

INTELIGENCIA ARTIFICIAL E INVESTIGACIÓN PENAL

PROTECCIÓN DE LOS DERECHOS
FUNDAMENTALES Y DEL PROCESO DEBIDO

MARÍA LOURDES NOYA FERREIRO

Prólogo

Víctor Moreno Catena

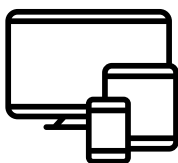




¡Gracias por confiar en nosotros!

La obra que acaba de adquirir incluye de forma gratuita la versión electrónica. Acceda a nuestra página web para aprovechar todas las funcionalidades de las que dispone en nuestro lector.

Funcionalidades eBook



**Acceso desde
cualquier dispositivo con
conexión a internet**



**Idéntica visualización
a la edición de papel**



Navegación intuitiva



Tamaño del texto adaptable

Síguenos en:



INTELIGENCIA ARTIFICIAL E INVESTIGACIÓN PENAL

**Protección de los derechos
fundamentales y del proceso debido**



INTELIGENCIA ARTIFICIAL E INVESTIGACIÓN PENAL

**Protección de los derechos
fundamentales y del proceso debido**

María Lourdes Noya Ferreiro

*Profesora Titular de Derecho Procesal
Universidad de Santiago de Compostela*

Prólogo

Víctor Moreno Catena

COLEX 2025

Copyright © 2025

Queda prohibida, salvo excepción prevista en la ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra sin contar con autorización de los titulares de propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (arts. 270 y sigs. del Código Penal). El Centro Español de Derechos Reprográficos (www.cedro.org) garantiza el respeto de los citados derechos.

Editorial Colex S.L. vela por la exactitud de los textos legales publicados. No obstante, advierte que la única normativa oficial se encuentra publicada en el BOE o Boletín Oficial correspondiente, siendo esta la única legalmente válida, y declinando cualquier responsabilidad por daños que puedan causarse debido a inexactitudes e incorrecciones en los mismos.

Editorial Colex S.L. habilitará a través de la web www.colex.es un servicio online para acceder a las eventuales correcciones de erratas de cualquier libro perteneciente a nuestra editorial.

© María Lourdes Noya Ferreiro

© Editorial Colex, S.L.
Calle Costa Rica, número 5, 3.º B (local comercial)
A Coruña, 15004, A Coruña (Galicia)
info@colex.es
www.colex.es

*A Victor Moreno Catena, del que he aprendido el espíritu
crítico en la Academia y la tolerancia en la vida.*

SUMARIO

PRÓLOGO

Prólogo	13
---------------	----

INTRODUCCIÓN

Introducción	17
--------------------	----

CAPÍTULO I

MARCO LEGISLATIVO

1. Regulación europea	21
1.1. El Libro Blanco sobre la Inteligencia Artificial	26
1.2. El Reglamento Europeo de Inteligencia Artificial y su influencia en la investigación penal	32
1.2.1. Clasificación de los sistemas de IA.	36
1.2.2. Garantías para el uso de los sistemas de IA del alto riesgo	43
1.2.3. Garantías relacionadas con el tratamiento de datos. Una aproximación a su estudio.	48
2. Inteligencia artificial y protección de datos	52
2.1. La Directiva 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de Protección de Datos Personales	52
2.1.1. Antecedentes	52
2.1.2. Ámbito objetivo y subjetivo de aplicación	58
2.1.3. La supervisión de la autoridad independiente de control. Su determinación respecto de los datos relacionados con la Administración de Justicia.	60
2.2. LO 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.	65
2.2.1. Ámbito objetivo y subjetivo de aplicación	65
2.2.2. Autoridades responsables del tratamiento y autoridades independientes de control	67

SUMARIO

2.2.3. Principios relativos al tratamiento de datos personales. Calidad de los datos.	69
2.2.4. Tratamiento de datos integrados en categorías especiales.	72
2.2.5. Tratamiento de los datos obtenidos de las cámaras de videovigilancia policiales	74

CAPÍTULO II

DERECHOS FUNDAMENTALES E INTELIGENCIA ARTIFICIAL

1. La investigación con sistemas de inteligencia artificial y la protección de los derechos fundamentales relacionados la vida privada. Especial referencia al derecho a la protección de datos personales y al entorno virtual . . .	77
1.1. Inteligencia artificial y derechos fundamentales.	77
1.2. La incidencia de la inteligencia artificial en los derechos fundamentales a la intimidad, a la inviolabilidad del domicilio y al secreto de las comunicaciones	81
1.2.1. La incidencia en el derecho a la intimidad	81
1.2.2. La incidencia en el derecho a la inviolabilidad del domicilio	88
1.2.3. La incidencia en el derecho al secreto de las comunicaciones.	90
1.3. Especial referencia a los derechos a la protección de datos personales y al entorno virtual como límite en la aplicación de los sistemas de inteligencia artificial	93
1.3.1. El derecho a la protección de datos	93
1.3.2. El derecho al entorno virtual o digital.	102
2. La incidencia de la inteligencia artificial en los derechos fundamentales de naturaleza procesal	106
2.1. Derecho a la tutela judicial efectiva e Inteligencia artificial	108
2.2. Derecho de defensa e Inteligencia artificial	113
2.3. Derecho a la presunción de inocencia e Inteligencia artificial.	122

CAPÍTULO III

LA ACTUACIÓN POLICIAL COMO PUNTO DE PARTIDA EN LA INVESTIGACIÓN PENAL

1. Reflexiones previas	127
2. Consideraciones puntuales sobre las actuaciones policiales a prevención	132
2.1. Una primera aproximación	132
2.2. Garantías frente a la actividad policial de prevención	136
3. La vigilancia policial	139
3.1. Consideraciones iniciales	139
3.2. Captación de imágenes. Videovigilancia; una breve referencia a los drones como instrumentos de vigilancia policial	144
3.2.1. Cámaras de videovigilancia	144
3.2.2. Vigilancia policial con drones	148

SUMARIO

3.3. Dispositivos de geolocalización y seguimiento: una aproximación a su estudio	152
3.3.1. Instrumentos vinculados al investigado	152
3.3.2. Geolocalización no vinculada al investigado.	156
3.3.3. Geolocalización vinculada a datos proporcionados por terceros . . .	158
3.4. Rastreo de redes	161

CAPÍTULO IV

LA EFICACIA DE LA INVESTIGACIÓN POLICIAL CON INTELIGENCIA ARTIFICIAL EN EL PROCESO PENAL. PROPORCIONALIDAD Y CONTROL JUDICIAL

1. Introducción.	169
2. El principio de proporcionalidad	174
2.1. Consideraciones previas.	174
2.1.1. Principio de idoneidad.	175
2.1.2. Principio de necesidad	175
2.1.3. Proporcionalidad en sentido estricto	176
2.2. El principio de proporcionalidad en la LO 13/2015, de modificación de la Ley de Enjuiciamiento Criminal	177
2.3. La aplicación del principio de proporcionalidad y la protección de datos personales.	179
3. El control judicial de las medidas policiales a prevención	184
3.1. Control judicial relativo a la adquisición del material obtenido	184
3.1.1. La importancia del control judicial	184
3.1.2. Elementos de referencia en el control judicial	188
3.2. Control judicial relativo a la incorporación del resultado al proceso	190
3.2.1. Incorporación del resultado de las medidas policiales a prevención al proceso.	190
3.2.2. Algunas reflexiones sobre la cadena de custodia.	195

BIBLIOGRAFÍA

Bibliografía	199
------------------------	-----

PRÓLOGO

La tarea de presentar una monografía, que ha requerido muchas semanas y meses de trabajo, de estudio de materiales, de análisis de toda la información disponible, de redacción del texto, de revisión y de actualización, es una encomienda bastante comprometida, especialmente si se aborda con el espíritu crítico que debe inspirar toda la actividad universitaria. El compromiso se agiganta cuando nos encontramos con una materia en formación, como es el desarrollo y aplicaciones de la inteligencia artificial (IA), que está mereciendo una abrumadora atención por estudiosos de las más diversas disciplinas, y también en cuanto incide en el ámbito de nuestro sistema de justicia.

He recibido con una inmensa alegría la petición de que redactara el prólogo de este libro, y he podido leer la generosa dedicatoria de Lourdes Noya; seguro que no merezco sus palabras, pero eso no me impide sentirme enormemente orgulloso. Aunque el contenido de un prólogo, salvo alguna extravagante excepción, debe ser elogioso con la obra que se presenta, en este caso los elogios responden con rigor al contenido de la monografía. Aquí estamos ante un trabajo arduo, complicado, que necesita de continuas actualizaciones porque el tema de estudio está sometido a constantes revisiones y aportaciones; pero el estudio de la IA en la investigación penal se aborda en este libro con una extraordinaria dosis de sentido práctico y pone en valor los principios y las garantías constitucionales básicas que legitiman la investigación de los delitos.

La Dra. Noya Ferreiro, que ha hecho anteriores incursiones en esta materia apasionante, nos ofrece ahora una obra muy relevante, sobre IA e investigación penal, que incide en la protección de los derechos fundamentales cuando se utilizan herramientas de IA para investigar delitos. El trabajo se centra en ciertas herramientas de investigación de delitos y su incidencia en el ejercicio de los derechos fundamentales de los ciudadanos, alejándose del uso de la IA con fines de predecir conductas delictivas.

La autora pone el énfasis en el control judicial, no solo para autorizar el uso de instrumentos de nuevas tecnologías, como sucede con las cámaras de videovigilancia, sino para incorporar al proceso penal el resultado de las

medidas utilizadas. Respecto del uso de videovigilancia, se analiza en el libro su utilización para diferentes finalidades: investigar a personas concretas, o para vigilancia indirecta, como cuando se graba en un lugar público, pero de acceso normalmente restringido. Asimismo, se estudian las medidas de geolocalización y rastreo en redes, lo que hace sumamente interesante y útil la lectura y consulta de esta investigación.

Pero seguramente uno de los puntos más señalados de esta obra sea su preocupación por la vigencia y aplicación del principio de proporcionalidad para autorizar el uso y controlar la incorporación al procedimiento de estas herramientas de IA, porque la inercia y una especie de «veneración» hacia la IA puede hacernos «bajar la guardia» ante las garantías.

No podemos olvidar que la IA se desarrolla esencialmente por el sector privado con fines estrictamente económicos, y que asistimos impasibles a estrategias diseñadas e implantadas por las compañías más poderosas que nunca han existido (Apple, Microsoft, Alphabet —Google—, Amazon, Meta...), dirigidas a ampliar el campo de sus potenciales «clientes» con la estrategia de monopolizar el mercado y obtener resultados económicos cada vez mayores, a costa del dinero y de las libertades de los ciudadanos. El *modus operandi* es simple: se lanzan unos productos atractivos para los clientes, que se ofrecen gratis o a precios muy reducidos, con lo que consiguen eliminar a sus anteriores competidores; despejado el campo, se rentabilizan con creces las aplicaciones (navegadores de internet, motores de búsqueda, mapas y herramientas de tráfico de vehículos, redes sociales, plataformas, etc.) de los modos y por las vías más diversas: insertando anuncios individualizados, sometiendo a vigilancia a los usuarios, obteniendo contratos con los responsables de seguridad (administraciones, policía y ejército), o simplemente incrementando el precio de las suscripciones, y todo ello apropiándose impunemente de todo el conocimiento generado por la humanidad (Naomí KLEIN se refiere al «gran robo de la inteligencia artificial»). Los que ganan no son los usuarios, sino las empresas propietarias de esos productos, y que, además, terminan despidiendo a miles y miles de trabajadores.

Aunque puedan parecer realidades o mundos desconectados y, en todo caso, distantes, la IA y la justicia penal guardan relaciones estrechas, porque los sistemas de IA pueden emplearse en apoyo de las partes, como instrumentos o herramientas de IA para la investigación y la prueba, una actividad que, con carácter general, es ajena a la función del juez, aunque estas herramientas están de modo casi exclusivo a disposición de las acusaciones.

Es evidente la preocupación de la legislación por las aplicaciones de IA en la investigación de los delitos, si bien la IA puede estar presente en procedimientos de otros órdenes. La Dra. Noya Ferreiro deja de lado los problemas de la actuación anticipatoria de los delitos, la llamada «policía predictiva», que opera en el terreno de la prevención de los delitos. Estos policías pueden usar sistemas de IA para, a modo de ejemplo y entre otros varios conocidos

hoy en día, la elaboración de patrones para predecir e investigar, la determinación de zonas de patrullaje preferente, la determinación del riesgo de victimización en violencia de género (*VioGen*, en funcionamiento en España desde 2007, que ha pasado en 2025 a *Viogen II*, con un protocolo avanzado de detección de riesgos).

También como pionero en el mundo, en materia de prevención, el Cuerpo Nacional de Policía de España puso en marcha en 2018 un sistema de detección de denuncias falsas en casos de robo con violencia, *VeriPol*, que ha estado vigente hasta octubre de 2024, cuando la policía decidió retirarlo aduciendo que carece de validez en procedimientos judiciales, si bien el hecho de la retirada ha coincidido con la publicación del Reglamento UE 2024/1689, de 13 de junio, de Inteligencia Artificial (RIA), que establece estrictos controles para el uso de los sistemas de IA de alto riesgo, y de un informe que señalaba serias deficiencias en el funcionamiento de la herramienta policial.

El Anexo III.6.e) del RIA contempla la habilitación a la policía para la «elaboración de perfiles» durante la investigación o el enjuiciamiento de delitos, lo que significa autorizar, con las prevenciones de los sistemas de IA de alto riesgo, el «tratamiento automatizado de datos personales» para «evaluar con ellos determinados aspectos personales», y «analizar o predecir aspectos relativos» a su «fiabilidad, comportamiento, ubicación o movimientos», según expresiones de la Directiva de protección de datos, sin que sea suficiente la limitación contenida en los arts. 10 y 11 de la misma Directiva (UE) 2016/680 del PE y del CE, de 27 de abril, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos,.

Tal vez sea importante resaltar que, dentro de la actividad de investigación y persecución de la delincuencia encomendada al sistema de justicia, el primero de los problemas que se advierte es el de la desigualdad de quienes intervienen en un procedimiento penal, pues comúnmente el acceso y el uso de la IA está a disposición de una de las partes (la acusación) en tanto la otra se encuentra imposibilitada de cuestionar siquiera el procedimiento de obtención de los datos o informaciones, o de reaccionar frente al resultado que se ofrece.

Para obtener pruebas durante las investigaciones, el Ministerio Fiscal y las fuerzas policiales pueden disponer de sistemas de IA, que son de titularidad pública y se encuentran a disposición exclusiva de la acusación, que debe ser una parte del proceso, mientras que el investigado habrá de soportar el resultado que arroje la IA.

Es cierto que se intenta limitar el campo de actuación de los sistemas de IA más invasivos y que afectan directamente los derechos fundamentales, frente a quienes invocan la seguridad pública y el furor punitivista y frente a

los intereses de los desarrolladores de IA, y el RIA cataloga en como prohibidos un conjunto de instrumentos susceptibles de un uso muy efectivo en tareas de persecución penal, aunque el problema seguirá subsistiendo si los resultados no terminan por aflorar en las diligencias judiciales y se usan para actuaciones policiales.

Además, se ha de tener en cuenta que cuando la acusación se ha valido de un resultado obtenido con IA, el imputado no tiene acceso al algoritmo y a las operaciones que el sistema ha realizado para arrojar el resultado que se incorpora al procedimiento. Es decir, la prueba se toma como «verdad revelada» e indiscutible porque en la práctica no se puede someter a contradicción. Como es obvio, el acusado carece de recursos (y normalmente de conocimientos) para analizar el algoritmo que se ha empleado y poder detectar posibles fallas, o modular el resultado; mucho menos, para crear un algoritmo alternativo que pudiera arrojar un resultado diferente (en todo o en parte diferente).

Se puede decir, y es cierto, que cuando las operaciones algorítmicas pueden afectar derechos fundamentales se deberá obtener una previa autorización judicial, pero, aun salvada esta objeción, el derecho de defensa y el debido proceso se niegan o se ponen en cuestión cuando se sustenta la acusación en medios de prueba obtenidos con IA, y no sirve con invocar el carácter público del sistema y su pretendida transparencia, porque acabamos de presenciar en España la retirada de un sistema público de detección de denuncias.

Víctor Moreno Catena

Catedrático Emérito de Derecho Procesal

INTRODUCCIÓN

La sociedad actual camina hacia un mundo en el que las conexiones entre seres humanos y máquinas serán lo más habitual, convirtiendo lo que hasta ahora era ficción literaria o cinematográfica, en una realidad que cada vez está más cerca.

Junto al uso, ya habitual, de las tecnologías de la información y de la comunicación (TIC), se suma ahora la constante evolución de un conjunto heterogéneo de sistemas o instrumentos a los que se denomina «Inteligencia Artificial» (IA). Estas aplicaciones «inteligentes» tienen ya cabida en muchas actividades del sistema sanitario, en el campo científico y de la investigación, en el marco de la seguridad, y también en el mundo laboral, empresarial, social, y desde luego en el ámbito jurídico.

Resulta evidente que el Sistema de Justicia, y especialmente de Justicia penal, no es ajeno, ni debe serlo, a la introducción de los avances tecnológicos y de los instrumentos de IA. La justicia del siglo XXI responde, como no puede ser de otra forma, a la evolución y los cambios que ha experimentado la sociedad actual. Cambios que se suceden a una velocidad impensable pocos años atrás, sin tiempo para la reflexión, y mucho menos para que las reformas legales se adapten y se consoliden en un tiempo en el que lo novedoso y la respuesta inmediata rige el día a día de los ciudadanos. En esta realidad cambiante, y sin tiempo para adaptar y consolidar principios y fundamentos propios de una justicia «moderna» y eficaz para la sociedad a la que se debe, los avances científicos y tecnológicos se convierten en un factor principal para el diseño de ese modelo de justicia, y desde luego, para el nuevo proceso penal. Tratándose de un recurso imprescindible para la investigación y prueba en el proceso penal, la implantación de los sistemas de IA requiere también nuevos modelos de control y de actuación de los distintos operadores que intervienen en él, todo ello con la finalidad de garantizar la eficacia sin perder de vista las garantías. Este nuevo modelo de justicia penal y de configuración del proceso penal, ha de articularse necesariamente sobre los principios estructurales que rigen el proceso penal constitucional.

La primera dificultad que surge a la hora de hacer referencia a las aplicaciones de inteligencia artificial, es la de dar un concepto que englobe todos

los instrumentos que se pueden integrar en esta categoría. Precisamente, la variedad y complejidad de estos instrumentos, y su constante evolución, requiere que el concepto que los defina se aborde desde la flexibilidad, lo que permitirá la integración de nuevos modelos.

Tanto la Comisión Europea en 2018, como el Parlamento Europeo en 2019 atendiendo a las recomendaciones del Grupo de Alto Nivel de Expertos en IA ha dado diferentes definiciones relativas a la Inteligencia artificial, para, en 2023, llegar a un acuerdo y tomar como referencia el enfoque propuesto por la OCDE, que la define como el conjunto de aquellos sistemas *«basados en máquinas que, mediante objetivos explícitos o implícitos, infiere, a partir de los inputs que recibe, cómo generar outputs, como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los distintos sistemas de IA varían en función de los niveles de autonomía y capacidad de adaptación tras su lanzamiento»*. Este enfoque ha pasado a convertirse en el concepto de inteligencia artificial establecido en el artículo 3.1.1) del 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.

Desde la perspectiva de su aplicación en la Administración de Justicia, preocupa especialmente su incorporación en la fase de investigación del proceso penal y en la investigación policial previa.

Es obvio que la función policial ha experimentado grandes cambios en los últimos años, pasando de una policía reactiva, que respondía ante la comisión de hechos delictivos, o ante los desórdenes públicos ocasionados por los ciudadanos, a una policía en la que las funciones preventivas e incluso predictivas se han convertido en importantes aportaciones en la defensa de la seguridad, y en la lucha contra la criminalidad.

Resulta evidente que los avances tecnológicos, y con ellos los avances en el campo de la inteligencia artificial, favorecen la comisión de hechos delictivos en los que se utilizan los sistemas inteligentes como instrumentos para facilitar actuaciones delictivas, y para evitar la persecución policial y penal. En este escenario, las unidades policiales han de recurrir también al uso de estos instrumentos en su lucha contra la criminalidad. Los avances que se han producido en estos últimos años en la función investigadora de la policía, se deben, en parte, a la utilización de sistemas que le permiten afrontar la investigación penal con mayores garantías de éxito y en un tiempo más reducido.

No obstante, también es una realidad, y así se refleja en los documentos internacionales y nacionales sobre inteligencia artificial, que la utilización de estos sistemas puede suponer un peligro para el proceso penal del Estado de Derecho y para los derechos fundamentales, tanto los relacionados con la vida privada de los ciudadanos, como aquellos de naturaleza procesal. Esta preocupación constante de doctrina y jurisprudencia, y de los legisladores

europeos y nacionales ha llevado al diseño, en algunos textos legales, de las garantías que han de observarse en su aplicación para preservar el proceso debido y proteger los derechos fundamentales de los ciudadanos.

Esta misma inquietud ha animado a un grupo de profesores universitarios y de expertos juristas a colaborar en un Proyecto de investigación I+D «*Inteligencia artificial, Justicia y Derecho: ¿irrupción o disrupción tecnológica en el proceso penal?*», (PID 2020-119324GB-I00), financiado por el Ministerio de Ciencia e Innovación, cuyo desarrollo se ha prolongado durante tres años, finalizando en el pasado mes de febrero.

La investigación realizada en estos años en el marco de dicho proyecto, ha centrado mi estudio en los límites a la aplicación de la Inteligencia Artificial en el proceso penal, convirtiéndose la investigación policial en el centro de atención. Motivo de ello no es solo el desarrollo de dicha investigación y los instrumentos utilizados por las unidades policiales, sino, fundamentalmente, las garantías que han de rodear el uso de dichos recursos tecnológicos como paraguas para la protección de los derechos fundamentales en juego, y los requisitos y condiciones que han de presidir la incorporación, en su caso, de los resultados obtenidos en el proceso.

Obviamente, no se ha tratado de llevar a cabo un análisis exhaustivo de los instrumentos relacionados con la inteligencia artificial que se emplean por la policía en la fase de investigación preprocesal. La intención es poner de relieve las garantías que han de observarse en su ejecución y en su posible traslado al proceso, todo ello con el fin de preservar los derechos fundamentales de los ciudadanos, el proceso debido y el proceso penal constitucional, en un momento en el que la línea que separa las actuaciones policiales preventivas y la investigación policial desarrollada en la fase de instrucción es cada vez más difusa.

Es cierto que la defensa de la seguridad y la persecución de actuaciones delictivas cada vez más complejas y sofisticadas, favorecidas por el avance tecnológico, ha de centrar y así lo hace, las funciones de las Fuerzas y Cuerpos de la Seguridad del Estado, que habrán de utilizar todos los recursos que la tecnología le ofrece. No obstante, en este loable empeño, no pueden ponerse en riesgo valores, principios y garantías constitucionalmente recogidos y que, desde un enfoque de la Administración de Justicia, constituyen la esencia del Estado de Derecho.

CAPÍTULO I

MARCO LEGISLATIVO

1. Regulación europea

El antecedente de la normativa europea relacionada con los sistemas de Inteligencia Artificial (IA) con incidencia en la investigación criminal, puede situarse en una serie de recomendaciones e indicaciones acordadas por grupos de expertos organizados por entidades e instituciones supranacionales, que colocan el respeto al Estado de Derecho y a los derechos y libertades de los ciudadanos, como pilares de la convivencia. Conscientes de los importantes avances que pueden derivar de la aplicación de la Inteligencia Artificial, también son prudentes al valorar los grandes retos que dicha aplicación supone. En consecuencia, con las citadas recomendaciones tratan de arbitrar principios, protocolos y directrices, que permitan que los recursos integrados en la Inteligencia artificial se administren buscando el equilibrio entre las garantías y la eficacia¹.

