tiene una incidencia directa en el círculo de exclusión que cada ciudadano define frente a terceros como esfera de su intimidad o vida privada y constituye uno de los supuestos de intromisión ilegítima a que se refiere el art. 7 de la L.O. 1/1982*.

la evolución de la jurisprudencia de la Corte Suprema norteamericana en materia de afectación a la Cuarta Enmienda —el derecho a la privacidad y a no sufrir una invasión o pesquisas arbitrarias— con motivo del rastreo y localización geográfica de un individuo[31]. Si en el caso *Knotts* (1983) se legitimó, sin necesidad de una decisión judicial previa (warrant), la instalación de un radiotransmisor en una lata de cloroformo que la policía vendió al sospechoso y que éste dejó en el interior de su vehículo porque una persona que viaja en un automóvil en la vía pública no tiene ninguna expectativa razonable de privacidad en sus movimientos de un lugar a otro, en el caso *Jones* (2012) se consideró que sí había habido una afectación a la Cuarta Enmienda con motivo de la instalación de un dispositivo GPS en un vehículo, no sólo por el desarrollo de la tecnología y del instrumento utilizado, sino también por el grado cuantitativo de la injerencia sobre la privacidad de los individuos, pues en el caso *Knotts* el dispositivo de seguimiento se empleó durante unas horas, mientras que en el caso *Jones* la policía controló los movimientos del vehículo del sospechoso las 24 horas del día durante 28 días, concluyendo el Alto Tribunal que "el seguimiento GPS durante un largo plazo en las investigaciones de la mayoría de los delitos afecta a las expectativas de privacidad, y una conclusión similar volvió a dictar en el asunto *Carpenter* (2018), no ya respecto del uso policial de una baliza GPS, sino respecto de la obtención policial de los datos de geolocalización del teléfono móvil del sospechoso conservados por la operadora de telecomunicaciones, tras concluir que el seguimiento de los movimientos pasados de una persona a través de esos datos de posicionamiento de su teléfono móvil resulta "detallado y enciclopédico" y constituye una injerencia sobre la intimidad de las personas mucho mayor que con el monitoreo GPS, pues ofrece "una ventana a la vida privada reveladora, no sólo de sus concretos movimientos, sino también, y a través de ellos, sus vínculos familiares, políticos, profesionales, religiosos y sexuales" y otorga al gobierno "una vigilancia perfecta que le permite viajar atrás en el tiempo para rastrear el paradero de una persona".

En la misma dirección, y con motivo de la reforma de la LECrim en virtud de la señalada L.O. 13/2015, el Tribunal Supremo ha modificado su anterior doctrina y ha terminado por reconocer que "el conocimiento por los investigadores del lugar exacto -presente, pasado o futuro- en el que podía hallarse una persona" puede resultar absolutamente decisivo para el esclarecimiento del hecho imputado"; que "la utilización de dispositivos de localización y seguimiento tiene una incidencia directa en el círculo de exclusión que cada ciudadano define frente a terceros y frente a los poderes públicos está ya fuera de cualquier duda. La afectación de la intimidad es incuestionable (...)"; y que "la entrada en vigor de la LO 13/2015 descarta cualquier duda acerca de la voluntad legislativa de blindar ese espacio de intimidad y subordinar la legitimidad del acto de intromisión a la previa autorización judicial[32]".

Como conclusión, y si se admite el Derecho a la intimidad como "elemento de desconexión social[33]", considero que se debería reconocer que el «Derecho a no estar localizado» es una manifestación más del derecho a la intimidad y a la protección de datos personales, de modo que será precisa una especial protección del mismo frente al

[31] Con mayor detalle, vid. ORTIZ PRADILLO, J. C.: "El impacto de la tecnología…", op. cit.

[32] STS núm. 141/2020, de 13 de mayo.

[33] REBOLLO DELGADO, L.: *Derechos fundamentales y protección de datos*. Dykinson, Madrid, 2004, p. 40.

conocimiento de los Poderes públicos[34] porque "forma parte del contenido constitucionalmente protegido (en nuestro caso, ex arts. 18.1 y 18.4 CE) la capacidad de cualquier ciudadano de situarse geográficamente en un punto del espacio, con la confianza en que el dato de su localización no va a ser captado, archivado y tratado de forma automatizada por terceros[35]".

[34] En este sentido, la Circular FGE 4/2019, de 6 de marzo, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización (p. 16) reconoce que el fundamento de la previsión legal del nuevo art. 588 quinquies LECRIM, según expone el Preámbulo de la LO 13/2015, "no es otro que la incidencia que en la intimidad de cualquier persona puede tener el conocimiento por los poderes públicos de su ubicación espacial".

[35] MARCHENA GÓMEZ, M. / GONZÁLEZ-CUÉLLAR SERRANO, N., *La reforma de la Ley de Enjuiciamiento Criminal*, ediciones jurídicas Castillo de Luna, Madrid, 2015, p. 363.