Esta doble vertiente en la aplicación de la Inteligencia Artificial se pone ya de manifiesto por la Comisión Europea en el Libro Blanco sobre la Inteligencia Artificial. Un enfoque europeo orientado a la excelencia y la confianza, cuando ya apunta, en la introducción, que *«La inteligencia artificial se está desarrollando rápido. Cambiará nuestras vidas, pues mejorará la atención sanitaria (por ejemplo, incrementando la precisión de los diagnósticos y permitiendo una mejor prevención de las enfermedades), aumentará la eficiencia de la agricultura, contribuirá a la mitigación del cambio climático y a la correspondiente adaptación, mejorará la eficiencia de los sistemas de producción a través de un mantenimiento predictivo, aumentará la seguridad de los europeos y nos aportará otros muchos cambios que de momento solo*

1 BARONA VILAR, S., *Algoritmización del derecho y de la justicia. De la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, Valencia, 2021, pág. 128.

podemos intuir. Al mismo tiempo, la inteligencia artificial (IA) conlleva una serie de riesgos potenciales, como la opacidad en la toma de decisiones, la discriminación de género o de otro tipo, la intromisión en nuestras vidas privadas o su uso con fines delictivos»².

Pero con anterioridad a este importante documento, ha de destacarse el esfuerzo realizado por la Organización para la Cooperación y el Desarrollo Económico (OCDE)³, una de las primeras en elaborar las directrices que, sobre el uso de los sistemas inteligentes, deberían presidir las políticas de los Estados cara a su desarrollo. Así, en mayo de 2019, se hacen públicas estas orientaciones, que son fruto del trabajo de diversas instituciones académicas, empresariales, científicas, etc.⁴. Los llamados *Principios de la OCDE sobre Inteligencia Artificial*⁵, no son vinculantes para los Estados miembros y firmantes, pero pueden tomarse como referencia para las regulaciones nacionales e internacionales⁶. Se fundamentan en el respeto a los derechos humanos y a los valores democráticos, la equidad y la innovación, atendiendo también a la inclusión como actuación vinculada a la diversidad, y se concretan en cinco bloques: 1) Crecimiento inclusivo, desarrollo sostenible y bienestar; 2) Respeto al Estado de Derecho, los derechos humanos y los valores

2 LIBRO BLANCO sobre la inteligencia artificial — un enfoque europeo orientado a la excelencia y la confianza — Publications Office of the EU (europa.eu)

3 La OCDE es una organización internacional de carácter intergubernamental en la que los Estados miembros trabajan conjuntamente para responder a los retos económicos, sociales y ambientales derivados de la interdependencia y la globalización. Se creó después de la Segunda Guerra Mundial bajo el nombre de Organización para la Cooperación Económica Europea (OECE) con el propósito de coordinar el Plan Marshall. En 1961, se convirtió en la Organización para la Cooperación y el Desarrollo Económico (OCDE), con vocación transatlántica y después mundial. España es miembro desde el 3 de agosto de 1961. Actualmente, la OCDE cuenta con más de 35 miembros. En materia económica y comercial lleva a cabo las siguientes actividades:

Analiza y publica datos comparativos y previsiones; Fomenta la adopción de medidas para promover el crecimiento y la estabilidad económica; Favorece la cooperación entre gobiernos para trabajar en el fortalecimiento del comercio multilateral; Fomenta la expansión de los servicios financieros y la inversión internacional; Impulsa buenas prácticas a nivel internacional.

Promueve acuerdos para la adopción de instrumentos, decisiones y recomendaciones que ayuden a crear reglas del juego comunes que faciliten el progreso de los países, en el marco de una economía mundial globalizada.

V. <https://comercio.gob.es/PoliticaComercialUE/OMCOrganismosInternacionales/Paginas/ocde.aspx>

4 A dichas orientaciones a los Estados miembros de la OCDE, se suman Argentina, Brasil, Colombia, Costa Rica, Perú y Rumanía

5 V. OECD Legal Instruments. <https://legalinstruments.oecd.org>

6 Además de los señalados en la nota anterior, las recomendaciones de la OCDE han sido acogidas por el G20, la Unión Europea, Japón, Estados Unidos y otras jurisdicciones, y han informado el trabajo de las Naciones Unidas y el Consejo de Comercio y Tecnología entre la UE y EE.UU.

democráticos, incluida la equidad y la privacidad; 3) Transparencia y explicabilidad; 4) Robustez y seguridad; 5) Rendición de cuentas.

En 2024 se aborda en la organización su actualización, proponiéndose actuaciones que pretenden el tratamiento de la seguridad, con la finalidad de proporcionar los mecanismos necesarios para evitar daños o comportamientos no deseados. Se traslada la importancia de salvaguardar una información segura y veraz. Se favorece la responsabilidad empresarial durante toda la vida del sistema inteligente. Se fomenta la transparencia en relación con el funcionamiento del sistema. Y también se hace referencia a la sostenibilidad ambiental, destacando la necesidad de un trabajo conjunto de todas las instituciones y organismos implicados⁷.

En noviembre de 2019, la 40ª Conferencia General de la UNESCO, elabora un documento, el *Proyecto de texto de la Recomendación sobre la Ética de la Inteligencia Artificial*, en el que defiende una recomendación sobre el uso ético de la inteligencia artificial, que se aprueba en la Asamblea General en noviembre de 2021, firmándola ciento noventa y tres países que forman parte de la UNESCO⁸. La aplicación ética de la Inteligencia artificial se ha de fundamentar en tres pilares, el respeto de los derechos humanos, el Estado de Derecho y la lucha contra la discriminación.

No cabe duda que el Consejo de Europa y la Unión Europea comparten principios y valores, lo cual ha permitido que buena parte de las reflexiones sobre el futuro marco jurídico para la inteligencia artificial, se hayan desarrollado no sólo en el seno de las instituciones de la Unión, sino también bajo el paraguas del Consejo de Europa. Algunas de sus grandes iniciativas han puesto de relieve los principios básicos que deben presidir la aplicación de la IA en los ámbitos relacionados con la Administración de Justicia: el respeto a los derechos humanos, la calidad y seguridad que han de ofrecer estas aplicaciones, la transparencia y el control por los usuarios.

Respondiendo a esta inquietud, la Comisión Europea para la eficacia de la Justicia (CEPEJ)⁹, ya en 2016, dicta las denominadas «*Recomendaciones para impulsar el cambio hacia la Ciberjusticia*». Para ello, parte del análisis de las aplicaciones utilizadas en aquel momento, centrándose en el acceso a la justicia, con el mantenimiento en todo caso de las garantías procesales, la

7 V. <https://www.camtic.org/actualidad-tic/ocde-actualiza-principios-de-ia-para-mantenerse-al-tanto-de-rapidos-avances-tecnologicos>.

8 V. <https://unesdoc.unesco.org/ark:/48223/pf0000376713>.

9 La Comisión Europea para la Eficacia de la Justicia (CEPEJ), creada en septiembre de 2002 (Resolución Res (2002)12 del Comité de Ministros del Consejo de Europa), se compone de expertos de todos los Estados Miembros del Consejo de Europa. Su función es mejorar la eficacia en el funcionamiento de Justicia en los Estados Miembros del Consejo de Europa y desarrollar la puesta en práctica de los instrumentos normativos adoptados por el Consejo de Europa. En ningún caso supervisa la actuación de los sistemas judiciales de los Estados miembros.

comunicación entre tribunales y profesionales, las aplicaciones relacionadas con la administración judicial, y la asistencia a la labor del juez y del letrado de la administración de justicia. Además, estas directrices pretenden también facilitar la labor de los responsables políticos, en relación con la búsqueda de una justicia más ágil y eficaz a través de la utilización de las aplicaciones de la IA, pero situando su actuación desde la perspectiva de los principios generales¹⁰.

Siguiendo esta línea, y centrándose en su aplicación en el ámbito judicial, también la CEPEJ elabora, en diciembre de 2018, la Carta Ética Europea sobre el uso de la Inteligencia Artificial en los Sistemas Judiciales y su entorno, en la que, partiendo de la aplicación de los sistemas de IA, trata de garantizar el respeto a los derechos protegidos en el Convenio Europeo de Derechos Humanos. En este documento se analiza la incorporación de aplicaciones de IA al proceso, poniendo de relieve algunas de las cautelas que han de presidir su utilización en el proceso penal, para preservar el derecho a un proceso justo. Son cinco los pilares sobre los que se construye este sistema de protección: el respeto de los derechos fundamentales, la no discriminación, la calidad y seguridad, la transparencia, imparcialidad y equidad, y el control del usuario¹¹.

Los riesgos relacionados con la utilización de los sistemas inteligentes se ponen una vez más de relieve por la «Conferencia sobre el impacto del desarrollo de la inteligencia artificial en los derechos humanos, la democracia y el Estado de Derecho», celebrada en Helsinki, en febrero de 2019¹². Entre sus conclusiones, señala que el diseño, el desarrollo y el despliegue de las herramientas de IA, deben ser objeto de una evaluación de riesgos conforme a los principios aplicables. Partiendo de esta premisa, todos los procesos automatizados deben ser diseñados para que puedan ser examinados por un revisor humano. La transparencia algorítmica es crucial para crear confianza y garantizar la debida protección de los derechos. Además, en todos los casos en que se alegue la existencia de violaciones de los derechos humanos, deben existir recursos eficaces en el marco de las competencias públicas y privadas. La igualdad ante la ley no debe verse comprometida por el cálculo algorítmico. Las herramientas de IA pueden apoyar a jueces capacitados,

10 En este sentido BARONA VILAR, S., *Algoritmización del derecho y de la justicia...*, op. cit., págs. 141 y 142

11 V. más ampliamente BARONA VILAR, S., *Algoritmización del derecho y de la justicia...*, op. cit., 2021, págs. 144 y 145.

12 Como consecuencia de esta conferencia, el Comité de Ministros del Consejo de Europa crea, en septiembre de 2019, un Comité sobre Inteligencia Artificial, con el objetivo de estudiar la viabilidad de un marco jurídico para el desarrollo, diseño y aplicación de la inteligencia artificial, basado en las normas del Consejo de Europa sobre derechos humanos, democracia y Estado de Derecho.

mientras que el contenido y los contornos de las leyes y los sistemas legales de las sociedades democráticas deben seguir siendo gobernados por seres humanos¹³.

Además de los antecedentes anteriores¹⁴, que reflejan la constante preocupación por una utilización ética y responsable de los avances tecnológicos, los progresos en innovación y la inteligencia artificial, en el seno de la Unión Europea se aborda una labor normativa que pretende diseñar una regulación marco que permita la armonización de las legislaciones de los Estados miembros. En este sentido, han de destacarse dos recomendaciones a la Comisión sobre la regulación de aspectos éticos y de responsabilidad civil relativos a la IA. La primera de ellas, de octubre de 2020, es una *Propuesta de Reglamento del Parlamento Europeo y del Consejo, sobre los principios éticos para el desarrollo, el despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas*. La segunda, también de octubre de 2020, incorpora una *Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a la responsabilidad civil por el funcionamiento de los sistemas de IA*. De igual forma, y persiguiendo ese objetivo de armonizar las legislaciones de los Estados miembros, se publica la *Propuesta de Directiva del Parlamento Europeo y del Consejo, relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial, y la Propuesta de Directiva del Parlamento Europeo y del Consejo, sobre responsabilidad por los daños causados por productos defectuosos*, de septiembre de 2022.

No obstante, el punto de partida en ese objetivo de establecer un marco normativo, lo marca, sin duda, la elaboración por la Comisión de la Unión Europea, en febrero de 2020, del *Libro Blanco sobre la inteligencia artificial—un enfoque europeo orientado a la excelencia y la confianza*¹⁵, al que sigue en abril de 2021, la *Propuesta de Reglamento del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial*, que ha sido aprobado en junio de 2024. Dado el objeto de esta obra, es obligado destacar la importancia de la Directiva 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de preven-

13 V. sobre esta cuestión, «El Consejo de Europa crea un Comité para impulsar la regulación de la Inteligencia artificial» en <https://elconsultor.laley.es>, 13 de septiembre de 2019.

14 Entre otros, cabe también hacer referencia a la Agenda Digital para Europa que, en 2010, reconoce el valor de las tecnologías de la información y la comunicación en el desarrollo de la Unión Europea. En abril de 2018 la Comisión Europea elabora la Comunicación Inteligencia artificial para Europa, y en diciembre del mismo año el Plan coordinado sobre la inteligencia artificial. En abril de 2019, se aprobó la Comunicación Directrices Éticas para una IA fiable que propugna como valores fundamentales para el uso de la inteligencia artificial el cumplimiento de la ley, el respeto a los principios éticos y la solidez.

15 LIBRO BLANCO sobre la inteligencia artificial —un enfoque europeo orientado a la excelencia y la confianza — Publications Office of the EU (europa.eu)

ción, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Obviamente, el estudio que se realiza en este apartado respecto de estos tres documentos normativos no tendrá carácter exhaustivo, ni pretende un análisis pormenorizado de todas las implicaciones que se derivan de su articulado. Se aborda con la intención de reflejar las cuestiones que, desde una perspectiva de su aplicación en la investigación penal, pueden resultar más relevantes.

1.1. El Libro Blanco sobre la Inteligencia Artificial

Como ya se ha apuntado, el punto de partida para una futura regulación marco sobre la Inteligencia artificial, se sitúa en la elaboración por la Comisión europea en febrero de 2020, del *Libro Blanco sobre la inteligencia artificial. Un enfoque europeo orientado a la excelencia y la confianza*¹⁶. Con este documento se pretende realizar una amplia consulta a la sociedad civil, la industria y el mundo académico de los Estados miembros, para que ofrezcan propuestas concretas en torno a un enfoque europeo de la IA. El análisis de dichas propuestas servirá de referencia a la Comisión en sus siguientes líneas de actuación.

La Comisión Europea parte de un hecho incuestionable, como es el constante progreso tecnológico en el campo de la computación, y la gran disponibilidad de datos en la sociedad actual. Atendiendo a ello, considera la gran oportunidad para Europa al establecer «*un marco regulador basado en sus valores fundamentales para convertirse en líder mundial de la innovación en la economía de los datos y sus aplicaciones*». De esta forma, se conseguiría acercar la tecnología a la sociedad y a la economía europea, proporcionando grandes ventajas a los ciudadanos, a las empresas, a los servicios públicos, etc.

El objetivo del Libro Blanco sobre la Inteligencia Artificial, tal y como expresamente se recoge, es «*...facilitar un desarrollo de la inteligencia artificial seguro y fiable en Europa, que respete plenamente los valores y los derechos de los ciudadanos de la UE*». Para ello, describe los pilares fundamentales en torno a los cuales se ha de desarrollar la implantación de los sistemas inteligentes:

El primero pretende promover un «ecosistema de excelencia», generando un marco político en el que se promueva la investigación y la innovación que permita a las empresas utilizar soluciones basadas en IA. De esta forma, las líneas de actuación se centran en la colaboración con los Estados miembros

16 LIBRO BLANCO sobre la inteligencia artificial — un enfoque europeo orientado a la excelencia y la confianza — Publications Office of the EU (europa.eu)

en áreas como la inversión y la investigación, en la potenciación de los centros de investigación, en la ampliación del conocimiento de la IA y de la formación de los trabajadores, en la orientación de las pequeñas y medianas empresas, en la colaboración del sector privado, y en la implantación de la IA en el sector público¹⁷.

El segundo pilar trata de crear un «ecosistema de confianza», a través de un marco normativo que vele por el cumplimiento de las normas de la UE, especialmente las relativas a la protección de los derechos fundamentales, y los derechos de los consumidores. Como recoge el documento en su introducción *«...este marco debe velar por el cumplimiento de las normas de la UE, especialmente las normas de protección de los derechos fundamentales y los derechos de los consumidores, y en concreto con relación a los sistemas de inteligencia artificial que operan en la UE y presentan un riesgo elevado. La Comisión respalda firmemente un enfoque antropocéntrico»*.

La base de este «ecosistema de confianza» la constituyen las directrices dadas por el grupo de expertos de alto nivel que, en abril de 2019, recoge siete requisitos claves que los sistemas inteligentes han de cumplir para ser confiables: acción y supervisión humanas; solidez técnica y seguridad; gestión de la privacidad y de los datos; transparencia; diversidad, o discriminación y equidad; bienestar social y medioambiental y rendición de cuentas¹⁸.

En el libro Blanco, al lado de las ventajas que ofrecen los sistemas de IA, se hace también referencia a las precauciones a adoptar para evitar los riesgos que su implantación puede generar¹⁹. A este respecto, recoge expresamente que *«Los desarrolladores e implementadores de la inteligencia artificial ya están sujetos a la legislación europea en materia de derechos fundamentales (la protección de datos, la privacidad o la no discriminación, entre otros), protección de los consumidores y normas sobre la seguridad de los productos y responsabilidad civil. Los consumidores esperan el mismo nivel de seguridad y respeto de sus derechos independientemente de si un producto o un sistema está basado en la IA o no. Sin embargo, algunas características especí-*

17 V. más ampliamente, GAMERO CASADO, E., «El enfoque europeo de inteligencia artificial», en *Revista de Derecho Administrativo*, 2021, CDA, 20, págs. 268 a 269.

18 Este grupo de expertos de alto nivel, nombrado en junio de 2018 por la Comisión europea, está compuesto por 52 miembros pertenecientes a diferentes especialidades, procedentes del mundo académico, empresarial y de la sociedad civil. Su misión principal será contribuir a la implementación de la estrategia europea en Inteligencia Artificial, y la elaboración de recomendaciones sobre el futuro desarrollo de políticas relacionadas con la IA, y cuestiones problemáticas sobre aspectos éticos, jurídicos y sociales, incluyendo cuestiones socioeconómicas.

19 La consideración de los sistemas de IA como de riesgo elevado se lleva a cabo atendiendo al sector en el que se aplica. Y en este grupo se incluye el sector público, en el que se integra el Poder Judicial. Otro elemento a tener en cuenta para considerar un sistema como de riesgo elevado es si su aplicación afecta a la seguridad física, o a la esfera jurídica de los ciudadanos. V. en este sentido Libro Blanco de IA, págs. 21 y ss.

ficas de la IA (como la opacidad) pueden hacer que la aplicación y ejecución de la legislación sea más compleja. Por esta razón, resulta necesario analizar si la legislación actual puede hacer frente a los riesgos de la IA y si su observancia es factible o si, por el contrario, es necesario adaptarla o se requiere nueva legislación»²⁰.

Se desprende ya de estas afirmaciones la preocupación de la Comisión por la implantación y utilización de los sistemas de IA, pretendiendo analizar si la legislación vigente es suficiente para garantizar el respeto de los derechos de los ciudadanos, o si, por el contrario, resulta necesario revisar el marco normativo con la finalidad de perfilar las garantías que permitan controlar la aplicación de los sistemas «inteligentes»²¹.

Considerando la trascendencia que supone la utilización de estos sistemas en el marco de la economía, en el desarrollo empresarial, en las relaciones comerciales y personales, en las instituciones y servicios públicos, y, en general en la vida de la sociedad actual, la Comisión *«ofrece alternativas políticas para facilitar un desarrollo de la inteligencia artificial seguro y fiable en Europa, que respete plenamente los valores y los derechos de los ciudadanos de la UE»²².*

Resulta obvio que la aplicación de los sistemas de Inteligencia Artificial se encuentra estrechamente vinculada a la obtención y el tratamiento de datos, poniendo ya de relieve la Comisión europea, como uno de los elementos fundamentales para el funcionamiento de las herramientas de IA, es la gran disponibilidad actual de datos, que resulta imprescindible en la utilización de la IA. De esta forma, señala, que los avances en computación y la creciente disponibilidad de datos son un motor fundamental en el pronunciado crecimiento actual de la inteligencia artificial.

Partiendo pues de estas afirmaciones sobre la relación entre la inteligencia artificial y el análisis de una gran cantidad de datos, la Comisión articula la implantación y desarrollo de la Inteligencia artificial vinculándola con la denominada «Estrategia Europea de Datos»²³. Es determinante en su fun-

20 Sobre el Libro Blanco de IA, ver más ampliamente DE HOYOS SANCHO, M., «Premisas y finalidades del Libro Blanco sobre Inteligencia Artificial de la Comisión Europea: perspectiva procesal del nuevo marco regulador», en *Justicia algorítmica y Neuroderecho. Una mirada interdisciplinar* (Barona Vilar, dir.), Tirant lo Blanch, Valencia, 2021, págs., 129 y ss. SCHUMANN BARRAGÁN, G., «La inteligencia artificial aplicada al proceso penal» en *Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos* (Pereira Puigvert/Ordóñez Ponz, dirs.), Aranzadi, Cizur Menor, 2021, págs. 517 a 539.

21 V. ESPARZA LEIBA, I., «La Inteligencia Artificial y el derecho fundamental a la protección de datos de carácter personal», en *Justicia algorítmica y Neuroderecho*, op. cit. pág. 277.

22 V. más ampliamente BARONA VILAR, S., *Algoritmización del derecho y de la justicia*, op. cit., págs. 148 y ss.

23 La Estrategia Europea de Datos busca convertir a la Unión en líder de una sociedad basada en los datos. La creación de un mercado único de datos permitirá que estos fluyan

cionamiento la capacidad de interrelacionar datos, y de obtener patrones de conducta o de comportamiento, en función precisamente del análisis de esos datos²⁴.

Precisamente esta capacidad de interrelación y de interpretación de los datos proporcionados, hace imprescindible promover una regulación clara sobre la aplicación de los sistemas inteligentes, regulación que ha de tener en cuenta la rápida evolución de estos sistemas, diseñando normas detalladas y precisas, pero flexibles, que permitan su aplicación para futuros desarrollos²⁵.

Con el fin de establecer un marco único, en el que se regulen las garantías que permitan controlar la correcta aplicación de los sistemas inteligentes, respetando los principios que informan la legislación europea y las normas por las que se rige, y atendiendo a las directrices del grupo de expertos de alto nivel²⁶, el Libro Blanco recoge una serie de directrices que se pueden agrupar en las siguientes categorías²⁷.

Datos de entrenamiento: si se parte de que los sistemas de IA se nutren de datos, su funcionamiento y aprovechamiento depende en gran medida de la calidad del conjunto de datos suministrados. Deben adoptarse, por tanto, todas las medidas necesarias para garantizar que los datos utilizados respeten los valores y normas de la UE, especialmente en lo que se refiere a la seguridad y protección de derechos fundamentales.

Conservación de registros y datos: teniendo en cuenta la complejidad de algunos sistemas de IA y la opacidad de su funcionamiento y desarrollo, es preciso la regulación de las directrices sobre la conservación de registros que recojan la programación algorítmica, así como los datos utilizado por el sistema. Con ello se facilita el seguimiento y la comprobación de las acciones o decisiones de los sistemas «inteligentes».

libremente por la Unión y de unos sectores a otros, en beneficio de las empresas, el personal investigador y las Administraciones públicas. V. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es

24 SOLAR CAYÓN, J.I., «Inteligencia artificial en la justicia penal: los sistemas algorítmicos» en *Dimensiones éticas y jurídicas de la Inteligencia artificial en el marco del Estado de Derecho*, Cuadernos de la Cátedra de Democracia y Derechos Humanos, 16, Universidad de Alcalá. Defensor del Pueblo, 2020, pág. 130.

25 BARONA VILAR, S., *Algoritmización del derecho y de la justicia...*, op. cit., pág. 193.

26 Este grupo de expertos de alto nivel ha elaborado en abril de 2019 un documento que recoge los criterios que aseguren que los sistemas de IA respetan los derechos fundamentales, la normativa aplicable y los principios básicos de la Unión Europea, y cómo la tecnología puede ser técnicamente robusta y fiable en este contexto. Las recomendaciones del Grupo han servido como guía para la elaboración, entre otros documentos, del Libro Blanco sobre la inteligencia artificial: un enfoque europeo de la excelencia y la confianza.

27 V. más ampliamente BARONA VILAR, S., *Algoritmización del derecho...*, op. cit., págs. 190 a 206.

Suministro de información: partiendo del hecho de que la transparencia en la utilización de los sistemas de IA, constituye la base de la confianza de los usuarios y afectados, es sumamente importante que se informe, tanto sobre el funcionamiento del sistema, como, en su caso, de que se está interactuando con un sistema de este tipo.

Solidez y exactitud: la calificación de un sistema de IA como fiable exige que técnicamente sean sólido, lo que conlleva que su implantación se lleve a cabo de forma responsable, una vez analizados los riesgos que conlleva. Deben, por tanto, adoptarse las medidas necesarias para reducir los riesgos y los posibles daños.

Supervisión humana: la supervisión humana de los sistemas de IA tiene como finalidad controlar su correcto funcionamiento, y evitar aquellos efectos no deseados. Para ello resulta imprescindible que se valide su puesta en funcionamiento y se garantice su intervención en tiempo real, facilitando incluso la interrupción del sistema en caso necesario.

Atendiendo a la responsabilidad y trascendencia que implica el tratamiento de los datos personales más sensibles, y su repercusión en derechos como la libertad, o la vida privada de las personas, al igual que en los derechos fundamentales de naturaleza procesal, el Libro Blanco dedica un apartado específico a los sistemas de identificación biométrica remota²⁸. A este respecto, la Comisión considera que sólo podrán utilizarse este tipo de sistemas cuando su uso «*esté debidamente justificado, sea proporcionado y esté sujeto a garantías adecuadas*». Para ello, deberán abordarse las posibles circunstancias o hechos que pueden justificar su utilización, así como las garantías comunes para su protección.

Tal y como se ha señalado, la Comisión Europea es consciente, tanto de las ventajas que proporciona la aplicación de los sistemas de IA en los distintos ámbitos y sectores económicos, jurídicos y sociales, como de los riesgos que conlleva. En este sentido, el propio documento hace referencia a los principales riesgos relacionados con el uso de la inteligencia artificial, que afectan, de un lado, a la aplicación de las normas diseñadas para proteger los derechos fundamentales y, de otro, a la seguridad, así como a las cuestiones relativas a la responsabilidad civil²⁹.

En relación con los derechos fundamentales, pone de relieve el documento, que la privacidad y obviamente la protección de los datos personales, se pondría en riesgo por la utilización de la IA, lo que hará necesario establecer límites concretos y garantías específicas que permitan una tutela clara y

28 Aunque estos sistemas serán objeto de estudio en apartados posteriores, ya ha se precisarse que se trata de sistemas de IA destinados a identificar a personas físicas sin su participación o consentimiento, por lo que se trata de un sistema de identificación a distancia en el que se comparan sus datos biométricos con los que figuran en una base de datos.

29 V. Libro Blanco sobre Inteligencia artificial... op. cit., pág. 13.

transparente. Derechos como la libertad de expresión, la libertad de reunión, la dignidad humana, la ausencia de discriminación por razón de sexo, raza u origen étnico, religión o credo, discapacidad, edad u orientación sexual y, en su aplicación en determinados ámbitos, la protección de los datos personales y de la vida privada, el derecho a una tutela judicial efectiva y a un juicio justo, o la protección de los consumidores, constituyen pilares fundamentales sobre los que se asientan el Derecho de la Unión, por lo que la incidencia en su esfera habrá de rodearse de los requisitos de control necesarios³⁰.

Como puede comprobarse entre los derechos fundamentales que pueden verse afectados por una utilización incorrecta de los instrumentos de inteligencia artificial, se encuentran derechos relacionados con el proceso penal, que tienen su aplicación en la fase de investigación y enjuiciamiento. Los derechos relacionados con la vida privada, como el derecho a la intimidad, el derecho al secreto de las comunicaciones y el derecho a la protección de datos y al entorno virtual, pueden verse afectados gravemente por la utilización de herramientas de inteligencia artificial en la fase de investigación del hecho delictivo. De igual forma, el derecho a la tutela judicial efectiva y el derecho a un proceso justo, que no puede hacerse efectivo sin el respeto al derecho de defensa y a la presunción de inocencia, también pueden resultar conculcados por un uso sin control de los sistemas inteligentes.

Las deficiencias en los tratamientos de datos que pueden derivar del incumplimiento de la normativa reguladora, de una mala utilización de los programas con la introducción de datos sesgados, de un diseño o funcionamiento defectuoso del sistema, o incluso del desconocimiento sobre su funcionamiento como consecuencia del autoaprendizaje (sistemas de inteligencia artificial basados en deep learning, redes neuronales y los llamados algoritmos de caja negra o black-box), aconsejan que la supervisión e intervención humana se convierta en el garante último de un correcto funcionamiento³¹.

Similares problemas pueden afectar a los sistemas de inteligencia artificial desde una perspectiva de la seguridad, lo que hará necesario arbitrar normas específicas en las que se regulen los mecanismos de control que permitan el uso seguro y fiable de estas herramientas, y mucho más si se tiene en cuenta que la evolución de los instrumentos de inteligencia artificial es imparable, lo que va a requerir una especial vigilancia. En este sentido, la Comisión señala, en el Libro Blanco, que las autoridades pueden encontrarse en situaciones en las que resulte confuso no solo intervenir, sino también decidir la forma de intervención más adecuada, lo que va a repercutir en la seguridad.

30 BARONA VILAR, S., *Algoritmización del derecho y de la justicia...*, op. cit., pág. 197.

31 SERRANO ACITORES, A., «Consideraciones éticas y legales en el uso de la inteligencia artificial: el enfoque de la unión europea», en *Revista de Fiscalidad Internacional y Negocios Transnacionales*, número 24, 2023, <https://soluciones-aranzadilale-y-es.ezbusc.usc.gal/Content/Documento.aspx>. pág. 10

1.2. El Reglamento Europeo de Inteligencia Artificial y su influencia en la investigación penal

En junio de 2024 se ha publicado el tan esperado Reglamento Europeo de IA (REIA), o con más precisión 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. El artículo 113 REIA contempla el plazo de entrada en vigor, y además prevé un proceso de aplicación en diferentes fases. Como regla general el citado artículo establece su entrada en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea (12 de julio de 2024), esto es, el 1 de agosto de 2024, aunque realmente su aplicación completa se pospondrá hasta el 2 de agosto de 2026.

No obstante, se recogen varias excepciones. Algunas de ellas prevén una aplicación anticipada a la fecha general, al establecer que los capítulos I y II se aplicarán a partir del 2 de febrero de 2025. Haciendo referencia a su contenido, el Capítulo I regula las disposiciones generales, divididas en cuatro artículos. El artículo 1 se refiere al objeto del Reglamento, el artículo 2 a su ámbito de aplicación, el artículo 3 a las definiciones relacionadas con la normativa IA, y el artículo 4 a la alfabetización en materia de inteligencia artificial. En cuanto al Capítulo II, se establecen en un único precepto, el artículo 5, las prácticas de inteligencia artificial prohibidas.

El Reglamento dispone la aplicación diferida de varios de sus preceptos. Así pospone al 2 de agosto de 2025 los siguientes capítulos: la sección 4 del Capítulo III sobre las autoridades notificantes y organismos notificados; el Capítulo V, que recoge los modelos de inteligencia artificial de uso general; el Capítulo VII, en el que se regula la gobernanza; el Capítulo XII, en el que se establecen las sanciones, con la excepción del artículo 101, que prevé las multas a proveedores de modelos de IA de uso general, y, finalmente el artículo 78, que regula la confidencialidad, y que se integra en la sección 3 del Capítulo IX.

Otra de las excepciones a la aplicación del Reglamento en agosto de 2026, es la prevista en el primer apartado del artículo 6, que regula las condiciones para considerar un sistema de inteligencia artificial como sistema de alto riesgo. Esta disposición se aplicará a partir del 2 de agosto de 2027, al igual que las obligaciones derivadas del Reglamento.

Esta entrada en vigor escalonada obedece a la complejidad y ámbito de esta normativa, y a la necesidad de proporcionar a todos los agentes afectados, que son muy variados, un margen temporal adecuado para adaptarse a las previsiones del reglamento, garantizado de esta forma la seguridad jurídica. No obstante, teniendo en cuenta la protección de los derechos y valores de la Unión Europea, el Reglamento anticipa la aplicación de algunas obligaciones. En este sentido, el considerando 179 señala que «*teniendo en*

cuenta el riesgo inaceptable asociado a determinadas formas de uso de la IA, las prohibiciones, así como las disposiciones generales del presente Reglamento, deben aplicarse ya desde el 2 de febrero de 2025»³².

El Reglamento, también conocido como Ley de Inteligencia artificial, constituye la primera regulación general a nivel mundial de la materia, y va a condicionar el desarrollo económico y social durante los próximos años. Se enmarca en la Estrategia europea sobre IA, que se inicia por parte de la Comisión europea en abril de 2018. Como ya se ha puesto de relieve, se propone que la aplicación de la inteligencia artificial se lleve a cabo desde un enfoque que coloque a la persona en el centro de su desarrollo, impulsando el uso de esta alta tecnología para resolver desafíos y problemas relacionados con la salud, la seguridad, la lucha contra la delincuencia, etc. Esta estrategia apoya una IA ética, segura y vanguardista, que se asienta sobre tres pilares: aumentar las inversiones públicas y privadas en IA, prepararse para los cambios socioeconómicos, y garantizar un marco ético y legal adecuado. Se trata de asegurar que, en el marco de la Unión Europea, los recursos derivados de la inteligencia artificial se centren en el ser humano, defendiendo una IA sostenible, segura, inclusiva y fiable, que garantice el respeto a los derechos fundamentales, la democracia, el Estado de Derecho y la sostenibilidad medioambiental. Al mismo tiempo, el Reglamento IA tiene por objetivo impulsar la innovación y establecer a la UE como líder en el campo de la IA, actuando como un catalizador de la industria³³.

En este sentido, el considerando número cuatro del REIA, pone de relieve las múltiples aplicaciones de los sistemas de inteligencia artificial, reseñando los beneficios económicos, sociales, asistenciales y de desarrollo, entre otros. Señala expresamente que *«la IA es un conjunto de tecnologías en rápida evolución que contribuye a generar beneficios económicos, medioambientales y sociales muy diversos en todos los sectores económicos y las actividades sociales. El uso de la IA puede proporcionar ventajas competitivas esenciales a las empresas y facilitar la obtención de resultados positivos desde el punto de vista social y medioambiental en los ámbitos de la asistencia sanitaria, la agricultura, la seguridad alimentaria, la educación y la formación, los medios de comunicación, el deporte, la cultura, la gestión de infraestructuras, la energía, el transporte y la logística, los servicios públicos, la seguridad, la justicia, la eficiencia de los recursos y la energía, el seguimiento ambiental, la conservación y restauración de la biodiversidad y los ecosistemas, y*

32 V. CAMPOS ACUÑA, C., «El Reglamento de Inteligencia Artificial ya está funcionando: a quién afecta, plazos y sanciones» en *Noticias Jurídicas. Actualidad noticias*, 3 de febrero de 2025, <https://noticias.juridicas.com/actualidad/noticias/19904-el-reglamento-de-inteligencia-artificial-ya-esta-funcionando>.

33 Sobre la importancia y el contenido del REIA se puede consultar, entre otros, BARRIO ANDRÉS, M., (dir.) *El Reglamento Europeo de Inteligencia Artificial*, Tirant lo Blanch, Valencia, 2024; dirigido por el mismo autor, *Comentarios al Reglamento europeo de Inteligencia artificial*, Editorial La Ley, Madrid, 2024.

la mitigación del cambio climático y la adaptación a él, entre otros, al mejorar la predicción, optimizar las operaciones y la asignación de los recursos, y personalizar las soluciones digitales que se encuentran a disposición de la población y las organizaciones».

Para apuntar a continuación, el objetivo de la regulación aprobada, que se centra en «...mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme, en particular para el desarrollo, la introducción en el mercado, la puesta en servicio y la utilización de sistemas de inteligencia artificial (en lo sucesivo, «sistemas de IA») en la Unión, de conformidad con los valores de la Unión, a fin de promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, proteger frente a los efectos perjudiciales de los sistemas de IA en la Unión, así como brindar apoyo a la innovación».

La premisa de la que parte el Reglamento, en cuanto a la aplicación de la IA y el objetivo que persigue, pone ya de relieve, desde un principio, la extrema complejidad de la norma. En un mismo cuerpo legal se establecen normas relativas a la comercialización y puesta en servicio de productos y sistemas de inteligencia artificial, y normas que pretenden la protección de los derechos fundamentales de las personas, del Estado de Derecho y de la democracia, regulando las obligaciones que se han de observar en la aplicación de estos sistemas inteligentes. Todo ello unido a la regulación de la responsabilidad de aquellos que vigilan o supervisan el funcionamiento de los sistemas de IA, y de las sanciones por el incumplimiento de los requisitos de su puesta en funcionamiento y de las obligaciones establecidas.

Se pretende la regulación del uso de este tipo de tecnología en sectores concretos, teniendo en cuenta su posible incidencia en los derechos fundamentales, en la salud y en la seguridad. Así se establecen distintos niveles de riesgo y, en función de esta clasificación, se fijan una serie de requisitos y obligaciones, regulando también la prohibición del uso de determinados sistemas cuando el riesgo es inasumible³⁴.

La supervisión del cumplimiento de las normas reguladoras de la aplicación de la inteligencia artificial se encomienda a autoridades de la Unión europea y autoridades nacionales. En la Unión Europea serán la Comisión europea,

34 BARRIO ANDRÉS. M., «Objeto, ámbito de aplicación y sentido del Reglamento Europeo de Inteligencia Artificial» en *El Reglamento Europeo de Inteligencia Artificial* (dirigido por Barrio Andrés), Tirant lo Blanch, Valencia 2024, pág. 33.

el Consejo europeo de IA³⁵ y la Oficina europea de IA³⁶, los encargados de esta función. El primer apartado del artículo 67 REIA prevé la creación de un «...*foro consultivo para proporcionar conocimientos técnicos y asesorar al Consejo de IA y a la Comisión, así como para contribuir a las funciones de estos en virtud del presente Reglamento*»³⁷. También se recoge en el artículo 68 REIA, la creación de un «grupo de expertos científicos independientes» destinado a apoyar las actividades de garantía del cumplimiento previstas en el presente Reglamento.

En cuanto a las autoridades nacionales, tal y como recoge el artículo 70 REIA, cada Estado miembro designará al menos una autoridad notificante, y al menos una autoridad de vigilancia del mercado, como autoridades nacionales competentes a los efectos del presente Reglamento. Dichas autoridades, sujetas al principio de confidencialidad previsto en el artículo 78 REIA, ejercerán sus poderes de manera independiente, imparcial y sin sesgos, a fin de preservar la objetividad de sus actividades y funciones, y de garantizar la aplicación y ejecución del presente Reglamento. Los Estados miembros tienen de plazo hasta el 2 de agosto de 2025 para designar a las autoridades nacionales competentes, que supervisarán la aplicación de las normas aplicables a los sistemas de IA y llevarán a cabo actividades de vigilancia del mercado.

La autoridad española de supervisión es la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA), creada por la disposición adicional séptima de la Ley 28/2022, de 21 de diciembre, de fomento del ecosistema de las empresas emergentes, que la considera como un «...*organismo público con personalidad jurídica pública, patrimonio propio, plena capacidad de obrar y potestades administrativa, inspectora y sancionadora que se le atribuyan en aplicación de la normativa nacional y europea en relación con el uso seguro y confiable de los sistemas de inteligencia artificial*»³⁸.

35 El Consejo europeo de IA se recoge en el artículo 65 del Reglamento y estará compuesto por un representante por cada Estado miembro. El Supervisor europeo de protección de datos y la Oficina de IA también podrá asistir a las reuniones sin participar en las votaciones. El Consejo podrá invitar a autoridades y expertos para que asistan a las reuniones.

36 La Oficina europea de IA, creada en el seno de la Comisión, tiene por objeto el desarrollo y uso de la IA, fomentando los beneficios sociales y económicos y la innovación, mitigando al mismo tiempo los riesgos. El considerando 47 REIA dispone que «la función de la Comisión consistente en contribuir a la implantación, el seguimiento y la supervisión de los sistemas de IA y modelos de IA de uso general, y a la gobernanza de la IA prevista por la Decisión de la Comisión de 24 de enero de 2024; las referencias hechas en el presente Reglamento a la Oficina de IA se entenderán hechas a la Comisión».

37 La Comisión nombrará a los miembros del foro consultivo de acuerdo con lo establecido en el artículo 67.2 REIA. La Agencia de los Derechos Fundamentales de la Unión Europea, la Agencia de la Unión Europea para la Ciberseguridad, el Comité Europeo de Normalización (CEN), el Comité Europeo de Normalización Electrotécnica (Cenelec) y el Instituto Europeo de Normas de Telecomunicaciones (ETSI) serán miembros permanentes del foro consultivo.

38 Su actuación responderá a los siguientes fines:

1.2.1. Clasificación de los sistemas de IA

Partiendo del objetivo de este trabajo, y desde la perspectiva de su aplicación en el sistema de justicia, es necesario examinar la regulación de la IA en el Reglamento, enfocando las prohibiciones, requisitos y garantías reguladas hacia la investigación penal, y teniendo en cuenta las obligaciones que han de cumplirse para que los instrumentos de IA puedan ser utilizados por las autoridades policiales y judiciales en el esclarecimiento de hechos delictivos.

Tomando como primera referencia los considerandos y el texto articulado, se pone de relieve la constante preocupación del legislador europeo por la protección de los derechos fundamentales como la dignidad, la intimidad y el secreto de las comunicaciones, la protección de los datos personales y de la privacidad en general, el derecho a la igualdad, los derechos fundamentales de naturaleza procesal, etc. En este sentido, el considerando 48 REIA señala que *«...la magnitud de las consecuencias adversas de un sistema de IA para los derechos fundamentales protegidos por la Carta es especialmente importante a la hora de clasificar un sistema de IA como de alto riesgo. Entre dichos derechos se incluyen el derecho a la dignidad humana, el respeto de la vida privada y familiar, la protección de datos de carácter personal, la libertad de expresión y de información, la libertad de reunión y de asociación, el derecho a la no discriminación, el derecho a la educación, la protección de los consumidores, los derechos de los trabajadores, los derechos de las personas discapacitadas, la igualdad entre hombres y mujeres, los derechos de propiedad intelectual, el derecho a la tutela judicial efectiva y a un juez imparcial, los derechos de la defensa y la presunción de inocencia, y el derecho a una buena administración»*³⁹.

Dicha preocupación sobre la protección y tutela de los derechos fundamentales es compartida también por la doctrina, que, si bien reconoce las ventajas que estos sistemas suponen para el sistema de justicia, también

a) La concienciación, divulgación y promoción de la formación y del desarrollo, y del uso responsable, sostenible y confiable de la inteligencia artificial.

b) La definición de mecanismos de asesoramiento y atención a la sociedad, y a otros actores relacionados con el desarrollo y uso de la inteligencia artificial.

c) La colaboración y coordinación con otras autoridades, nacionales y supranacionales, de supervisión de inteligencia artificial.

d) El fomento de entornos reales de prueba de los sistemas de inteligencia artificial, para reforzar la protección de los usuarios.

e) La supervisión de la puesta en marcha, uso o comercialización de sistemas que incluyan inteligencia artificial y, especialmente, aquellos que puedan suponer riesgos significativos para la salud, seguridad y los derechos fundamentales.

39 En este mismo considerando se hace especial referencia a la especial protección de los menores con una mención específica del artículo 24 de la Carta y en la Convención sobre los Derechos del Niño de las Naciones Unidas, y su desarrollo en la observación general n.º 25 de la Convención sobre los Derechos del Niño de Naciones Unidas relativa a los derechos de los niños en relación con el entorno digital.

advierte de los peligros de una utilización inadecuada y de los riesgos que conllevan, y más concretamente para el derecho a la tutela judicial efectiva y a un juez imparcial, los derechos de la defensa y la presunción de inocencia, mencionados expresamente en el considerando 48 REIA⁴⁰.

Precisamente, el peligro de la utilización de los sistemas de IA motiva su clasificación atendiendo al riesgo que ocasionan, determinando una mayor o menor exigencia de requisitos para su aplicación y de garantías en su protección⁴¹.

En primer lugar, en su artículo 5, el Reglamento hace referencia a los **sistemas de riesgo inaceptable o sistemas prohibidos**⁴². Se trata de una serie de sistemas de IA, listados de forma tasada y periódicamente revisados, cuyo uso estaría prohibido por implicar un riesgo inadmisible para la seguridad, la vida y los derechos fundamentales. En esta categoría se integran aquellas aplicaciones de IA que permiten la clasificación de las personas en función de su comportamiento o características personales, cuando induzcan a discriminación⁴³. Este tipo de aplicaciones pueden afectar a la dignidad de la persona, a la justicia o a la igualdad.

40 BARONA VILAR, S., Algoritmización del derecho y de la justicia, *op. cit.*, págs. 25 y ss.; COLOMER HERNÁNDEZ, I., «Control y límites en el uso de la información y los datos personales por parte de la Inteligencia artificial en los procesos penales», en *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar* (Barona Vilar, editora). Tirant lo Blanch, Valencia, 2021, pág. 293; ESPARZA LEIBAR, I., «Derecho fundamental a la protección de datos de carácter personal en el ámbito jurisdiccional e inteligencia artificial. En especial la LO 7/2021, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales», en *Inteligencia artificial legal y Administración de justicia* (Calaza López y Llorente Sánchez-Arjona, dirs.), Aranzadi, Cizur Menor (Navarra), 2022, pág. 188; GÓMEZ COLOMER, J.L., «Derechos fundamentales, proceso e Inteligencia Artificial: una reflexión» en *Inteligencia artificial legal y Administración de justicia, op. cit.*, pág. 259. GUZMÁN FLUJA, V., «Arbitraje y soluciones técnicas inteligentes: elementos para un debate», en *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar...*, *op. cit.*, págs. 553 y ss.; MARTÍN DÍZ, F., «Herramientas de inteligencia artificial y adecuación en el ámbito del proceso judicial», en *Derecho Procesal. Retos y transformaciones*, Atelier y Fundación Serra Domínguez, Barcelona, 2021, págs. 298-299; MORENO CATENA, V., «Los datos en el sistema de justicia y la propuesta de reglamento UE sobre Inteligencia artificial» en *Uso de la información y de los datos personales en los procesos: los cambios de la era digital*, (Colomer Hernández, dir.), Aranzadi, Cizur Menor, 2022, pág. 48, entre otros.

41 V. en este sentido, BUENO DE MATA, F., «Protección de datos, investigación de infracciones penales e inteligencia artificial: novedades y desafíos a nivel nacional y europeo en la era postcovid» en *La Ley Penal*, número 150, , mayo-junio 2021, *La Ley Digital*, de 25 de enero de 2022, pág. 10.

42 V. más ampliamente MÍGUEZ MACHO, L./MARCOS TORRES, C., «Sistemas de IA prohibidos y sistemas de IA de alto riesgo» en *El Reglamento Europeo de Inteligencia Artificial* (Barrio Andrés, dir.), *op. cit.*, págs. 49-85.

43 Esta previsión se corresponde con los sistemas prohibidos del artículo 11 de la Directiva de 2016, que hacía referencia a las categorías especiales de datos.

Recoge expresamente el Reglamento, en su considerando 31, que *«la puntuación ciudadana resultante de dichos sistemas de IA puede dar lugar a un trato perjudicial o desfavorable de determinadas personas físicas o colectivos enteros en contextos sociales que no guardan relación con el contexto donde se generaron o recabaron los datos originalmente, o a un trato perjudicial desproporcionado o injustificado en relación con la gravedad de su comportamiento social. Por lo tanto, deben prohibirse los sistemas de IA que impliquen esas prácticas inaceptables de puntuación y den lugar a esos resultados perjudiciales o desfavorables»*

También se integrarían en este grupo, aquellos instrumentos que permiten manipular la voluntad y el comportamiento humano, de modo que puedan provocar perjuicios físicos o psicológicos, y los sistemas de identificación biométrica en tiempo real en lugares de acceso público con la finalidad de aplicación de la ley, con las excepciones recogidas en el precepto, que serán objeto de tratamiento posterior⁴⁴.

Desde la perspectiva de la aplicación de los sistemas inteligentes en la investigación y enjuiciamiento penal, resulta de especial importancia la inclusión entre los instrumentos prohibidos, o de riesgo inaceptable, de algunas aplicaciones.

El precepto citado hace referencia expresa a la *«la introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA para evaluar o clasificar a personas físicas o a colectivos de personas durante un período determinado de tiempo atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante provoque una o varias de las situaciones siguientes:*

- i) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente,*
- ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este».*

44 Conforme a lo previsto en el apartado 34, del artículo 3 del Reglamento, se entienden por datos biométricos, los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Los sistemas de identificación biométrica, tal y como recoge el Reglamento en el apartado 35 del artículo 3, son sistemas de IA destinados al «reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos». En este tipo de identificación el usuario del sistema desconoce si la persona se encuentra en la base de datos del sistema.

Y todavía más concretamente a *«la introducción en el mercado, la puesta en servicio para este fin específico o el uso de un sistema de IA para realizar evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de que una persona física cometa un delito basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad; esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva»*.

Parece que el Reglamento diferencia claramente entre la elaboración de «perfiles» de una persona, o grupos de personas, cuando no son objeto de una investigación concreta y determinada, de aquella otra que se enmarca en una investigación delictiva en la que ya constan *hechos objetivos y verificables directamente relacionados con una actividad*⁴⁵. Si esto es así, se está aludiendo a la existencia de un proceso penal en curso y a la adopción de determinadas diligencias de investigación bajo el paraguas supervisor de una autoridad judicial.

Especial mención requiere la regulación que el Reglamento establece en relación con los sistemas de identificación biométrica, previstos como sistemas prohibidos en el citado artículo 5, apartado h. Se refiere el REIA a los sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho⁴⁶. Inicialmente se considera como un sistema prohibido, salvo que su uso resulte estrictamente necesario para los fines que se mencionan en el propio precepto, y de acuerdo con los requisitos y garantías dispuestos en los apartados dos, tres y cinco del citado artículo 5⁴⁷.

Resulta evidente la importancia que tiene en la investigación delictiva la identificación de aquellas personas que pueden resultar sospechosas de la comisión de hechos delictivos. Que los rasgos físicos o fisiológicos puedan ser tratados por sistemas de IA a través de la utilización de un tratamiento algorítmico, es un avance trascendental para el éxito de la investigación.

45 V. ESCAJEDO SAN-EPIFANIO, L., «El reconocimiento biométrico en el Reglamento de inteligencia artificial: exenciones, prohibiciones y especialidades de alto riesgo», en Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea (Cotino Hueso/Simón Castellano, dirs.), Aranzadi, Madrid, 2024, pág. 212.

46 En el artículo 1 se recoge la definición número 46, que señala lo que ha de entenderse por «garantía del cumplimiento del Derecho» desde la perspectiva del REIA, estableciendo que comprenden «las actividades realizadas por las autoridades garantes del cumplimiento del Derecho, o en su nombre, para la prevención, la investigación, la detección o el enjuiciamiento de delitos o la ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas».

47 V. más ampliamente, ESCAJEDO SAN-EPIFANIO, L., «El reconocimiento biométrico en el Reglamento de inteligencia artificial: exenciones, prohibiciones y especialidades de alto riesgo», en Tratado sobre el Reglamento..., *op. cit.*, págs. 183 y ss.

No obstante, no cabe duda que la utilización de este tipo de datos y su tratamiento mediante el cruce de algoritmos, debe sujetarse a un estricto control judicial, limitando su aplicación en función de los tipos delictivos y con sujeción al principio de proporcionalidad⁴⁸. La injerencia en la vida privada de los ciudadanos, en su intimidad, e incluso en su libertad de movimientos, conlleva que la utilización de este tipo de instrumentos se declaren prohibida con carácter general, aunque, como veremos, puedan ser utilizados excepcionalmente⁴⁹.

Si bien se parte de la especial sensibilidad de los datos biométricos, también resulta claro que su uso es imprescindible para proceder a la identificación biométrica, definida en el considerando 15, como *«el reconocimiento automatizado de características humanas de tipo físico, fisiológico o conductual, como la cara, el movimiento ocular, la forma del cuerpo, la voz, la entonación, el modo de andar, la postura, la frecuencia cardíaca, la presión arterial, el olor o las características de las pulsaciones de tecla, a fin de determinar la identidad de una persona comparando sus datos biométricos con los datos biométricos de personas almacenados en un base de datos de referencia, independientemente de que la persona haya dado o no su consentimiento»*. Y diferencia la identificación biométrica de la «verificación biométrica», que define como el proceso de autenticación *«...cuyo único propósito es confirmar que una persona física concreta es la persona que dice ser, así como la identidad de una persona física con la finalidad exclusiva de que tenga acceso a un servicio, desbloquee un dispositivo o tenga acceso de seguridad a un local»*.

Dentro de la identificación biométrica, distingue entre identificación biométrica remota, e identificación biométrica real. En la primera categoría se incluyen aquellos sistemas de IA destinados a identificar a personas físicas sin su participación o consentimiento, por lo que se trata de un sistema de identificación a distancia en el que se comparan sus datos biométricos con los que figuran en una base de datos. Por el contrario, en los sistemas identificación biométrica real, o en tiempo real, la recogida de los datos biométricos, su comparación y la identificación que se pretende, se llevan a cabo de forma instantánea, sin una demora importante. Para ello se pueden utilizar grabaciones en video, o las obtenidas de una cámara.

En relación con el uso de estos sistemas en espacios públicos con fines de garantía en el cumplimiento de la ley⁵⁰, considera el Reglamento, en su con-

48 V. en este sentido ETXEBERRÍA GURIDI, J.F. «El uso de sistemas de inteligencia artificial (IA) de identificación biométrica remota en espacios públicos en la ley europea de IA» en *Actualidad Jurídica Iberoamericana*, número 21, agosto 2024, pág. 531.

49 V. IGLESIAS CANLE, I., «Registros biométricos y su aplicación al proceso penal en España e Italia», en *Inteligencia artificial legal y Administración de Justicia*, op. cit., pág. 348.

50 El REIA en su artículo 3, punto 44, define lo que ha de entenderse por espacio acceso público a efectos de la aplicación del Reglamento, considerándolo como «...cualquier

siderando 32, que invade gravemente derechos fundamentales como la vida privada, dando lugar a una sospecha de vigilancia constante por parte de los poderes públicos, lo que puede llevar a los ciudadanos a no ejercer con libertad otros derechos como el derecho de reunión. Además, los posibles sesgos que pueden derivarse de la aplicación de estos sistemas, y el resultado que ocasionan, generan un riesgo difícil de asumir, y más cuando no se pueden realizar comprobaciones inmediatas que puedan descartar el resultado ofrecido por la IA.

La gravedad de la injerencia es evidente, se trata de una identificación en tiempo real de personas que se encuentran en lugares públicos, sin diferenciar si se trata de sospechosos de la comisión de hechos delictivos o no. No se puede obviar en este punto, que, aún en espacios públicos, los derechos integrados en la vida privada han de protegerse⁵¹. Consecuencia de ello, es que el propio Reglamento prohíbe su utilización, salvo situaciones excepcionales que compense el riesgo que suponen, situaciones especialmente previstas en el propio Reglamento que, como ya se ha apuntado, se tratarán en páginas posteriores.

Continuando con la clasificación que realiza el Reglamento, relativa a la aplicación de los sistemas de IA en función del riesgo que generan, el segundo nivel lo integran los denominados **sistemas de alto riesgo**. Se integran en esta categoría otros sistemas de IA, que, si bien no están prohibidos, suponen un «alto riesgo» para los derechos y libertades de los individuos y, por consiguiente, deben estar sujetos a ciertas obligaciones reforzadas que garanticen su uso legal y ético.

El Reglamento los recoge en el primer apartado del artículo 6, haciendo referencia a una serie de sistemas destinados a ser utilizados, bien como componentes de seguridad de un producto de los recogidos en el anexo I⁵², o bien que el propio sistema sea uno de esos productos, siempre que deban someterse a una evaluación de conformidad por terceros para su introducción en el mercado, conforme a lo previsto en ese anexo I.

El segundo apartado del precepto se remite al anexo III, para considerar los sistemas que se relacionan como de alto riesgo, que se regulan atendiendo a su finalidad. Por lo que interesa a este estudio, han de mencionarse necesariamente los sistemas relacionados con la biometría, los sistemas relaciona-

lugar físico, de propiedad privada o pública, al que pueda acceder un número indeterminado de personas físicas, con independencia de que deban cumplirse determinadas condiciones de acceso y con independencia de las posibles restricciones de capacidad».

51 ETXEBERRIA GURIDI, J.F. «El uso de sistemas de inteligencia artificial (IA)...» *op. cit.*, pág. 546.

52 En el citado anexo I se agrupa la legislación armonizada que da cobertura la regulación de una serie de materias como la seguridad de los juguetes, de los ascensores, productos sanitarios, motos acuáticas, aviación civil, etc.

dos con la garantía del cumplimiento del Derecho y los sistemas relacionados con la Administración de justicia⁵³.

Como puede comprobarse los sistemas recogidos en el anexo III son utilizados habitualmente por la policía en sus funciones de investigación criminal, o incluso en sus funciones a prevención. Se catalogan como sistemas relacionados con la garantía del cumplimiento del Derecho, y se establece como primera condición para su uso, que se permita por el Derecho de la Unión, y por el Derecho del Estado miembro en el que se pretenda aplicar:

- a) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho, para evaluar el riesgo de que una persona física sea víctima de delitos.
- b) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho, como polígrafos o herramientas similares
- c) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho, para evaluar la fiabilidad de las pruebas durante la investigación o el enjuiciamiento de delitos
- d) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho, para evaluar el riesgo de que una persona física cometa un delito, o reincida en la comisión de un delito, atendiendo no solo a la elaboración de perfiles de personas físicas mencionada en el artículo 3, punto 4, de la Directiva (UE) 2016/680, o para evaluar rasgos y características de la personalidad o comportamientos delictivos pasados de personas físicas o colectivos.
- e) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho, para elaborar perfiles de personas físicas, como se menciona en el artículo 3, punto 4, de

53 Sobre esta cuestión, ver más ampliamente DE HOYOS SANCHO, M., «El proyecto de Reglamento de la Unión Europea sobre inteligencia artificial, los sistemas de alto riesgo y la creación de un ecosistema de confianza» en *Justicia poliédrica en periodo de mudanza: Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad* (Barona Vilar (edit), 2022, págs. 411 y ss.

la Directiva (UE) 2016/680, durante la detección, la investigación o el enjuiciamiento de delitos. Además, también se consideran de algo riesgo, los sistemas de IA destinados a ayudar a una autoridad judicial en la investigación e interpretación de hechos y de la ley, así como en la aplicación de la ley a un conjunto concreto de hechos, tal y como se recoge en el apartado 8 del citado anexo III.

De conformidad con el artículo 7.1 REIA, esta relación de sistemas podrá ampliarse con otros nuevos que conlleven un riesgo para la salud o la seguridad, o puedan afectar negativamente a los derechos fundamentales, siempre que la gravedad o la probabilidad del riesgo de causar perjuicios resulten equivalentes a los ya previstos.

En cuanto a los sistemas relacionados con la Administración de Justicia y los procesos democráticos previstos en el apartado 8 del Anexo III, se encuentran aquellos que están destinados a ayudar a una autoridad judicial en la investigación y en la interpretación de la ley, así como en su aplicación.

Continuando con la clasificación recogida en el Reglamento, se distinguen también, en función del riesgo que pueden generar:

Sistemas de IA de riesgo medio/bajo, que no suponen un alto riesgo para los derechos y libertades, en los que se incluyen determinadas tecnologías de menor sofisticación o capacidad de intrusión, tales como asistentes virtuales como chatbots, y finalmente el **resto de sistemas de IA**, que, en principio, no estarían sujetos a ninguna obligación en particular, pudiendo los agentes de la cadena elegir si desean adherirse a sistemas voluntarios de cumplimiento. Por consiguiente, estos sistemas quedarían, en principio, fuera del ámbito de aplicación del Reglamento.

La regulación reglamentaria evidencia que la valoración del riesgo alto de un sistema no impide su utilización, siempre que se someta a los requisitos exigidos y a las garantías reguladas para proteger los derechos y libertades fundamentales, el Estado de Derecho, la Administración de Justicia y los procesos democráticos. En función de ello, se regula también en el artículo 9 REIA, la implantación de un sistema de gestión de riesgos asociado a la aplicación de IA, que abarcará todo el ciclo de vida, requiriendo actualizaciones sistemáticas y periódicas. Además, estos sistemas se someterán a las pruebas necesarias para identificar cuáles son las medidas de gestión de riesgos más adecuadas.

1.2.2. Garantías para el uso de los sistemas de IA del alto riesgo

No cabe duda de que los sistemas que se integran en la categoría de alto riesgo podrán utilizarse en la investigación penal, aunque han de someterse a la estricta observancia de las garantías previstas en protección de los derechos y libertades de los ciudadanos. Al resultar imposible abordar en este trabajo todos aquellos sistemas que pueden integrarse en esta categoría,

se realizará el estudio de las garantías en relación a aquellos que suponen un peligro de mayor intensidad. Se trata de los sistemas de identificación biométrica con fines de garantía del cumplimiento del Derecho, que, a pesar de considerarse inicialmente como sistemas prohibidos, el artículo 5 REIA permite su utilización cuando son autorizados por las normas de un Estado miembro, y de acuerdo con la excepcionalidad prevista en la letra h) del primer apartado del precepto.

De esta forma, se autoriza la utilización de estos sistemas siempre condicionada a que esta medida resulte estrictamente necesaria, lo que va a exigir la aplicación del juicio de proporcionalidad, y que se destine a uno de estos objetivos:

1. La búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos, o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas. Se trata en los tres casos de la localización de víctimas de hechos delictivos o de personas desaparecidas.
2. La prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas, o de una amenaza real y actual o real y previsible de un atentado terrorista.
3. La localización o identificación de una persona sospechosa de haber cometido un delito, a fin de llevar a cabo una investigación o un enjuiciamiento penales, o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II, que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

Precisa el REIA, respecto de la excepción prevista en el número 2, que «... una amenaza inminente para la vida o la seguridad física de las personas físicas también podría derivarse de una perturbación grave de infraestructuras críticas, tal como se definen en el artículo 2, punto 4, de la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo (19), cuando la perturbación o destrucción de dichas infraestructuras críticas suponga una amenaza inminente para la vida o la seguridad física de una persona, también al perjudicar gravemente el suministro de productos básicos a la población o el ejercicio de la función esencial del Estado»⁵⁴.

Otra de las excepciones, la prevista en el apartado 3, hace referencia a los hechos delictivos recogidos en el anexo II del Reglamento: terrorismo, trata de seres humanos, explotación sexual de menores y pornografía infantil, tráfico ilícito de estupefacientes o sustancias psicotrópicas, tráfico ilícito de armas, municiones y explosivos, homicidio voluntario, agresión con lesiones graves, tráfico ilícito de órganos o tejidos humanos, tráfico ilícito de materia-

54 Considerando 33 REIA.

les nucleares o radiactivos, secuestro, detención ilegal o toma de rehenes, delitos que son competencia de la Corte Penal Internacional, secuestro de aeronaves o buques, violación, delitos contra el medio ambiente, robo organizado o a mano armada, sabotaje y participación en una organización delictiva implicada en uno o varios de los delitos enumerados en esta lista.

Pero, además, de exigir que la acción delictiva constituya alguno de los tipos descritos, exige también que la legislación del Estado miembro sancione ese hecho con una pena máxima de al menos cuatro años. Es preciso realizar aquí un breve comentario sobre esta última excepción. Conviene matizar, que la aplicación del límite de la pena prevista por la legislación nacional ha de relacionarse con los tipos delictivos recogidos en el anexo II, sin que pueda considerarse aisladamente. Lo contrario supondría convertir este supuesto en un cajón de sastre que permitiría la aplicación de estos sistemas con una excesiva amplitud. Si se entendiera que el límite de la sanción de una duración máxima de al menos cuatro años, pudiera tomarse aisladamente de los tipos relacionados en el anexo II, se trataría de una norma totalmente permisiva, que no se corresponde con la protección de derechos fundamentales de tanta trascendencia como los afectados por este tipo de sistemas. En este sentido, si se toma en consideración nuestro ordenamiento jurídico penal, podría aplicarse respecto de hechos delictivos que no tengan la consideración de delitos graves atendiendo a la duración de la pena. En el Código Penal se clasifican como penas graves aquellas que tengan una duración superior a cinco años, y como penas menos graves las que tengan una duración entre tres meses y cinco años⁵⁵. Por ello, y atendiendo a la literalidad del artículo 5.1h), habrá de interpretarse que la previsión de la pena se encuentra vinculada a los delitos recogidos en el anexo, sin que pueda considerarse aisladamente.

El segundo apartado del artículo 5 REIA, incide en la finalidad de la utilización de los sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho, reiterando que su objetivo ha de ser la localización o identificación de una persona sospechosa de haber cometido un delito, a fin de llevar a cabo una investigación o un enjuiciamiento penal, o de ejecutar una sanción penal por alguno de los delitos mencionados. Y establece que la decisión sobre su uso deberá tener en cuenta, de un lado la *naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema*; y de otro, *las consecuencias que tendría el uso del sistema en los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias*.

55 V. MORENO CATENA, V., «Los datos en el sistema de justicia y la propuesta de reglamento UE...», *Uso de la información y de los datos personales...*, op. cit., pág. 54.

No cabe duda que el legislador europeo está condicionando el uso de los sistemas de identificación biométrica remota en tiempo real a la valoración del denominado juicio de proporcionalidad. Es más, toda la redacción de la letra h) del primer apartado del precepto, conlleva una remisión a este principio considerado en toda su extensión. De un lado, se limita el uso de este tipo de sistemas, pero atendiendo a su necesidad para la investigación de hechos delictivos considerados graves o muy graves, permite su utilización con el objetivo de identificar y localizar a la persona que puede resultar responsable, o que ya lo es, y está pendiente de ejecutarse la sanción. De otro, y con carácter previo al empleo de estos sistemas, obliga a tener en cuenta la naturaleza de la situación y el perjuicio que se produciría al no recurrir a este sistema (de nuevo el principio de necesidad), y en el otro lado de la balanza el impacto que podría darse en los derechos y libertades de los ciudadanos. La referencia al juicio de proporcionalidad es evidente y lleva necesariamente a relacionar la autorización de estos sistemas con los principios rectores de las medidas de investigación tecnológicas previstos en la Ley de Enjuiciamiento Criminal⁵⁶.

Continúa el precepto estableciendo los límites que rodean la utilización de este tipo de sistemas. Más allá del ámbito objetivo, ya delimitado en el apartado 1h) del artículo 5, y de la aplicación del principio de proporcionalidad, prevé también el precepto la regulación de otros requisitos que garanticen que la injerencia en los derechos de los ciudadanos resulte lo menos perjudicial posible. En este sentido, encomienda a la legislación de los Estados miembros, la regulación de los límites temporales, geográficos y personales que garanticen una utilización adecuada de estas herramientas⁵⁷.

Otra de las garantías previstas en el precepto, que se recogen en su tercer apartado, y centrando su aplicación en la investigación penal, es la exigencia de autorización judicial previa para su utilización. Dicha autorización se otorgará una vez presentada solicitud motivada, y de conformidad con la legislación nacional. Es evidente que el contenido de esta solicitud se puede reconducir a la prevista en el artículo 588 bis b) LECrim, que lo recoge en relación a la petición formulada por la policía judicial o el Ministerio fiscal, al dirigirse al juez para la adopción de alguna de las medidas de investigación tecnológicas previstas, como son, la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales

56 CUATRECASAS MONFORTE, C., «IA: herramienta de investigación criminal» en *La Ley digital*, 24 enero 2024, pág. 95.

57 La regulación de las medidas de investigación tecnológica introducida en la Ley de enjuiciamiento Criminal por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la LECrim, podría servir como referencia respecto de los principios rectores y las garantías procesales aplicables en la utilización de estos sistemas. En este sentido y en relación a la utilización de los drones como diligencia de investigación, se pronuncia BUENO DE MATA, F., «La utilización de drones como diligencia de investigación tecnológica: consecuencias probatorias» en *Diario La Ley*, número 16, 20 de Marzo de 2018, <https://laleydigital.laley-next.es/>, págs.. 3 y ss.

mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.

No obstante, permite el artículo 5.3 REIA, que en casos de urgencia debidamente justificados, como se prevé también en la Ley procesal penal respecto de las medidas de investigación tecnológica⁵⁸, se puede proceder a la utilización del sistema sin dicha autorización previa, siempre que se solicite la convalidación en el plazo de 24 horas. En caso de rechazarse, deberá interrumpirse su uso, destruyendo los resultados.

El tercer apartado del artículo 5 REIA regula la intervención de la autoridad judicial respecto de la autorización del uso de estos sistemas inteligentes. Aunque el precepto únicamente hace alusión a los sistemas de identificación biométrica remota en tiempo real, lo cierto es que la garantía de la autorización judicial previa, o la convalidación posterior en caso de urgencia, debería regularse con carácter general para todo tipo de utilización de sistemas de alto riesgo, cuando afecten a sujetos determinados. En este sentido el precepto alude a la resolución motivada de la autoridad judicial, previo examen de pruebas objetivas o indicios claros, y realizado el juicio de proporcionalidad.

Finalmente, el Reglamento concede a los Estados miembros la posibilidad de regular la utilización de los sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho, pero condiciona dicha regulación a que se realice dentro de los límites marcados por el artículo 5.1h) REIA, y en las condiciones previstas en los apartados 2 y 3. En este sentido, se prevé en el precepto que dichas normas deberán establecer el procedimiento para la solicitud y la autorización previstas. Además, *«...especificarán también para qué objetivos de los enumerados en el apartado 1, párrafo primero, letra h), y en su caso en relación con qué delitos de los indicados en la letra h), inciso iii), se podrá autorizar a las autoridades competentes para que utilicen esos sistemas con fines de garantía del cumplimiento del Derecho»*. Como ya se ha indicado, dicho inciso iii) se remite a los tipos delictivos previstos en el anexo II, que ya se han mencionado anteriormente, exigiendo, además, como también se ha indicado, como requisito vinculado a los tipos descritos, que la legislación del Estado miembro sancione ese hecho con una pena máxima de al menos cuatro años.

Las garantías previstas en el tantas veces citado artículo 5 REIA, se completan con las previstas en el décimo apartado del artículo 26 de la norma, que alude a las actuaciones policiales relativas a la búsqueda de una persona sospechosa de haber cometido un delito, o condenado por ello⁵⁹. Así, exige

58 Artículo 588 ter d) apartado tercero en relación con las intervenciones telefónicas; Artículo 588 quinquies b) apartado cuatro; 588 sexies c) apartados tercero y cuarto.

59 El Reglamento en este artículo 26.10 hace referencia al «responsable del despliegue»

la previa autorización judicial para la utilización de los sistemas de identificación biométrica remota en diferido, en el plazo más breve posible y, en todo caso, en un plazo de cuarenta y ocho horas. Excepciona el precepto aquellos supuestos en los que la identificación del sospechoso se realice sobre la base de hechos objetivos y verificables vinculados directamente al delito. En caso de que se deniegue la autorización dejará de utilizarse el sistema, y deberán eliminarse los datos resultantes de su utilización.

Finaliza el apartado citado prohibiendo la utilización de estos sistemas de forma indiscriminada y sin vinculación con una actuación delictiva, un proceso penal, una amenaza real y actual, o real y previsible de delito, o con la búsqueda de una persona desaparecida concreta. Además, se velará para que las autoridades garantes del cumplimiento del Derecho, no puedan adoptar ninguna decisión que produzca efectos jurídicos adversos para una persona exclusivamente sobre la base de los resultados de salida de dichos sistemas de identificación biométrica remota en diferido⁶⁰.

Lo que se desprende de esta regulación, es la aplicación a los sistemas de IA relacionados con la aplicación de la ley, de un régimen similar al previsto en el proceso penal para la adopción de diligencias de investigación que limiten derechos fundamentales. La reserva de ley, la reserva jurisdiccional que permita un examen detallado y autorice motivadamente la aplicación del sistema, y la valoración, en función del principio de proporcionalidad, de la necesidad e idoneidad de su utilización, constituyen un conjunto de garantías diseñado para la protección de los derechos de los ciudadanos⁶¹. Junto a todo ello, el examen de los indicios y las evidencias presentadas exige la previa incoación de un proceso penal, tal y como también se prevé respecto de la autorización de otras medidas de investigación.

1.2.3. Garantías relacionadas con el tratamiento de datos. Una aproximación a su estudio

Si bien la relación entre la inteligencia artificial y la protección de datos personales será objeto de tratamiento en el epígrafe siguiente, se ha consi-

entendiendo por tal, como recoge el artículo 6.4 REIA, una persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional.

60 En relación a esta cuestión el Reglamento permite el tratamiento de los datos biométricos conforme a lo prescrito en el artículo 9 del Reglamento (UE) 2016/679 y del artículo 10 de la Directiva (UE) 2016/680.

61 DE HOYOS SANCHO, M., «El proyecto de Reglamento de la Unión Europea sobre inteligencia artificial, los sistemas de alto riesgo y la creación de un ecosistema de confianza», en *Justicia poliédrica en periodo de mudanza (Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad)*, dirigido por Barona Vilar, Tirant lo Blanch, Valencia, 2022, pág. 409.

derado conveniente hacer una breve referencia en este apartado, debido a las previsiones que el REIA recoge respecto de esta cuestión.

Partiendo del hecho de que los sistemas de IA se alimentan de datos para su procesamiento y análisis, la alta calidad del conjunto de datos es una exigencia irrenunciable. Pero también lo es, que se habiliten mecanismos que permitan controlar la trazabilidad de dichos sistemas y la vigilancia de su funcionamiento. Para ello es fundamental facilitar la documentación técnica que describa en un lenguaje comprensible las capacidades y utilidades del sistema, sus características y condiciones de funcionamiento, pero también los riesgos y limitaciones. El Reglamento de Inteligencia Artificial establece que los sistemas calificados de alto riesgo, han de permitir el registro automático de las actuaciones, mediante archivos de registro, y durante toda la vida útil del sistema. Estos registros permitirán acceder a las actuaciones realizadas facilitando su control por parte de los responsables⁶².

En este sentido, no se puede perder de vista que la opacidad de estos sistemas y la complejidad de su funcionamiento, fundamentalmente en aquellos que utilizan algoritmos de aprendizaje automático, es una de las principales preocupaciones cuando se trata de utilizarlos en el sistema de justicia penal⁶³. La legitimidad del sistema se encuentra estrechamente relacionada con la calidad de los datos introducidos, su trazabilidad y con la transparencia de su funcionamiento. En otro caso se pondría en peligro la posición procesal de las personas investigadas, y el propio sistema penal basado en la contradicción y la igualdad de armas⁶⁴.

Así lo señala el Reglamento en su considerando 59 cuando afirma que «*si el sistema de IA no está entrenado con datos de buena calidad, no cumple los requisitos adecuados en términos de rendimiento, de precisión o de solidez, o no se diseña y prueba debidamente antes de introducirlo en el mercado o ponerlo en servicio, es posible que señale a personas de manera discriminatoria, incorrecta o injusta. Además, podría impedir el ejercicio de importantes derechos procesales fundamentales, como el derecho a la tutela judicial efectiva y a un juez imparcial, así como el derecho a la defensa y a la presunción de inocencia, sobre todo cuando dichos sistemas de IA no sean lo suficientemente transparentes y explicables ni estén suficientemente bien*

62 DE HOYOS SANCHO, M., «El uso jurisdiccional de los sistemas de inteligencia artificial y la necesidad de su armonización en el contexto de la Unión Europea» en *Revista General de Derecho Procesal*, número 55, 2021, pág. 21 y ss.

63 V. ALONSO SALGADO, C., «El problema de la falta de transparencia en la interacción de la inteligencia artificial y la justicia», en *Inteligencia artificial legal...*, op. cit., pág. 519.

64 BARONA VILAR, S., *Algoritmización del derecho y de la justicia*, op. cit., pág. 197; GASCÓN INCHAUSTI, F., «Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial», en *La justicia digital en España y la Unión Europea* (Conde Fuentes y Serrano Hoyo, dirs.), Atelier y Fundación Serra Domínguez, Barcelona, 2019, págs. 203 y ss.

documentados. Por consiguiente, en la medida en que su uso esté permitido conforme al Derecho de la Unión y nacional pertinente, procede clasificar como de alto riesgo varios sistemas de IA destinados a ser utilizados con fines de garantía del cumplimiento del Derecho cuando su precisión, fiabilidad y transparencia sean especialmente importantes para evitar consecuencias adversas, conservar la confianza de la población y garantizar la rendición de cuentas y unas vías de recurso efectivas... No debe ignorarse el impacto del uso de herramientas de IA en los derechos de defensa de los sospechosos, en particular la dificultad para obtener información significativa sobre el funcionamiento de dichos sistemas y la consiguiente dificultad para impugnar sus resultados ante los tribunales, en particular por parte de las personas físicas investigadas».

Poniendo el foco de atención en la Administración de Justicia, es importante tener en cuenta que los datos aportados al sistema de justicia son datos sensibles, relacionados con la vida privada de las personas, y proporcionados, en muchos casos, por los propios sujetos implicados. Por tanto, son datos que pertenecen a las partes implicadas, que los aportan únicamente para que puedan ser tratados en ese proceso concreto, sin renunciar a su titularidad⁶⁵.

Los sistemas de IA han de responder a la finalidad para la que se diseñan, por lo que han de revestir un nivel adecuado de precisión, robustez y ciberseguridad, a lo largo de todo su ciclo de vida útil. Para ello, en aquellos instrumentos de IA que continúan con el aprendizaje una vez puestos en funcionamiento, deben establecerse mecanismos de control que eviten que la retroalimentación provoque resultados erróneos. También es preciso que su diseño vaya acompañado de aplicaciones que permitan prevenir y controlar ataques de terceros, con el objetivo de provocar errores de funcionamiento.

El Reglamento asegura el control de los sistemas de IA a través de una serie de requisitos recogidos en su articulado. Las medidas de control incorporadas al propio sistema deben estar diseñadas para limitar su funcionamiento a los fines previstos, sin que puedan autodesactivarse, y deben responder a la supervisión humana.

De esta forma, el control o supervisión de una persona física se considera como garantía de seguridad en el funcionamiento y utilización de las aplicaciones de IA, estableciendo el artículo 14 REIA, que el objetivo de dicha supervisión será el de prevenir o reducir los riesgos que supone la utilización de estos sistemas, tanto para la salud como para la seguridad, o el ejercicio de los derechos fundamentales. También recoge el precepto las medidas de supervisión que pueden arbitrarse, que serán proporcionales a los riesgos del sistema.

65 MORENO CATENA, V., «Los datos en el sistema de justicia y la propuesta de reglamento UE...», *Uso de la información y de los datos personales...*, op. cit., pág. 57.

Es importante destacar, y así lo recoge el cuarto apartado del artículo 26 REIA, que la persona física designada como responsable del sistema, deberá controlar la pertinencia y utilidad de los datos que se introducen, y valorar que son los adecuados para la finalidad que se persigue.

Resulta obligado relacionar las previsiones sobre el tratamiento de los datos personales recogidas en el Reglamento europeo de IA, con las establecidas en la legislación española. No es posible por razones de espacio abordar un análisis completo de la regulación española que ha de aplicarse, pero sí hacer una breve mención, que se ampliará en un siguiente apartado. La LO 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, constituye sin duda la norma de referencia. Su primer precepto señala el objeto de la norma, centrándolo en la *protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública*».

Precisamente esa protección de las personas físicas en relación al tratamiento de sus datos personales, es lo que marca el límite fundamental respecto de dicho tratamiento, establecido en el artículo 11.1, que sólo lo permite cuando resulte necesarios para los fines previstos en el artículo 1, y siempre que la persona que lo realice tenga la condición de autoridad competente, y lo haga en el ejercicio de sus funciones.

Los artículos 6 y 7 de esta norma establecen los requisitos o garantías que han de observarse en el tratamiento de los datos personales, y las condiciones de su tratamiento por parte de los responsables autorizados. El artículo 7 regula el deber de colaboración de las Administraciones públicas, pero extiende este deber a cualquier persona física o jurídica. Por tanto, este deber de colaboración con las autoridades judiciales, el Ministerio fiscal y la policía judicial, se extiende a todos los ciudadanos, administraciones, instituciones y personas jurídicas en general, si bien lo condiciona a que resulte necesaria para alguno de los fines descritos en el artículo 1 de la Ley.

Es importante destacar, que la petición policial se ha de realizar motivadamente, exigiendo que dicha motivación ha de ser concreta y específica, y que deberá darse cuenta a la autoridad judicial y fiscal. Se garantiza así el control judicial sobre actuaciones que suponen una injerencia en derechos fundamentales como la intimidad, el secreto de las comunicaciones o al entorno digital. De esta forma, se impide que la obtención de datos se realice con carácter general, al exigir la vinculación a una investigación concreta y determinada⁶⁶.

66 DE LEMUS VARA, F.J., «Límites para el tratamiento de los datos de los no investigados en el proceso penal», en *Uso de la información y de los datos personales...op. cit.*, pág. 561.

Teniendo en cuenta que el tratamiento de datos personales sensibles⁶⁷ y su utilización, incluso, por las autoridades policiales y judiciales, puede suponer una injerencia grave en los derechos fundamentales, al afectar a la esfera privada de los ciudadanos, al derecho a la libertad y a otros derechos fundamentales de contenido procesal, el artículo 13 de la LO 7/2021, lo regula de forma muy restrictiva, permitiéndolo cuando «*sea estrictamente necesario*» y condicionándolo al cumplimiento de las garantías de protección de los derechos y libertades, y siempre que se cumplan alguna de las circunstancias específicamente previstas en el precepto.

2. Inteligencia artificial y protección de datos

2.1. La Directiva 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de Protección de Datos Personales

2.1.1. Antecedentes

La protección de datos de las personas físicas se configura como un derecho fundamental que adquiere especial importancia en los últimos años, como consecuencia de la utilización de los sistemas relacionados con las nuevas tecnologías y la inteligencia artificial que pueden incidir gravemente en su esfera de aplicación. Un análisis más amplio sobre el contenido de este derecho se abordará en el siguiente capítulo.

Es evidente que la libre circulación de datos personales y su tratamiento por sistemas de IA supone una ventaja indudable para la prevención, investigación y enjuiciamiento de conductas criminales, pero también resulta obvio que este tipo de actuación debe estar sujeta a un conjunto de garantías que protejan los derechos de los ciudadanos.

La Directiva 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de Protección de Datos Personales⁶⁸, marca ya un importante

67 Se refiere el precepto a datos personales que «...revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, los datos relativos a la salud o a la vida sexual o a la orientación sexual de una persona física...».

68 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Diario Oficial de la Unión Europea de 4 de mayo de 2016.

punto de partida, al considerar la protección de los datos de carácter personal como un derecho fundamental de las personas físicas (artículo 1.2a), consideración que también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea⁶⁹, y en el artículo 16 del Tratado de Funcionamiento de la Unión Europea⁷⁰, al determinar que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

La categoría de derecho fundamental de la protección de datos personales, y su relación con otros derechos fundamentales como la libertad, la vida privada y los derechos de naturaleza procesal, determina que el título de la Directiva ya haga referencia a su tratamiento para la investigación, detección o enjuiciamiento de hechos delictivos, en un empeño de establecer un equilibrio entre la protección del derecho fundamental, y la necesaria aplicación del tratamiento de datos en el proceso penal⁷¹.

Por tanto, del título de la Directiva deriva su ámbito de aplicación, ya que el tratamiento de datos que regula, debe limitarse a los objetivos previstos de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales. Además, dicho tratamiento se llevará a cabo por las autoridades encargadas de esas funciones, en nuestro país, las autoridades policiales, el Ministerio fiscal y las autoridades judiciales.

La nueva regulación refleja la política de la Unión Europea sobre el equilibrio entre la protección de los datos personales, y su libre circulación para la prevención, investigación, detección o enjuiciamiento por un delito. Por lo que se confirma la necesidad de libre circulación de datos de carácter personal, pero respetando los requisitos de su protección⁷².

69 Artículo 8. Protección de datos de carácter personal: 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

70 Artículo 9 del Tratado de Lisboa: 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes. Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea.

71 V. FIDOROVA, A., «Directiva 2016/680: hacia mayor coherencia de protección de datos personales en la cooperación policial y judicial penal», en *Nuevos postulados de la cooperación judicial en la Unión Europea*. Libro homenaje a la profesora M.ª Isabel González Cano (Moreno Catena/Romero Pradas, dirs.), Tirant lo Blanch, Valencia, 2021, pág. 719.

72 V. más ampliamente SANTOS SÁNCHEZ, D.J., «Los tratamientos de datos personales para la prevención, investigación, detección o enjuiciamiento de infracciones penales: considera-

Partiendo de esta protección, y de una utilización adecuada de los datos personales de las víctimas, testigos y sospechosos de hechos delictivos, la Directiva facilita la cooperación internacional en la lucha contra la delincuencia. Con esta finalidad, establece una serie de límites en la utilización de los datos personales con fines de prevención, detección, investigación o enjuiciamiento de infracciones penales, prohibiendo en el artículo 11, la toma de decisiones basadas exclusivamente en un tratamiento automatizado de datos, salvo que esté específicamente previsto en la legislación del Estado miembro. Además, reconoce el derecho del interesado a solicitar la intervención humana en esta toma de decisiones, cuando le afecten jurídicamente, o puedan causarle un perjuicio.

En la misma línea, afirma que la toma automática de decisiones no puede basarse en los datos a los que se refiere el artículo 10 (origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida sexual o las orientaciones sexuales de una persona física), salvo que se garanticen los derechos y libertades del interesado. Se prohíbe también la elaboración de perfiles que puedan dar lugar a una discriminación de las personas físicas, utilizando los datos previstos en el ya citado artículo 10⁷³.

En este contexto, la sentencia de 8 de abril de 2014, del Tribunal de Justicia (Gran Sala)⁷⁴, en la que el Tribunal invalida la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público, o de redes públicas de comunicaciones, y por la que se modificaba la Directiva 2002/58/CE (asuntos C-293/12 y C-594/12), puede considerarse un antecedente inmediato de la vigente directiva 2016/680, de 27 de abril.

Es importante plantear el punto de partida de esta resolución del Tribunal de Justicia. Conscientes de la importancia cada vez mayor del tratamiento de los datos personales en todas sus múltiples aplicaciones (actividad empresarial y económica, actividad profesional, desarrollo científico, relaciones personales, etc.), y su repercusión en los derechos fundamentales de los ciudadanos, el Parlamento europeo y el Consejo dictan la directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, y a la libre circulación

ciones de la AEPD» en *Investigación y proceso penal en el siglo XXI. Nuevas tecnologías y protección de datos* (Pereira Puigvert/Ordoñez Ponz, dirs), Editorial Aranzadi, Cizur Menor (Navarra), págs. 713 y ss.

73 Sobre la denominada «Justicia automatizada» puede consultarse GUZMÁN FLUJA, V., «Proceso penal y justicia automatizada» en *Revista General del Derecho*, número 53, 2021.

74 Sentencia del Tribunal de Justicia (Gran Sala) de 8 de abril de 2014 — Comisión Europea/Hungría (Asunto C-288/12)

de estos datos⁷⁵, que se complementa con la Directiva 2002/58/CE, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, tal y como se recoge en su artículo 1.2. El artículo 5 de esta última directiva, establece la confidencialidad de las comunicaciones y de los datos de tráfico asociados a ellas, prohibiendo su almacenamiento salvo autorización del interesado, o en los casos y condiciones previstos en el artículo 15⁷⁶, mientras que su artículo 6.1 regula la eliminación de los datos, o su conversión en anónimos⁷⁷.

En marzo de 2006, el Parlamento y el Consejo Europeo, dictan la Directiva 2006/24/CE, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público, o de redes públicas de comunicaciones, directiva que modifica la 2002/58, permitiendo la conservación de los datos en el artículo 3, y el acceso a los mismos en el artículo 4.

Esta directiva 2006/24, parte de la existencia en varios Estados miembros de legislaciones que regulan la conservación de datos por los prestadores de servicios para la prevención, investigación, detección y enjuiciamiento de delitos, señalando que estas disposiciones varían considerablemente de unos países a otros, perjudicando el mercado interior de las comunicaciones electrónicas, y la actividad de los prestadores de estos servicios. Además, teniendo muy en cuenta la importancia que el tratamiento de los datos personales representa en la investigación de delitos de tanta gravedad como los relacionados con el terrorismo, o los cometidos por la delincuencia organizada, se considera relevante armonizar las disposiciones de los Estados miembros relativas a la conservación de datos. En este sentido el artículo 1 establece que 1. *«La presente Directiva se propone armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas*

75 La citada directiva se deroga por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

76 En el precepto se recogen excepciones cuando se trata de una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE.

77 Artículo 6.1. «Sin perjuicio de lo dispuesto en los apartados 2, 3 y 5 del presente artículo y en el apartado 1 del artículo 15, los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación».

de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro. 2. La presente Directiva se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas».

La sentencia del Tribunal de Justicia de la UE, trae causa de dos cuestiones prejudiciales planteadas por Irlanda y Austria, sobre la validez de la citada directiva 2006/24, de conservación de datos, en relación con los artículos 7, 8 y 11 de la Carta de los Derechos Fundamentales de la Unión Europea. Considera el Tribunal que *«Estos datos, considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan»*. Por tal motivo, y pese a que no se autoriza el acceso a la información consultada en las redes, sí puede apreciarse que la propia conservación supone una injerencia en el derecho a la libertad de expresión, y condicionar el uso de los medios referenciados por la directiva. Además, la citada conservación supone también, ya de por sí, una injerencia en el derecho a la protección de la vida privada, recogido en el artículo 7 de la Carta, al dictarse la propia directiva para excepcionar la protección que se otorgaba en la Directiva 95/96, suponiendo asimismo una injerencia en el derecho a la protección de datos personales previsto en el artículo 8 de la Carta.

El Tribunal no cuestiona la necesidad de la conservación de estos datos y el acceso a ellos con fines de investigación, defensa, seguridad, interés general, etc., tal y como se recoge en la Directiva. Es más, en su considerando 51 defiende su necesidad y eficacia, pero también advierte, que tal y como se regula, se está afectando a los derechos fundamentales de toda la población de la Unión Europea, sin distinción. *«Abarca de manera generalizada a todas las personas, medios de comunicación electrónica y datos relativos al tráfico sin que se establezca ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves»*.

Se permite esta medida con carácter general, sin que las personas cuyos datos se conservan se encuentren, ni siquiera indirectamente, en una situación que pueda dar lugar a acciones penales, sin que existan indicios de criminalidad, o se encuentren indirectamente vinculadas con los sospechosos de acciones delictivas, pudiendo incluso afectar a aquellos que se encuentran amparados por el secreto profesional. Tampoco se establece una limitación

temporal o geográfica, no se limita, o condiciona, a las personas que pueden tener acceso, ni se somete a ningún control judicial para la autorización⁷⁸.

Finaliza el Tribunal afirmando, que «la Directiva 2006/24 no establece reglas claras y precisas que regulen el alcance de la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta. Por lo tanto, debe considerarse que esta Directiva constituye una injerencia en los derechos fundamentales de gran magnitud y especial gravedad en el ordenamiento jurídico de la Unión, sin que esta injerencia esté regulada de manera precisa por disposiciones que permitan garantizar que se limita efectivamente a lo estrictamente necesario». En consecuencia, acuerda la invalidez de esa Directiva.

Sentados estos antecedentes, se elabora la Directiva 2016/680, de 27 de abril. En este texto el legislador europeo, además de regular la protección de las personas físicas respecto del tratamiento de sus datos personales por autoridades competente con los fines que se describe, deroga también la Decisión Marco 2008/977/JAI del Consejo, en la que se establecen las pautas a seguir por los Estados miembros de la Unión Europea⁷⁹. Respecto de esta Decisión Marco de 27 de noviembre, sobre protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal en el ámbito de la UE, ya se habían puesto de relieve algunas deficiencias en su regulación, fundamentalmente centradas en los mecanismos de protección de los derechos fundamentales, al establecer limitaciones no sujetas a suficientes garantías de concreción, y al no prever los derechos de los afectados por el tratamiento de datos, dejando en manos de los Estados miembros su regulación, sin proporcionar unas directrices comunes sobre las que se pueda articular un sistema unificado⁸⁰.

Estas deficiencias, y las que derivaban de las normativas precedentes, se pretenden resolver con la Directiva 2016/680, que se dicta con la finalidad de proporcionar a los Estados miembros, las bases para articular un régimen armonizado de protección y libre circulación de datos respecto de los fines

78 V. más ampliamente RODRÍGUEZ LAINZ, J.L., «La nueva doctrina del Tribunal Supremo frente a la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de conservación preventiva de datos de telecomunicaciones» en *Uso de la información y de los datos personales...*, págs. 375-421.

79 V. GONZÁLEZ CANO, I., «Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680», en *Revista Brasileña de Derecho Procesal Penal*, volumen 5, número 3, 2019, pág. 1336.

80 V. más ampliamente, Pillado González, M.E., «Principios generales de protección de datos en la cesión de información en la persecución criminal a la vista de la Directiva 2016/680 del Parlamento europeo y del Consejo, de 27 de abril de 2016, por la que se deroga la Decisión Marco 2008/977», en *Nuevos postulados de la cooperación judicial en la Unión Europea... op.cit.*, págs. 787-789. V. también, V. FIODOROVA, A., «Directiva 2016/680: hacia mayor coherencia de protección de datos personales en la cooperación policial y judicial penal», en *Nuevos postulados de la cooperación judicial...*, op. cit., pág. 716.

previstos, atendiendo a las directrices e indicaciones marcadas por el Consejo, la Comisión Europea y el Parlamento Europeo⁸¹.

2.1.2. Ámbito objetivo y subjetivo de aplicación

Como ya se ha señalado, el ámbito objetivo de aplicación está, en principio, claramente reflejado en su título, abarcando no sólo las fases por las que discurre el proceso penal (detección, investigación, enjuiciamiento de infracciones penales o de ejecución de sanciones penales), sino también las actuaciones relacionadas con la prevención de las actuaciones delictivas. De esta forma, las medidas de protección que pueden ejercer los sujetos afectados, lo son también en relación a las actuaciones preventivas. En este aspecto, es importante destacar que las actuaciones preventivas, e incluso predictivas llevadas a cabo por las autoridades policiales, en su labor de lucha contra la criminalidad, han adquirido en los últimos años una extraordinaria relevancia, directamente vinculada a la aplicación de los adelantos tecnológicos y de los sistemas de inteligencia artificial, cuestión ésta que se tratará en un capítulo posterior.

No obstante, si es necesario precisar la referencia que la Directiva hace a la seguridad pública, vinculándola a las actuaciones que se integran en el objetivo de su regulación. El artículo 1, al establecer su objeto, recoge expresamente «*La presente Directiva establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por parte de las autoridades competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública*». Si bien el concepto de seguridad pública abarca múltiples actuaciones que se apartan de las que se relacionan con la criminalidad, lo cierto es que éstas últimas han de integrarse en la defensa de la seguridad pública. Pero el legislador europeo, ha querido ir más allá en un intento de salvaguardar, de forma más extensa, la protección de datos personales, y al mismo tiempo, rodear la actuaciones de seguridad pública ajenas a las investigaciones delictiva, de las mismas garantías y principios que protegen estas últimas⁸².

Respecto a su ámbito subjetivo, el artículo 6 de la norma recoge distintas categorías de interesados, encomendando a los Estados miembros la elaboración, por parte del responsable del tratamiento, de una clasificación que

81 La citada directiva es objeto de transposición a nuestro ordenamiento jurídico por la LO 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.

82 GUZMÁN FLUJA, V., «Consideraciones sobre el alcance objetivo y subjetivo de la Directiva 2016/680» en *Nuevos postulados de la cooperación judicial en la Unión Europea...*, op. cit., pág. 845.

establezca una clara distinción entre los datos personales de cada grupo. Dicha clasificación responde a la evidencia de que, si bien todos los sujetos integrantes del grupo se ven afectados por el tratamiento de sus datos personales, no todos lo son en la misma medida, al igual que tampoco lo es su posición respecto del proceso penal. Consecuentemente, las medidas relativas a la protección de sus datos personales también podrán ser diferentes⁸³. En consecuencia, se distinguen cuatro grandes bloques:

- a) personas sobre las que existan motivos fundados para presumir que han cometido, o van a cometer una infracción penal. La expresión «motivos fundados» utilizada por el legislador, podrá equipararse a la recogida por nuestra norma procesal penal cuando regula la adopción de alguna medida de protección o de investigación, basando su acuerdo en la existencia de «indicios fundados»⁸⁴. Mayores problemas plantean la interpretación de lo que ha de entenderse por «...presumir que han cometido, o van a cometer una infracción penal», al referirse no sólo a actuaciones materiales de las que ha de deducirse la presunción, sino que esas actuaciones han de enmarcarse en un espacio temporal. Será necesario determinar cuál es la autoridad que debe realizar dicha valoración, lo que puede plantear algún problema cuando se trata de actuaciones a prevención⁸⁵.
- b) personas condenadas por una infracción penal;
- c) víctimas de una infracción penal, o personas que, en atención a determinados hechos, puedan ser víctimas de una infracción penal;
- d) terceras partes involucradas en una infracción penal (testigos, informadores o personas relacionados con las mencionadas en las letras a) y b).

En relación con la protección de su derecho a la privacidad de los datos, se ha reforzado la posición del interesado, esto es, de la persona física identificada o identificable, titular de la información o datos personales tratados (art. 3.1). Así, se prevé el reconocimiento específico de los derechos en el Capítulo III de la Directiva (art. 12 a 18), que no sólo contiene, como una novedad en relación con los datos personales penales, el reconocimiento de los

83 Sobre la conveniencia de esta clasificación y sus consecuencias puede consultarse GUZMÁN FLUJA, V., «Consideraciones sobre el alcance objetivo y subjetivo de la Directiva...», *op. cit.*, págs. 864-870.

84 El artículo 588 bis b) 2. 2º LECrim hace referencia a los indicios de criminalidad que habrán de reflejarse en la solicitud para la autorización judicial de una intervención de comunicaciones personales. El artículo 588 bis c) 93.a, se refiere a los indicios racionales para fundar la medida en la resolución autorizante de las citadas intervenciones. El Artículo 588 quinquies sobre la captación de imágenes en lugares o espacios públicos, recoge los indicios fundados de la relación de terceros con los investigados, entre otros.

85 V. sobre esta cuestión GUZMÁN FLUJA, V., «Consideraciones sobre el alcance objetivo y subjetivo de la Directiva...», *op. cit.*, págs. 874-878.

derechos ARCO (acceso, rectificación, cancelación y oposición), en favor de los titulares de los datos que sean objeto de tratamiento, sino que, además, reconoce a los interesados la posibilidad de ejercicio de esos derechos tanto en las investigaciones y procesos penales que se hayan desarrollado (art. 18.5), como en las comprobaciones llevadas a cabo por la autoridad independiente de control (art. 17), es decir, en lo relativo a las actuaciones que pueda llevar a cabo la autoridad independiente de control con la finalidad de proteger los derechos y libertades fundamentales de las personas respecto al tratamiento de sus datos personales⁸⁶.

2.1.3. La supervisión de la autoridad independiente de control. Su determinación respecto de los datos relacionados con la Administración de Justicia

La Directiva establece la supervisión del tratamiento de los datos personales por una autoridad independiente, de carácter administrativo, que tendrá que llevar a cabo una actividad de control para proteger los derechos fundamentales, actividad que, en el marco de un proceso penal, ha de coordinar, en su caso, con las autoridades judiciales o de investigación de los hechos delictivos. Habrá que determinar si la Directiva ofrece los instrumentos adecuados para que ese control sobre los datos personales pueda respetarse adecuadamente en la investigación penal. Se trata de comprobar cómo puede accederse a los datos personales de los ciudadanos, para que su utilización en un proceso penal no vulnere los derechos fundamentales de los investigados, o de terceros que resulten afectados en ese proceso. Además, resulta necesario verificar si la autoridad administrativa de control es competente también para la supervisión del tratamiento de datos personales en los órganos judiciales con los fines descritos en la Directiva, o bien resulta necesario designar otras autoridades independientes que asuman exclusivamente el control en los órganos judiciales.

El artículo 41 prevé la designación de una autoridad independiente de control que supervise su aplicación, y la de la norma que la desarrolle, con la finalidad de proteger los derechos y libertades fundamentales de las personas respecto al tratamiento de sus datos personales. En este sentido, será necesario aclarar la legitimación de dicha autoridad competente para llevar a cabo esa función, y hasta donde llegan sus competencias. Además, también deberá precisarse qué tipo de datos pueden controlar, y cuáles son las consecuencias o efectos de dicho control⁸⁷.

86 COLOMER HERNÁNDEZ, I., «Control y límites en el uso de la información y los datos personales por parte de la Inteligencia artificial en los procesos penales», en *Justicia algorítmica...*, op. cit., pág. 291.

87 COLOMER HERNÁNDEZ, I., «Control y límites en el uso de los datos personales penales en la investigación y represión de los delitos a la luz de la directiva 2016/6801» en *Nuevos postulados de la cooperación judicial en la Unión Europea...*, op. cit., págs. 296-297

Partiendo de este contexto, resulta obligado definir o delimitar las funciones de esta autoridad de control, en relación con el uso y tratamiento de los datos personales trasladados al proceso penal por parte de las autoridades policiales y judiciales. Esta actuación es, si cabe, más relevante cuando se trata de supervisar los datos a los que pueden acceder los sistemas de IA. Se trata de aclarar si entre las funciones de las autoridades de control se encuentra la de supervisar el acceso de los sistemas inteligentes a los datos personales, o, dicho de otra forma, ¿pueden estas autoridades filtrar los datos con los que se nutren estos sistemas cuando se trata de utilizarlos o de aplicarlos en el sistema de justicia penal?⁸⁸.

Sobre esta cuestión es necesario abordar varias reflexiones. En primer lugar, precisar que la actividad de supervisión y control de la autoridad independiente se centrará en comprobar que el tratamiento de datos se ha llevado cabo conforme a los principios recogidos en el artículo 4 de la Directiva, esto es:

- a) Que sean tratados de manera lícita y leal;
- b) Recogidos con fines determinados, explícitos y legítimos, y no ser tratados de forma incompatible con esos fines;
- c) Adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados;
- d) Exactos y, si fuera necesario, actualizados; se habrán de adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que son tratados;
- e) Conservados de forma que permita identificar al interesado durante un período no superior al necesario para los fines para los que son tratados;
- f) Tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas.

No cabe duda que esta regulación trae a colación, una vez más, la aplicación del principio de proporcionalidad en toda su extensión. Los principios de necesidad, idoneidad y proporcionalidad en sentido estricto, vuelven a ser de obligado cumplimiento en este tipo de actuaciones, como lo son en todas aquellas que supongan una restricción o limitación de derechos fundamentales. Junto con el respeto al principio de legalidad y a la exclusividad

88 V. más ampliamente, COLOMER HERNÁNDEZ, I., «Control y límites en el uso de la información...», *op. cit.*, pág. 294.

jurisdiccional en su autorización, conforman las garantías básicas del procedimiento para su utilización en el proceso penal⁸⁹.

Y, en segundo lugar, es importante poner de relieve que la citada Directiva, no establece las consecuencias o efectos de la aplicación, o de la incorporación en el proceso penal de resultados o propuestas obtenidas de las aplicaciones relacionadas con la inteligencia artificial, que han sido tratados con datos personales ilícitamente obtenidos. Por ello, lo único que cabe es la aplicación de la exclusión probatoria, tal y como se recoge en el artículo 236 ter LOPJ, en relación con la regulación del artículo 11.1 LOPJ⁹⁰.

Pero volviendo a la intervención de la autoridad de control, la Directiva establece en sus artículos 46 y siguientes, un sistema de protección de los interesados frente al tratamiento irregular o ilegal de sus datos personales con fines penales, que recoge un conjunto de garantías buscando el equilibrio entre el derecho a la protección de datos personales, y el derecho de investigación y enjuiciamiento de las infracciones penales⁹¹.

Como ya se ha apuntado anteriormente, y atendiendo precisamente a esta función de la autoridad independiente, resulta de interés determinar si la autoridad independiente de control para los datos personales con relevancia penal, puede ser la misma que se encarga de su protección general, o por el contrario, ha de designarse una autoridad independiente *ad hoc* para este tipo de datos⁹². La propia especialidad de los datos a que se refiere la Directiva, junto con la también especial finalidad de su tratamiento, hacen aconsejable que la autoridad de control independiente sea una autoridad específica para este tipo de tratamiento.

En este sentido, el artículo 41.3 de la Directiva establece que «*Los Estados miembros podrán disponer que una autoridad de control creada en virtud del Reglamento (UE) 2016/679 pueda ser la autoridad de control mencionada en la presente Directiva y asuma la responsabilidad de las funciones de la autoridad de control que vayan a crearse de conformidad con el apartado 1 del presente artículo*». De tal forma que, en función de los dispuesto

89 GONZÁLEZ CANO, I., «Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680», en *Revista Brasileira de Direito Processual Penal*, 2019, volumen. 5, número 3, pág. 1369.

90 V. DELGADO MARTÍN, J., «Protección de datos personales y prueba en el proceso» en *Diario La Ley*, 2019, número 9383; V. ampliamente PÉREZ GIL, J., «Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal», en *Justicia: ¿garantías versus eficiencia?*, Tirant lo Blanch, Valencia, 2019, pág. 399 a 441.

91 COLOMER HERNÁNDEZ, I., «Control y límites en el uso de los datos personales penales en la investigación...», *op. cit.*, pág. 741.

92 COLOMER HERNÁNDEZ, I., «Control y límites en el uso de la información y los datos personales por parte de la Inteligencia artificial en los procesos penales», en *Justicia algorítmica...*, pág. 289.

por este precepto, podría encargarse a la Agencia Española de Protección de Datos, creada por la Ley 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales⁹³. Sin embargo, pese a que la citada Ley 3/2018, deroga la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, su disposición transitoria cuarta señala expresamente, que los tratamientos de datos con relevancia penal a los que se refiere la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, «...continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva». El citado artículo 22 regulaba los ficheros de las Fuerzas y Cuerpos de la Seguridad del Estado, relativo al tratamiento de datos personales que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales⁹⁴.

Como se verá en el siguiente apartado, es la Ley 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, la que traspone la Directiva al ordenamiento jurídico español, regulando tanto las autoridades encargadas del control sobre el tratamiento de datos, como sus funciones.

Tres son los requisitos que regula la Directiva 2016/680 para garantizar la independencia y funcionamiento de las autoridades independientes de control: en primer lugar, y como no puede ser de otra forma, la independencia de la autoridad designada; en segundo lugar, el establecimiento de un régimen jurídico o estatuto legal en el que se recojan todos los elementos que figuran en el artículo 44 de la Directiva (condiciones para su nombramiento, procedimiento de designación, duración del mandato, obligaciones, incompatibilidades...), y, finalmente, prevé el deber de secreto profesional al que está sujeta dicha autoridad independiente.

La función principal de esta autoridad independiente es la de supervisar el cumplimiento de la Directiva y de las normas de trasposición, atendiendo al

93 El artículo 44.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, regula la Agencia Española de Protección de Datos, considerándola como «...una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones». Dichas funciones se detallan en los artículos siguientes (artículos 44 a 56).

94 Conforme a lo establecido en el tercer apartado del artículo 44 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, la cooperación entre la Agencia, el CGPJ y la FGE deberá ser un principio de actuación en materia de protección de datos personales en el ámbito de la Administración de Justicia.

objeto y finalidad que se contempla, y con el fin último de proteger los derechos y libertades fundamentales de los ciudadanos respecto del tratamiento de sus datos personales⁹⁵.

En este contexto, es necesario poner de relieve lo establecido en el artículo 45.2 de la Directiva, en relación con el tratamiento de datos realizado por los órganos jurisdiccionales, que faculta a los Estados miembros a excluir dicho tratamiento del control de las autoridades independientes designadas conforme al artículo 44. Así, establece el precepto que «*Los Estados miembros dispondrán que cada autoridad de control no sea competente para controlar las operaciones de tratamiento efectuadas por los órganos jurisdiccionales en el ejercicio de su función judicial.*».

Sobre esta cuestión se había pronunciado el Tribunal Supremo, considerando que la Agencia Española de Protección de Datos no puede considerarse un órgano independiente a efectos del control del tratamiento de datos personales de la Administración de Justicia, al tratarse de un órgano que se inserta en el Poder ejecutivo. Conforme a lo establecido en el artículo 122 CE, es el Consejo General del Poder Judicial el órgano encargado de la supervisión del funcionamiento de los órganos jurisdiccionales, de las actuaciones realizadas por jueces y magistrados y de la actividad que, en ejercicio de la potestad jurisdiccional, se desarrolla en los órganos jurisdiccionales, señalando que también es competencia de este CGPJ, el control de la actividad desarrollada por los jueces y magistrados en el ejercicio de funciones no jurisdiccionales⁹⁶.

En atención a ello, el artículo 2.2 de la LO 7/2021, excluye del control de las autoridades designadas en su artículo 48.1 (Agencia Estatal de Protección de Datos y de las autoridades autonómicas de protección de datos), el tratamiento de los datos personales realizado por los órganos judiciales y las fiscalías en la actuaciones o procesos de los que sean competentes, al igual que el realizado en el ámbito de gestión de las Oficina judicial y fiscal con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública. Serán las disposiciones de la LO 6/1985, de 1 de julio, del Poder Judicial, las que determinen dicho control⁹⁷.

95 COLOMER HERNÁNDEZ, I., «Control y límites en el uso de los datos personales penales en la investigación...», *op. cit.*, pág. 750.

96 V, más ampliamente la STS 8497/2011, de 2 de diciembre.

97 Es la LO 7/2015, de 21 de julio, por la que se modifica la LO 6/1985, de 1 de julio, del Poder Judicial, la que introduce el Capítulo I bis del título III del Libro III, integrado por los artículos 236 bis a 236 decies, rotulado la Protección de datos de carácter personal en el ámbito de la Administración de Justicia, la que introduce la normativa relativa a estas cuestiones, normativa que es actualizada posteriormente por la L.O. 7/2021, de 26 de mayo, que da nueva redacción al artículo 236 decies.

A estos efectos, es obligada una primera referencia al artículo 236 bis LOPJ, que distingue entre el tratamiento de datos con fines jurisdiccionales, y el que se lleva a cabo con fines extrajurisdiccionales, para a continuación establecer en el siguiente precepto, artículo 236 ter, que, en el ámbito de la jurisdicción penal (más técnicamente orden jurisdiccional penal), dicho tratamiento, realizado en la tramitación procesal por los órganos jurisdiccionales, las fiscalías y las oficinas judiciales y fiscales, se regirá por la LO 7/2021, y por las disposiciones del presente Capítulo I bis LOPJ. Por el contrario, cuando se trate de tratamiento con fines no jurisdiccionales, serán de aplicación el Reglamento (UE) 2016/679, la Ley Orgánica 3/2018, y su normativa de desarrollo.

Es el artículo 236 octies LOPJ, el que regula las autoridades encargadas del control del tratamiento, y en consecuencia con lo señalado anteriormente, dispone que, en las operaciones de tratamiento efectuadas con fines jurisdiccionales por los Juzgados, Tribunales, Fiscalías, y las Oficinas judicial y fiscal, corresponderán al Consejo General del Poder Judicial y a la Fiscalía General del Estado⁹⁸, desenvolver las funciones de control establecidas en el precepto. Precisa también que la supervisión del tratamiento de datos personales que no tenga fines jurisdiccionales se llevará a cabo por la AEPD.

Así pues, son tres las autoridades de control sobre el tratamiento de datos personales en la Administración de Justicia, la AEPD y sus equivalentes autonómicos respecto de los datos personales que no tengan fines jurisdiccionales, y el CGPJ y la FGE para los datos personales con fines jurisdiccionales⁹⁹.

2.2. LO 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

2.2.1. Ámbito objetivo y subjetivo de aplicación

La Directiva 2016/680, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades

98 Será la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial la competente para esta función según lo dispuesto en el artículo 236 nonies y la Unidad de Supervisión y Control de Protección de Datos de la FGE, a tenor de artículo 12 n) EOMF.

99 V. más ampliamente ESTÉVEZ MENDONZA, L.M.^a, «Luces y sombras en la protección de datos personales en las investigaciones penales: perspectiva española» en *Investigación y proceso penal en el siglo XXI. Nuevas tecnologías y protección de datos* (Pereira Puigvert y Ordoñez Ponz, dirs), Editorial Aranzadi, Cizur Menor (Navarra), págs. 669-687. FRIAS MARTÍNEZ, E., «Ficheros jurisdiccionales. Autoridad de control» en *Diario La Ley*, número 9986, 11 de Enero de 2022, <https://laleydigital-laleynext-es.ezbusc.usc.gal/Content/Documento.aspx>.

competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, estableció, en su artículo 63, el plazo para su transposición al ordenamiento jurídico de los Estados miembros, fijando el 6 de mayo de 2018, como fecha límite para dar cumplimiento a ese mandato. España incumple el plazo señalado, y el TSJUE condena a nuestro país con una multa, en la que se incluye una cuantía de partida y otra periódica que se debe computar diariamente desde la notificación de la sentencia¹⁰⁰.

Finalmente, la trasposición de la Directiva 2016/680, de protección de datos al Ordenamiento jurídico español, se lleva a cabo por 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. Ante la imposibilidad de abordar un análisis exhaustivo de la citada norma, se opta por poner de relieve aquellos aspectos de especial interés teniendo en cuenta la finalidad de este trabajo.

El objeto de la Ley se recoge en su artículo 1 y es, como ya se desprende del título *«...establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública»*.

Un dato a resaltar, es que la protección de datos personales de las personas físicas, no sólo se predica en la fase de investigación y enjuiciamiento de un proceso penal, sino también en las actuaciones a prevención realizadas por las autoridades competentes, básicamente por los miembros y fuerzas de la seguridad del Estado. Es importante poner de relieve la referencia a este tipo de intervenciones, y relacionarlas con el tratamiento de datos por la policía en aquellas diligencias que se llevan a cabo con anterioridad al inicio del proceso, e incluso a la comisión de actuaciones delictivas, y ello por su posible repercusión en la fase de instrucción del proceso y en la fase probatoria desarrollada en el juicio oral.

El ámbito de aplicación se recoge en el artículo 2, que lo regula en relación con el tratamiento automatizado total o parcial de datos personales, así como con su tratamiento no automatizado, con la finalidad de su inclusión en un fichero para los fines descritos en el precepto anterior. Sin embargo, en el segundo apartado del artículo, el legislador dispone una precisión respecto al tratamiento *«de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de las actuaciones o procesos*

100 V. STJUE 25 de febrero de 2021 (Asunto C-658/19 Comisión/España), <https://eur-lex.europa.eu/legal-content>

de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal», señalando que dicho tratamiento, esto es, el llevado a cabo con fines jurisdiccionales, se regirá por las disposiciones de la LOPJ, las leyes procesales que resulten aplicables y por EOMF, sin perjuicio de la aplicación de la LOPDPP. En consecuencia, y como ya se ha apuntado, las autoridades de protección de datos a las que se refiere el capítulo VI (AEPD y las autoridades autonómicas), no serán competentes para el control de este tipo de operaciones.

En relación con los sujetos cuyos datos pueden ser objeto de tratamiento y que también se integran en los grupos protegidos por la norma, se trata de personas físicas que se encuentren en alguna de las categorías previstas en el artículo 9: a) Personas respecto de las cuales existan motivos fundados para presumir que hayan cometido, puedan cometer o colaborar en la comisión de una infracción penal; b) Personas condenadas o sancionadas por una infracción penal; c) Víctimas o afectados por una infracción penal o que puedan serlo; d) Terceros involucrados en una infracción penal como son: personas que puedan ser citadas a testificar en investigaciones relacionadas con infracciones o procesos penales ulteriores, personas que puedan facilitar información sobre dichas infracciones, o personas de contacto o asociados de una de las personas mencionadas en las letras a) y b). Como puede fácilmente comprobarse el precepto es una reproducción prácticamente literal de los previsto en el artículo 6 de la Directiva 2016/680.

Finaliza el precepto estableciendo que las actuaciones de tratamiento no deben impedir la aplicación de la presunción de inocencia del artículo 24 CE. Si bien esta aclaración puede resultar obvia, en realidad puede no serlo tanto, al estar reivindicando la aplicación de la presunción de inocencia no sólo en las actuaciones de investigación derivada de la incoación de un proceso penal, si no también, en todas aquellas actuaciones previas, preprocesales, que se integran en las labores policiales a prevención o incluso predictivas¹⁰¹.

2.2.2. Autoridades responsables del tratamiento y autoridades independientes de control

Es necesario diferenciar entre las autoridades competentes para el tratamiento de los datos personales, y las autoridades independientes que tienen encomendado el control del tratamiento. En el primer caso, autoridades competentes para el tratamiento, se recogen en el artículo 4 de la Ley, que encarga dicho tratamiento a las Fuerzas y Cuerpos de Seguridad; las Administraciones Penitenciarias; la Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria; el Servicio Ejecutivo de la

101 GUZMÁN FLUJA, V., «Ideas para un debate sobre la predicción del crimen» en *Inteligencia artificial legal y Administración de Justicia...*, op. cit., pág. 332.

Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y la Comisión de Vigilancia de Actividades de Financiación del Terrorismo. Para el tratamiento de datos personales con fines jurisdiccionales se consideran autoridades competentes, las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal.

En el segundo caso, son autoridades independientes de control, la AGEPD y las autoridades autonómicas, y en relación con el tratamiento de los datos con fines jurisdiccionales, tal y como ya se ha puesto de relieve en páginas anteriores, el CGPJ y la FGE, más concretamente, la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial y la Unidad de Supervisión y Control de Protección de Datos de la FGE.

Si ponemos el foco de atención en el responsable del tratamiento, habrá que acudir al artículo 5.1 de la Ley que lo define en la letra g) como *«la autoridad competente que sola o conjuntamente con otras, determine los fines y medios del tratamiento de datos personales; en caso de que los fines y medios del tratamiento estén determinados por el Derecho de la Unión Europea o por la legislación española, dichas normas podrán designar al responsable del tratamiento, o bien los criterios para su nombramiento»*. Resulta obvio que este responsable es el competente para la toma de decisiones sobre los fines del tratamiento y los medios que se utilicen, siendo por tanto el encargado de vigilar el cumplimiento de los mandatos de la Ley, y de la aplicación de las garantías previstas. Además, en la letra h) del precepto se hace referencia al encargado del tratamiento, que es la *«persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento»*, será por tanto la que efectúe directamente el tratamiento bajo las instrucciones y supervisión del responsable.

Llegados a este punto, y por lo que tiene de interés para este trabajo, se hace ineludible dedicar la atención a la función de la policía judicial como autoridad competente que puede erigirse como responsable, o como encargado del tratamiento de los datos personales. Y en este papel también es importante diferenciar cuando se encuentra realizando labores a prevención, o de investigación delictiva preprocesal, y cuando lleva a cabo diligencias de investigación en el marco de un proceso penal.

En el primer caso, investigación preprocesal o actuaciones a prevención, la policía actúa con plena autonomía, fijando la finalidad de su actuación, los medios técnicos que han de asignarse, los datos personales que deben tratarse y las condiciones y garantías que han de observarse en ese tratamiento. Asume las funciones de responsable del tratamiento, encargando a miembros del cuerpo, el desarrollo efectivo del tratamiento. En el segundo caso, las unidades policiales actúan bajo la dirección del juez instructor, o del Ministerio Fiscal, en su caso, que son los responsables del tratamiento, mientras que los miembros del cuerpo son los encargados de realizar el tra-

tamiento encargado por la autoridad judicial o fiscal. Carecen de autonomía y se encuentra bajo la supervisión y control de estas autoridades¹⁰².

2.2.3. Principios relativos al tratamiento de datos personales. Calidad de los datos

El artículo 6 LOPDP regula los fines legítimos, y por tanto protegidos legalmente, en atención a los que puede permitirse el tratamiento de datos personales, señalando que dicho tratamiento se ha de llevar a cabo de forma lícita y leal, lo que exige la intervención de las autoridades responsables y encargadas y de acuerdo con los fines descritos en el artículo 1 de la Ley, además de realizarse bajo las reglas de la buena fe; los datos personales han de recogerse para fines determinados, legítimos y concretos; la selección de datos será la adecuada para los fines que se persiguen; esos datos han de ser exactos y estar actualizados, y se conservarán de forma que permitan identificar al interesado durante el tiempo necesario para el fin previsto. Finalmente, el tratamiento se realizará garantizando la seguridad de los datos, y adoptando las medidas necesarias para evitar un tratamiento no autorizado, y la pérdida, destrucción o daño accidental.

Teniendo en cuenta la importancia de la utilización de los sistemas de inteligencia artificial en el proceso penal, y partiendo del hecho incuestionable de que dichos sistemas funcionan con datos, es importante hacer una breve referencia a la calidad de los datos que se han de introducir en el sistema. La alta calidad de los datos es esencial para el buen funcionamiento de la IA, por ello, los responsables del tratamiento deberán controlar que los datos utilizados sean los más adecuados y completos, que estén actualizados y que sean exactos. Así se recoge en el artículo 10 LOPDP, que encarga al responsable del tratamiento la supervisión de la calidad de los datos, y la «...distinción entre datos personales basados en hechos y los basados en apreciaciones personales». Además, el precepto encarga a la autoridad responsable, la adopción de las medidas adecuadas para que los datos que no sean exactos, actuales o completos no se transmitan, ni se pongan a disposición de terceros, adoptando las actuaciones necesarias para su eliminación en la medida de lo posible, o en su caso, para el traslado de la información para que se valore su naturaleza.

Es evidente que los datos pueden obtenerse de fuentes variadas, públicas y privadas, todas ellas sometidas a la legislación relativa a la protección de datos. En relación a los datos que se han de introducir en el sistema inteligente y su selección, no es tan importante la cantidad de datos que se sumi-

102 MONTORO SÁNCHEZ, J.A., «La obtención y tratamiento de datos de carácter personal con fines penales por la policía judicial» en *Uso de la información y de los datos personales...*, pág. 637.

nistran como su calidad y representatividad. Por tal motivo, resulta obligado para la garantía del tratamiento la identificación de la fuente y su ubicación temporal y espacial¹⁰³.

A la calidad de los datos hace referencia el artículo 10 REIA que establece unos parámetros de referencia en los apartados dos a cinco. En el segundo apartado alude a las prácticas de gobernanza y gestión de los datos, que han de adecuarse a la finalidad prevista para el sistema, precisando que las citadas prácticas se centrarán en:

- a) *las decisiones pertinentes relativas al diseño;*
- b) *los procesos de recogida de datos y el origen de los datos y, en el caso de los datos personales, la finalidad original de la recogida de datos;*
- c) *las operaciones de tratamiento oportunas para la preparación de los datos, como la anotación, el etiquetado, la depuración, la actualización, el enriquecimiento y la agregación;*
- d) *la formulación de supuestos, en particular en lo que respecta a la información que se supone que miden y representan los datos;*
- e) *una evaluación de la disponibilidad, la cantidad y la adecuación de los conjuntos de datos necesarios;*
- f) *el examen atendiendo a posibles sesgos que puedan afectar a la salud y la seguridad de las personas, afectar negativamente a los derechos fundamentales o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión, especialmente cuando las salidas de datos influyan en las informaciones de entrada de futuras operaciones;*
- g) *medidas adecuadas para detectar, prevenir y mitigar posibles sesgos detectados con arreglo a la letra f);*
- h) *la detección de lagunas o deficiencias pertinentes en los datos que impidan el cumplimiento del presente Reglamento, y la forma de subsanarlas.*

También precisa el precepto en sus apartados tres, cuatro y cinco que el conjunto de datos han de ser suficientemente representativos y en la medida de lo posible carecerán de errores y han de ser completos en atención a la finalidad prevista. Además, recoge que deberá tenerse en cuenta para la selección del conjunto de datos, y en atención a la finalidad prevista, «...los elementos particulares del entorno geográfico, contextual, conductual o funcional específico en el que está previsto que se utilice el sistema de IA de alto riesgo».

103 ARIZA COLMENAREJO, M^a.J. «Fuentes de datos al servicio de sistemas de inteligencia artificial dirigidos a la toma de decisiones judiciales» en *Inteligencia artificial y proceso penal: un reto para la Justicia*, (Castillejo Manzanares/Noya Ferreiro, dirs.), Aranzadi, Cizur Menor (Navarra), 2023, pág. 34.

Es importante precisar la importancia de la representatividad de la muestra, esto es, que la selección de los datos abarque aquellos que resulten más representativos respecto de la finalidad que se persigue. Esta importancia se fundamenta en que el funcionamiento del sistema y el resultado que va a proporcionar deriva de los elementos que se introducen. Obviamente, esta es una tarea que corresponde realizar a los responsables del tratamiento, que no sólo han de seleccionar los datos, sino también etiquetarlos de forma correcta. A través de su etiquetación se va a clasificar el número de datos y se les asignará un valor, que podrá ser examinado por el sistema, y a la hora de relacionar y cruzar los datos introducidos, ese valor se estimará respecto del conjunto. Si este procedimiento no se realiza correctamente el resultado no podrá ser fiable¹⁰⁴.

En esta selección será conveniente adoptar las medidas necesarias para garantizar que la relación de datos respeta los valores y principios previstos en la normativa nacional y de la Unión Europea, fundamentalmente respecto de la seguridad y la protección de los derechos fundamentales¹⁰⁵.

La intervención humana en la etiquetación es incuestionable, y de sus conocimientos específicos sobre el objeto y finalidad de la utilización de los sistemas de inteligencia artificial, junto con la objetividad en el procedimiento de selección, va a depender la fiabilidad del sistema y del resultado proporcionado.

Otra cuestión que debe mencionarse también es la duración de la representatividad de la muestra. Es evidente que el transcurso del tiempo va a afectar claramente a esa representatividad, por lo que será necesario actualizar el sistema cada cierto tiempo, proporcionándole nuevos datos más acordes con la situación temporal.

Una de las ventajas que se han predicado del uso de la inteligencia artificial y su aplicación en el sistema de justicia, es la objetividad de los resultados proporcionados. Sin embargo, partiendo de la incorporación de datos y su selección ha de ponerse de relieve, que el resultado proporcionado por la máquina puede tener los mismos sesgos y perjuicios que el aportado por el ser humano, todo va a depender de la calidad de los datos introducidos en el sistema¹⁰⁶.

104 V. más ampliamente, SAN MIGUEL DEL CASO, C., «Inteligencia artificial y algoritmos: la controvertida evolución de la tutela judicial efectiva en el proceso penal» en *Estudios penales y criminológicos XXXI*, volumen 44, 2023, págs. 1-23.

105 DE HOYOS SANCHO, M., «Premisas y finalidades del Libro Blanco sobre Inteligencia Artificial de la Comisión Europea: perspectiva procesal del nuevo marco regulador», en *Justicia algorítmica y Neuroderecho...*, op. cit., pág.

106 V. SAN MIGUEL DEL CASO, C., «Inteligencia artificial y algoritmos...», op. cit., pág. 7.

2.2.4. Tratamiento de datos integrados en categorías especiales

Es obligada la referencia al tratamiento de aquellos datos que se integran en categorías especiales debido a su incidencia en derechos fundamentales relacionados con la salud, la vida privada, la igualdad y la dignidad de las personas. Se regulan en el artículo 13 de la Ley Orgánica, que hace referencia a los siguientes tipos de datos: los que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, los datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona física, los datos relativos a la salud, a la vida sexual o a la orientación sexual de una persona física.

Su tratamiento requiere una situación de necesidad o, tal y como recoge literalmente la ley «...sólo se permitirá cuando sea estrictamente necesario...», y ha de sujetarse a las garantías que permitan la protección de los derechos y libertades del interesado. También prevé el precepto tres requisitos (o circunstancias como se recoge en la Ley) a observar:

- a) Que se encuentre previsto por una norma con rango de ley, o por el Derecho de la Unión Europea.
- b) Que resulte necesario para proteger los intereses vitales, así como los derechos y libertades fundamentales del interesado, o de otra persona física.
- c) Que, dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

Continúa estableciendo el precepto en su segundo apartado, que «*las autoridades competentes, en el marco de sus respectivas funciones y competencias, podrán tratar datos biométricos dirigidos a identificar de manera unívoca a una persona física con los fines de prevención, investigación, detección de infracciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública*».

Sobre este artículo caben varias reflexiones. En primer lugar, es preciso destacar su indefinición, cuestión ésta que entraña un grave peligro cuando se están regulando actuaciones de investigación en el proceso penal, que pueden incidir en derechos fundamentales de las personas. Señala expresamente que el tratamiento de los datos recogidos en la categoría de especiales (según reza el propio título del precepto), «*sólo se permitirá cuando sea estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado...*».

Pero, ¿a qué se refiere el legislador cuando autoriza su tratamiento «*cuando sea estrictamente necesario*», ¿qué tipo de situaciones pueden permitir la utilización de este tipo de datos? La determinación de esta clase de situaciones, ¿no sería uno de los objetivos de la Ley? En este sentido, no cabe

perder de vista el objeto de esta Ley, que, tal y como recoge su artículo 1, es *«establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública»*, marcando ya una primera limitación a la utilización de los datos de carácter personal.

Así, un primer límite en el tratamiento de los datos personales recogidos en el artículo 13, lo constituye su finalidad: esto es, cuando se trate de actuaciones relativas a la prevención detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales. Por tanto, dentro de este marco de prevención, investigación y enjuiciamiento, será lógico que la ley de desarrollo precise qué tipo de situaciones pueden justificar, por considerarse estrictamente necesario, que se pueda acudir al tratamiento de los datos incluidos en la categoría especial.

Otra cuestión de interés, que también se desprende del precepto, es la vaga alusión a las garantías adecuadas para los derechos y libertades del interesado, redacción que deja un indeterminado abanico de decisiones respecto al tipo de garantías a observar. Pero sin duda, lo más sorprendente es la exigencia del legislador, en el mismo artículo 13, de que en el tratamiento de este tipo de datos se cumplan alguna de las circunstancias que se prevén en el primer apartado. Ya es llamativo que le denomine «circunstancias» y no requisitos, pues en buena técnica legislativa la previsión del tratamiento en una ley no puede calificarse de circunstancia. Pero, además, no se exige el cumplimiento de todas ellas, sino de alguna.

Como se ha señalado supra, pero es necesario reiterar, el precepto permite el tratamiento de estos datos de categoría especiales porque afectan a derechos fundamentales *«...cuando se cumplan alguna de las siguientes circunstancias: a) Que se encuentre previsto por una norma con rango de ley, o por el Derecho de la Unión Europea; b) Que resulte necesario para proteger los intereses vitales, así como los derechos y libertades fundamentales del interesado, o de otra persona física; c) Que, dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos»*.

Quiere ello decir que el tratamiento de estos datos de categoría especial cuando *«...resulte necesarios para la protección de los derechos y libertades del interesado, o de otra persona física o de sus intereses vitales...»*, (circunstancia prevista en la letra b) del primer apartado), se puede realizar sin que se encuentre previsto en una ley (circunstancia prevista en la letra a) del primer apartado), aunque dicho tratamiento interfiera en la situación personal, o en los intereses y derechos de terceros. No parece esta la interpretación más acorde con la protección de los derechos de los ciudadanos en relación a sus datos personales.

Este artículo 13, lo que hace en realidad es trasponer exactamente el contenido del artículo 10 de la Directiva (UE) 2016/680, sin realizar ninguna precisión más, cuando lo que se espera de la Ley orgánica que desarrolla o traspone una directiva, es abordar su contenido con más detalle, y estableciendo los principios o requisitos que garantice su efectividad. Así lo recoge expresamente la propia Directiva, cuando afirma en su considerando número 20 que *«la presente Directiva no impide que, en las normas nacionales relativas a los procesos penales, los Estados miembros especifiquen operaciones y procedimientos de tratamiento relativos al tratamiento de datos personales por parte de tribunales y otras autoridades judiciales, en particular en lo que respecta a los datos personales contenidos en resoluciones judiciales o en registros relacionados con procesos penales»*.

Como resulta obvio, cuando el tratamiento de los datos personales se vincula a su utilización con fines de prevención o de investigación en el proceso penal, las precauciones y cautelas han de ser más estrictas, para dar protección no sólo a los derechos relacionados con la vida privada de los ciudadanos, sino también a todo el conjunto de derechos de naturaleza procesal que se constituyen en los pilares del proceso de un Estado de Derecho (presunción de inocencia, contradicción y derechos de defensa, proceso debido...). Su tratamiento ha de ser regulado de forma completa y precisa, estableciendo un protocolo donde la transparencia y la accesibilidad se respeten a lo largo de todo el procedimiento. Las autoridades independientes de control deberán vigilar la aplicación del procedimiento establecido para la introducción de los datos de carácter personal en el proceso. Se trata de conjugar los derechos fundamentales del ciudadano, frente el derecho a la investigación penal por parte del Estado¹⁰⁷.

2.2.5. Tratamiento de los datos obtenidos de las cámaras de videovigilancia policiales

Ya es habitual la instalación por la policía en espacios públicos de las conocidas cámaras de videovigilancia, que en la mayoría de las ocasiones pretenden garantizar la seguridad de los ciudadanos, o bien vigilar el cumplimiento de las normas de tráfico. Lo importante para este estudio, es determinar el destino que se puede dar a las imágenes obtenidas y en qué condiciones han de grabarse.

A esta cuestión responde la regulación de los artículos 15 y siguientes en la LOPDPP, que recoge las normas sobre el tratamiento de los datos personales por los Cuerpos y Fuerzas de la Seguridad del Estado, en el ámbito de la videovigilancia. Lo primero que cabe destacar es que la obtención de estas

107 ESPARZA LEIBAR, I., «Derecho fundamental a la protección de datos de carácter personal...», *op. cit.*, pág. 201.

imágenes tiene lugar en espacios públicos. No se regula en esta norma, ni tampoco en la Ley procesal penal, la toma de imágenes en espacios privados, salvo aquellas que se permiten con la instalación de dispositivos para la intervención de las comunicaciones orales directas, reguladas en los artículos 588 quater y siguientes LECrim. El artículo 588 quinquies LECrim prevé la captación por la policía de imágenes de una persona que está siendo objeto de una investigación, pero «...cuando se encuentre en un lugar o espacio público...», condicionando la captación a que resulte necesaria para su identificación, o para la localización de instrumentos o efectos del delito, o para obtener datos relevantes para el esclarecimiento de los hechos. En determinadas circunstancias, previstas en el segundo apartado del precepto, se permite también la grabación de terceros.

La regulación del artículo 588 quinquies LECrim, autoriza a la policía judicial a captar las imágenes en espacios públicos, sin exigir la autorización judicial previa. A sensu contrario, puede mantenerse que dicha autorización judicial previa podrá levantar la protección de los derechos fundamentales citados, y servir a la policía como licencia o permiso para proceder a la captación de las imágenes en espacios privados. Obviamente, en estos casos se requiere la existencia de un proceso penal en curso¹⁰⁸.

La instalación de cámaras fijas se realizará conforme a lo establecido en la LO 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos y su Reglamento de desarrollo, siendo también de aplicación el artículo 16.3 LO 7/2021. Por su parte, la instalación de dispositivos móviles se llevará a cabo conforme a lo dispuesto en el artículo 17.1 de la citada LO 7/2021.

El artículo 16 LOPDPP, en su segundo apartado, recoge los fines u objetivos (criterios señala el legislador) que permiten la instalación de estos dispositivos fijos, colocando el principio de proporcionalidad como garante de la actuación de las fuerzas policiales. De esta forma, uno de los objetivos que recoge el precepto es «...detectar o investigar la comisión de infracciones penales y la protección y prevención frente a las amenazas contra la seguridad pública». La valoración de la proporcionalidad de la instalación por el responsable del tratamiento, exige tener en cuenta la idoneidad del dispositivo, esto es que su instalación sea adecuada para el fin que se persigue, la intervención mínima y la ponderación de los intereses en conflicto, que exige valorar los perjuicios causados a los ciudadanos en relación con la finalidad perseguida.

En el caso de los dispositivos móviles, previstos en el artículo 17 LOPDPP, su autorización se encomienda al Delegado o Subdelegado del gobierno,

108 V. más ampliamente ARIZA COLMENAREJO, M^a.J., «Garantías procesales en el uso de drones en la investigación penal», en *Era digital, sociedad y Derecho* (Fuentes Soriano, dir.), Tirant lo Blanch, Valencia, 2020, pág. 331.

para un evento concreto o en caso de peligro que se intenta evitar, debiendo valorarse las circunstancias concretas en cada caso. Su instalación no tendrá carácter indefinido y dependerá de las circunstancias específicas del evento, estableciendo, el segundo apartado, el límite de un mes prorrogable por otro. Como no puede ser de otra forma, las cámaras móviles requieren un mayor control y exigencia para su instalación, debido a que también suponen una injerencia más grave, o de mayor intensidad, en la esfera personal de los ciudadanos¹⁰⁹.

A tenor del artículo 18 de la Ley 7/2021, cuando las cámaras instaladas graben la comisión de hechos que pudieran calificarse de delictivos, los soportes originales se podrán a disposición de la autoridad judicial en el plazo más breve posible y «...*en todo caso, en el plazo máximo de setenta y dos horas desde su grabación*». Cuando no pueda redactarse en ese plazo el correspondiente atestado, se informará verbalmente a la autoridad judicial o del Ministerio Fiscal, poniendo el soporte original a su disposición.

109 DE LEMUS VARA, F.J., «Límites para el tratamiento de los datos de los no investigados en el proceso penal», en *Uso de la información...*, op. cit., pág. 562.

CAPÍTULO II

DERECHOS FUNDAMENTALES E INTELIGENCIA ARTIFICIAL

1. La investigación con sistemas de inteligencia artificial y la protección de los derechos fundamentales relacionados la vida privada. Especial referencia al derecho a la protección de datos personales y al entorno virtual

1.1. Inteligencia artificial y derechos fundamentales

La aplicación de los sistemas de Inteligencia Artificial en la Administración de Justicia, y más concretamente en la justicia penal, ha de partir de los documentos internacionales de protección de los derechos fundamentales, y del respeto a los principios democráticos y al Estado de Derecho. Centrando este análisis en los textos internacionales de la Unión Europea, una primera referencia ha de hacerse a la Carta de los Derechos Fundamentales, de 18 de diciembre de 2000, revisada en diciembre de 2007, y jurídicamente vinculante a partir del Tratado de Lisboa en 2009¹¹⁰. Su preámbulo recoge expresamente que *«consciente de su patrimonio espiritual y moral, la Unión está fundada sobre los valores indivisibles y universales de la dignidad humana, la libertad, la igualdad y la solidaridad, y se basa en los principios de la democracia y el Estado de Derecho. Al instituir la ciudadanía de la Unión y crear un espacio de libertad, seguridad y justicia, sitúa a la persona en el centro de su*

110 La Carta de los Derechos Fundamentales de la Unión Europea proclamada por el Parlamento europeo, el Consejo y la Comisión, en Niza en diciembre de 2000, fue revisada en diciembre de 2007 (DO C 303 de 14.12.2007, p. 1), y se encuentra en vigor desde diciembre de 2009, fecha de la entrada en vigor del Tratado de Lisboa. Conforme a lo dispuesto en el artículo 6, apartado 1, párrafo primero, del Tratado de la Unión Europea, la Carta proclamada en 2007 tiene el mismo valor jurídico que los Tratados. <https://www.boe.es/buscar/doc>.

actuación». Después de esta alusión a los fines y valores de la Unión, continúa señalando que, para preservar esos fines y valores y darles mayor protección, es necesario «...*reforzar la protección de los derechos fundamentales a tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos*».

Dentro de esta misma línea, se enmarca la Carta Ética Europea sobre el uso de la Inteligencia Artificial en los Sistemas Judiciales y su entorno¹¹¹, que trata de garantizar el respeto a los derechos protegidos en el Convenio Europeo de Derechos Humanos¹¹². En este documento, al que se ha hecho alusión en el primer capítulo, se analiza la incorporación de aplicaciones de IA al proceso, poniendo de relieve algunas de las cautelas que han de presidir su utilización en el proceso penal, para preservar el derecho a un proceso justo. Son cinco los pilares sobre los que se construye este sistema de protección: el respeto de los derechos fundamentales, la no discriminación, la calidad y seguridad, la transparencia, la imparcialidad y equidad, y el control del usuario¹¹³.

Como ya se ha puesto de relieve, también el Reglamento Europeo de Inteligencia Artificial refuerza y promueve la protección de los derechos fundamentales reconocidos en la Carta de Derechos Fundamentales de la UE, y por lo que nos interesa, el derecho a la dignidad humana (artículo 1), el respeto de la vida privada y familiar y la protección de datos de carácter personal (artículos 7 y 8), la no discriminación (artículo 21) y la igualdad entre hombres y mujeres (artículo 23). Además, en su objetivo está garantizar el derecho a la tutela judicial efectiva y a un juez imparcial, a la presunción de inocencia y los derechos de la defensa (artículos 47 y 48).

En este mismo sentido, se pronuncia la Agencia de los Derechos Fundamentales de la UE¹¹⁴, que identifica como riesgo principal en la aplicación de sistemas de IA, la afectación a los derechos fundamentales a la igualdad, a la intimidad y a la tutela judicial efectiva. Considera la Agencia, que la opacidad relacionada con el funcionamiento de este tipo de instrumentos, supone

111 Adoptada por la Comisión Europea para la Eficacia de la Justicia (CEPEJ) en Estrasburgo, diciembre de 2018. <https://www.pj.gob.pe/wps/wcm/connect>

112 V. sobre la importancia de los derechos humanos considerados como derechos que desarrollan la inteligencia de los individuos y hacen a las sociedades más inteligentes, v. MARTÍNEZ GARCÍA J. I., «Inteligencia y derechos humanos en la sociedad digital» en *Cuadernos electrónicos de Filosofía del Derecho*, número 40, 2019, págs. 168 y ss.

113 V. más ampliamente BARONA VILAR, S., *Algoritmización del derecho y de la justicia...*, op. cit., 2021, págs. 144 y 145.

114 La Agencia de los Derechos Fundamentales de la UE, es un organismo creado en 2007 que asesora a las instituciones de la UE y los gobiernos nacionales en materia de derechos fundamentales, concretamente en los siguientes aspectos: Discriminación, Acceso a la justicia, Racismo y xenofobia, Protección de datos, Derechos de las víctimas y Derechos del niño. La agencia tiene como objetivo ayudar a promover y proteger más eficazmente los derechos fundamentales en la UE.

un riesgo indudable para el ejercicio del derecho a la tutela judicial efectiva, por lo que habrá que proporcionar a los ciudadanos la información necesaria sobre su utilización en la toma de decisiones, y sobre la forma de acceder al contenido del sistema y a su funcionamiento¹¹⁵.

También el Consejo de la Unión Europea se ha preocupado de garantizar los principios y derechos que rigen en los Estados de la Unión, instando en sus conclusiones de 21 de octubre de 2020, «*a afrontar la opacidad, la complejidad, el sesgo, cierto grado de imprevisibilidad y un comportamiento parcialmente autónomo de ciertos sistemas de IA, para garantizar su compatibilidad con los derechos fundamentales y facilitar la aplicación de las normas jurídicas*».

En definitiva, la implantación de la IA y su constante evolución hacia nuevas aplicaciones, exige una regulación que vaya más allá de los principios éticos exigibles, y se convierta en una normativa completa, vinculante e imperativa, que permita la protección de los derechos fundamentales y del Estado de Derecho.

La protección de los derechos fundamentales de los ciudadanos ha centrado también la posición del Consejo de Europa, alertando de las posibles consecuencias negativas de la implantación de los sistemas de inteligencia artificial. En 2019 estableció las bases para que la introducción de los instrumentos de inteligencia artificial, no afectara de forma negativa al sistema de derechos humanos, y al correcto funcionamiento del Estado de Derecho. Entre las conclusiones de la Conferencia sobre esta materia, celebrada en Helsinki en febrero de 2019, se encuentran referencias al diseño, el desarrollo y el despliegue de las herramientas de IA, precisando que deben ser objeto de una evaluación de riesgos conforme a los principios aplicables. Todos los procesos automatizados deben ser diseñados para que puedan ser examinados por un revisor humano. En todos los casos en que se alegue la existencia de violaciones de los derechos humanos, deben existir recursos eficaces en el marco de las competencias públicas y privadas. La transparencia algorítmica es crucial para crear confianza y garantizar la debida protección de los derechos¹¹⁶.

Resulta evidente que el sistema de justicia, y especialmente de justicia penal, no es ajeno, ni debe serlo, a la introducción de los avances tecnológicos y de los instrumentos de IA. Así lo demuestra el día a día de cualquier investigación criminal¹¹⁷. Junto al examen de las huellas, muestras y vesti-

115 SCHUMANN BARRAGÁN, G., «La inteligencia artificial aplicada al proceso penal desde la perspectiva de la UE», en *Investigación y proceso penal en el siglo XXI*, op. cit., pág. 12.

116 V. sobre esta cuestión, «El Consejo de Europa crea un Comité para impulsar la regulación de la Inteligencia artificial» en <https://elconsultor.laley.es>, 13 de septiembre de 2019.

117 GASCÓN INCHAUSTI, F., «Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial», en *La justicia digital en España y la Unión Europea*, (Conde Fuentes/Serrano Hoyo, dir.), Editorial Atelier, Barcelona, 2019, pág. 192.

gios encontrados en el lugar de comisión del hecho delictivo, análisis que se llevan a cabo utilizando instrumentos de procesamiento avanzado de datos, se analizan y estudian ahora los datos y la información que se puede encontrar en los dispositivos electrónicos del investigado y su entorno. La ubicación de un sujeto en un lugar concreto y determinado, y la determinación de su perfil, o conjuntos de rasgos que configuran su personalidad¹¹⁸, a efectos de identificarlo y sujetarlo a la investigación penal, no resulta ya nada extraño, y cada vez se puede llevar a cabo con más facilidad, utilizando los datos proporcionados no sólo por el sujeto investigado, sino también por dispositivos de otras personas que ha utilizado, o que se encontraban en su entorno.

En este sentido, la conservación de los datos almacenados por estos dispositivos, y su análisis cruzado por aplicaciones informáticas que ejecutan el tratamiento de los llamados Big Data, permiten avances muy importantes en la investigación criminal¹¹⁹. No obstante, son muchas las voces que se pronuncian en contra del uso indiscriminado de este tipo de aplicaciones que inciden en los derechos fundamentales de los individuos, fundamentalmente en el derecho a la intimidad, la protección de datos personales y la vida privada en general, además de aquellos derechos fundamentales de naturaleza procesal que se tratarán en un epígrafe posterior¹²⁰.

El artículo 18 CE recoge aquellos derechos fundamentales que tienen en común la protección de la vida privada de los ciudadanos. El derecho al honor, el derecho a la intimidad, el derecho a la propia imagen, la inviolabilidad del domicilio, el secreto de las comunicaciones personales, y el ahora conocido como derecho al entorno digital, se convierten en el escudo protector de la esfera privada. Como derechos fundamentales consagrados constitucionalmente, su limitación ha de realizarse por ley orgánica que especifique los supuestos, requisitos, procedimiento y, en definitiva, las garantías que han de rodear una posible injerencia.

118 Sobre la elaboración de perfiles han de tenerse en cuenta las limitaciones reguladas en el REIA y en la Directiva 2016/680.

119 Sobre esta cuestión, v. ORTIZ PRADILLO, J.C., «Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos fundamentales en el proceso penal», *La ley digital*, de 25 de enero de 2022, pág. 2 y ss.

120 V. más ampliamente, COLOMER HERÁNDEZ/OUBIÑA BARBOLLA (directores) *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Aranzadi, Cizur Menor (Navarra), 2015; VELASCO NUÑEZ, E., «Investigación penal y protección de datos» en *El Cronista del Estado Social y Democrático de Derecho*, número 88-89, 2020.

1.2. La incidencia de la inteligencia artificial en los derechos fundamentales a la intimidad, a la inviolabilidad del domicilio y al secreto de las comunicaciones¹²¹

1.2.1. La incidencia en el derecho a la intimidad

Inicialmente, la obtención de material incriminatorio derivado del uso de las llamadas «aplicaciones inteligentes» se empezó relacionando con su incidencia en el derecho a la intimidad, en el derecho a la inviolabilidad del domicilio, o en el derecho al secreto de las comunicaciones.

En este sentido, se diferenciaba entre aquellas actuaciones policiales que requerían una autorización judicial previa (arg. ex art. 18.2 y 3 CE), cuando se trataba de una injerencia en el derecho a la inviolabilidad del domicilio, o en el derecho al secreto de las comunicaciones, y la no exigencia de dicha autorización previa cuando se afectaba al derecho a la intimidad.

Siguiendo esta corriente, el Tribunal Supremo se ha ocupado, en una primera etapa, de fijar las pautas a seguir en diligencias policiales de investigación en las que se utilizaban instrumentos de IA, con la finalidad de garantizar la protección de los derechos fundamentales y libertades públicas, preservando al mismo tiempo la investigación policial preprocesal, y la desarrollada en la fase de instrucción. En esta primera línea jurisprudencial, tal y como se verá, el Tribunal consideraba que la utilización de aquellos instrumentos que podían incidir en el derecho a la intimidad, no siempre requería un pronunciamiento judicial previo.

Sin embargo, en sus últimas resoluciones, y principalmente como consecuencia de la regulación en la Ley procesal penal de las diligencias de investigación tecnológica, trata de acotar las injerencias en derechos que protegen la vida privada de las personas, restringiendo, o limitando, las actuaciones policiales que puedan considerarse una vulneración de estos derechos fundamentales. Igual tendencia sigue la evolución legislativa, y así han de entenderse las garantías que se recogen en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, que establece el régimen jurídico aplicable a la investigación por medios tecnológicos, y que marca un antes y un después en los requisitos que se han de observar en la investigación que utilice este tipo de instrumentos.

¹²¹ Las abundantes aportaciones jurisprudenciales y doctrinales sobre la naturaleza, contenido y protección de estos derechos fundamentales, eximen de abordar un análisis extenso, que llevaría a posiciones ya de sobra conocidas, por lo que su tratamiento sólo se realizará respecto a cuestiones puntuales relacionadas con la utilización de instrumentos tecnológicos vinculados a la inteligencia artificial.

Sin duda, el progreso tecnológico y la evolución de las aplicaciones de inteligencia artificial, hacen cada vez más difícil preservar la vida privada de los ciudadanos, lo que ha provocado los cambios legislativos y jurisprudenciales de los últimos años, respecto de la utilización de estas aplicaciones en la investigación penal. Además, los dispositivos inteligentes son cada vez más avanzados. Los instrumentos que antes se utilizaban para determinar la ubicación de una persona, o para intervenir sus comunicaciones, se están sustituyendo por otros más sofisticados que permiten fijar la ubicación, y al mismo tiempo intervenir las comunicaciones, o penetrar en el espacio inviolable del domicilio captando imágenes de su interior. A esta evolución ya hace referencia el Tribunal Supremo cuando afirma que *«...los datos de geolocalización pueden obtenerse, en principio, mediante procedimientos distintos, como recuerda la doctrina, nuestra práctica procesal penal suele aludir a ellos mediante el término genérico de "balizas", vocablo en el que parecen quedar integradas diferentes modalidades tecnológicas: las que utilizan GPS, las basadas en módulos de satélite independientes (sistema alpha), las basadas en radiofrecuencia, las basadas en la comunicación de GSM (telefonía móvil) o los dispositivos de descarga de localización (Qlog). Muchas son las funcionalidades de tales sistemas de geolocalización y muchas también las singularidades técnicas que define cada uno de ellos. De ahí que la regulación del nuevo art. 588 quinquies b) en su apartado 2º se exige que la autoridad judicial especifique "...el medio técnico que va a ser utilizado". Por tanto lo que contempla este precepto es la instalación de un dispositivo técnico que, durante un plazo determinado, permita conocer las coordenadas geográficas en las que se sitúa el investigado con independencia de que se valga o no de un equipo determinado para sus comunicaciones electrónicas»*¹²².

En los últimos años, el Tribunal Supremo ha modificado su doctrina jurisprudencial relativa a la protección de los derechos previstos en el artículo 18 CE, principalmente en relación con el derecho a la intimidad. Esta variación se produce, fundamentalmente, en atención a dos cuestiones importantes que han provocado pronunciamientos más restrictivos sobre las injerencias en la vida privada de los ciudadanos. De un lado, la utilización en la investigación de instrumentos tecnológicos y relacionados con la inteligencia artificial, que suponen una invasión en la vida privada de una entidad hasta ahora desconocida. De otro, los efectos de la aplicación de las disposiciones relativas a las diligencias de investigación tecnológica, introducidas por la LO 13/2015, de modificación de la Ley de Enjuiciamiento Criminal.

Es evidente, que la citada ley ha supuesto un cambio sustancial en la regulación de las medidas de investigación tecnológica. El tan esperado desarrollo legislativo que estableciera el régimen jurídico aplicable en la limitación de los derechos previstos en el artículo 18 CE¹²³, ve la luz en esta norma, res-

122 STS 291/2021, de 7 de abril.

123 Derecho a la intimidad y a la propia imagen, derecho a la inviolabilidad del domicilio, derecho al secreto de las comunicaciones personales, y al derecho a la protección de datos y al entorno virtual.

pondiendo a las exigencias del Tribunal Europeo de Derechos Humanos¹²⁴. De esta forma, la tantas veces reclamada previsión legislativa, que ha obligado al Tribunal Constitucional y al Tribunal Supremo, a abordar una construcción jurisprudencial para colmar las lagunas de nuestro ordenamiento en materias como la intervención de comunicaciones, se concreta en esta modificación de la Ley procesal penal, que recoge no sólo los presupuestos, requisitos y efectos de las medidas de intervención telefónica, sino que extiende su regulación a la intervención de otro tipo de comunicaciones habituales ya en nuestra sociedad, y a la utilización de dispositivos de seguimiento, localización y captación de imágenes, al igual que el uso de otro tipo de dispositivos informáticos¹²⁵.

Se da, así, cobertura legal a las medidas de investigación tecnológica, empleando el legislador un lenguaje abierto que permite la aplicación de esta regulación a futuros sistemas o instrumentos que se puedan encuadrar en los bloques previstos en la norma: la intervención de las comunicaciones personales; la captación y grabación de comunicaciones orales e imágenes mediante la utilización de dispositivos electrónicos; la utilización de dispositivos técnicos de seguimiento, localización y captación de imágenes; y por último, el registro de dispositivos de almacenamiento masivo de información¹²⁶.

Partiendo de la regulación constitucional del derecho a la intimidad en el artículo 18.1 CE, lo primero que ha de ponerse de relieve es la ausencia de

124 Por todas, SSTEDH de 6 de septiembre de 1978, caso Klass y otros; de 25 de marzo de 1983; caso Silver y otros; de 27 de octubre de 1983, caso Malone; de 30 de julio de 1988, Caso Valenzuela Contreras; de 18 febrero de 2003, Caso Prado Bugallo; de 31 mayo 2005, Caso Vetter; de 1 julio 2008, Caso Liberty y otros.

125 La citada Ley agrupa ahora en el Título VIII del Libro II de la Ley de Enjuiciamiento Criminal, las medidas de investigación limitativas de los derechos reconocidos en el art. 18 CE, distribuyéndolas en diez capítulos. Los dos primeros recogen las medidas de entrada y registro en lugar cerrado. El tercero, las medidas de intervención de la correspondencia escrita y telegráfica. El Capítulo IV, las disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos. El Capítulo V que recoge las intervenciones telefónicas y telemáticas. La medida de captación y grabación de las comunicaciones orales (también denominadas ambientales) a través de la utilización de dispositivos electrónicos se recoge en el Capítulo VI, mientras que el Capítulo VII se ocupa de la medida de captación de la imagen, de seguimiento y de localización por medio de dispositivos técnicos. El registro de dispositivos de almacenamiento masivo de información y el registro remoto sobre equipos informáticos se regulan en los Capítulos VIII y IX. Finalmente, el Capítulo X recoge las denominadas medidas de aseguramiento y la conservación de los datos obtenidos.

126 BUENO DE MATA, F., «La utilización de drones como diligencia de investigación tecnológica: consecuencias probatorias» en *Diario La Ley*, número 16, 20 de Marzo de 2018, <https://diariolaley.laleynext.es/Content/Documento.aspx>, pág. 3.

una exigencia expresa de autorización judicial previa para su limitación. Este hecho marca una importante diferencia a la hora de su interpretación jurisprudencial, en relación con el derecho a la inviolabilidad del domicilio, recogido en el segundo apartado del precepto, y del derecho al secreto de las comunicaciones, previsto en su apartado tercero. En estos dos últimos derechos el legislador constitucional requiere la autorización judicial previa para proceder a su limitación, cuando no exista consentimiento del titular.

Una primera interpretación del Tribunal Supremo sobre este presupuesto se refleja en una resolución dictada con ocasión de pronunciarse sobre la instalación de dispositivos de localización y seguimiento. Considera el Tribunal que cuando la policía no solicita autorización previa, no siempre se produce una vulneración del derecho a la intimidad. Sin embargo, es necesario precisar que esta postura de nuestros tribunales es anterior a la entrada en vigor de la Ley 13/2015.

Consideraba el Tribunal Supremo, en aquel momento, que este tipo de intromisiones no suponían una injerencia sustancial en ese derecho fundamental. Así afirmaba que *«...El uso de radiotransmisores (balizas de seguimiento GPS), para la localización de embarcaciones en alta mar por la policía no vulnera el derecho fundamental al secreto de las comunicaciones o supone una injerencia excesiva sobre el derecho fundamental a la intimidad a los efectos de exigir un control jurisdiccional previo y una ponderación sobre dicha afectación constitucional. Para esta Sala Segunda Tribunal Supremo la ausencia de relevancia constitucional se deriva de que se trata de "diligencias de investigación legítimas desde la función constitucional que tiene la policía judicial, sin que en su colocación se interfiera en su derecho fundamental que requerirá la intervención judicial»*¹²⁷.

En el mismo sentido se pronunciaba la sentencia 489/2018, de 23 de octubre, que se hace eco de la doctrina jurisprudencial del Tribunal Constitucional¹²⁸, para afirmar que *«...Recuerda el Tribunal Constitucional que la intervención de las comunicaciones requiere siempre de autorización judicial, pero el art. 18.1 CE no prevé esa misma garantía respecto del derecho a la intimidad, por lo que se admite la legitimidad constitucional de que la policía realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas sin previa autorización judicial (y sin consentimiento del afectado), siempre que exista la suficiente y precisa habilitación legal y se hayan respetado las exigencias dimanantes del principio de proporcionalidad»*¹²⁹.

127 STS 610/2016, de 7 de julio. V. en el mismo sentido la SSTS 562/2007, de 22 de junio; 523/2008, de 11 de julio; 906/2008, de 19 de diciembre y 798/2013, de 5 de noviembre.

128 STC 115/2013, de 9 de mayo. V. también las SSTC 70/2002, de 3 de abril; 123/2002, de 20 de mayo; 56/2003, de 24 de marzo; 281/2006, de 9 de octubre; 142/2012, de 2 de julio, entre otras.

129 La sentencia citada si bien trata de hechos ocurridos con anterioridad a la entrada en vigor de la Ley 13/2015, ya hace referencia a la protección del derecho a la intimidad depen-

De esta forma, la injerencia de las actuaciones policiales en el derecho a la intimidad era justificada constitucionalmente siempre que cumpliera con los siguientes requisitos: que la medida respondiera a un fin legítimo, como es la investigación delictiva; que la medida adoptada por la policía estuviera contemplada en una norma legal; que la actuación obedeciera a la existencia de una situación de urgencia que justificaba la intervención inmediata; y que se haya respetado el principio de proporcionalidad¹³⁰.

En la misma línea, la jurisprudencia del TEDH permitía también el uso de herramientas tecnológicas sin autorización judicial, aún en aquellos casos en los que se podía producir una injerencia en el derecho a la intimidad, al considerar que se trataba de una injerencia de menor intensidad¹³¹. No obstante, sí consideraba necesario el Tribunal europeo, que la urgencia de la medida y, por tanto, la situación que impedía recabar la autorización judicial, estuviese plenamente justificada¹³².

Pero esta posición jurisprudencial no se predicaba con carácter general, ya que estaba condicionada a la intensidad de la injerencia. La afectación del derecho a la intimidad no siempre era considerada de una entidad suficiente para requerir un pronunciamiento judicial previo. Si bien, en algunas ocasiones, la localización a través de dispositivos de seguimiento no se apreciaba como una injerencia relevante, no ocurría lo mismo con la obtención de información a través del almacenamiento masivo de datos de los ordenadores¹³³.

Así, en algunas resoluciones anteriores a la entrada en vigor de la Ley 13/2015, el Tribunal Constitucional ya ponía de relieve que la información obtenida de un ordenador podía afectar a la esfera más íntima de la persona, por cuanto el rastro dejado por su titular (intervención en foros, fotografías, videos, conversaciones por correo electrónico, descargo de archivos, comercio electrónico y un largo etcétera), si es analizado en su conjunto, proporciona un «...*perfil altamente descriptivo de la personalidad de su titular*». Precisa el Tribunal Constitucional «...*que el ordenador es un instrumento útil para la*

diendo de la intensidad de la injerencia, y al cambio que supone la entrada en vigor de la citada Ley. V. también sobre esta cuestión las SSTS 562/2007, de 22 de junio; 906/2008, de 19 de diciembre; 777/2013, de 7 de octubre; 798/2013, de 5 de noviembre; 489/2018, de 23 de octubre, entre otras.

130 GARCÍA MARCOS, J., «Hacia una exclusiva reserva jurisdiccional en la protección del derecho a la Intimidad» en *Actualidad Civil*, número 4, abril 2024, <https://laleydigital-laleynext-es.ezbusc.usc.gal/Content/Documento.aspx>, pág. 2.

131 V. en este sentido la STEDH de 2 de septiembre de 2010, caso Uzun contra Alemania.

132 Así lo considera en su sentencia de 30 de mayo de 2017, Asunto Trabajo Rueda contra España, en la que se cuestionó que el examen de un ordenador personal por parte de un informático en relación con una investigación de pornografía infantil, obedeciera a razones de urgencia, y que no se pudieran esperar a obtener la correspondiente autorización judicial,

133 V. STS 489/2018, de 23 de octubre.

*emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática, así como de las nuevas tecnologías de la información*¹³⁴.

En este sentido, si bien se refiere a hechos anteriores a la entrada en vigor de la Ley 13/2015, la citada sentencia del Tribunal Supremo 489/2018, ya se hace eco de la diferente protección que ha de otorgarse al derecho a la intimidad, dependiendo del tipo de diligencia, o del sistema que se utilice en la investigación, y que puede provocar una injerencia en ese derecho, y en otros estrechamente relacionados. Así afirma que «...desde la perspectiva del derecho de exclusión del propio entorno virtual, como de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante. Y esa autorización no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentran instalados. De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, el órgano jurisdiccional ha de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como sede física en el que se ejercen los derechos individuales más elementales, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías».

El cambio jurisprudencial que se produce como consecuencia de la entrada en vigor de la Ley 13/2015, es explicado por el propio Tribunal Supremo, que considera que «...El hecho de que nuestro sistema jurídico, hasta la entrada en vigor de la LO 13/2015, 5 de octubre, no haya venido exigiendo autorización judicial para la utilización de este tipo de dispositivos, ha suscitado las dudas propias de todo cambio normativo que obliga a rectificar pautas de actuación policial, hasta ahora validadas por la jurisprudencia de esta Sala. El aval otorgado por el TEDH a aquellos modelos constitucionales que no condicionan la validez de la injerencia a la obtención de autorización judicial, alienta la controversia y refuerza la argumentación de quienes ven en la utilización de este tipo de dispositivos una injerencia de menor intensidad en el ámbito de la intimidad protegida constitucionalmente. (...)»¹³⁵.

134 STC 173/2011, 7 de noviembre.

135 STS 835/2022, de 21 de octubre.

Una vez promulgada la Ley 13/2015, es la sentencia 141/2020, de 13 de mayo, la que recoge de forma exhaustiva los requisitos y garantías que, a partir de su regulación, habrán de observarse también para la instalación de dispositivos de localización. En este sentido, ha señalado el alto Tribunal 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, más allá de que, conforme a la jurisprudencia constitucional y de esta Sala, existan actos de injerencia que, sin estar expresamente reservados a la autorización judicial, pueden ser plenamente válidos al perseguir un fin constitucionalmente legítimo en una sociedad democrática. 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»*¹³⁶.

Para el Tribunal, el riesgo que afecta al derecho a la intimidad con la utilización de estos instrumentos de localización y seguimiento, no está en determinar la posición de la persona sujeta a la investigación policial, sino en que, a través de sucesivas localizaciones derivadas de dicho seguimiento, se pueden deducir costumbres, preferencias, opciones políticas o ideológicas, y por tanto, pueden llegar a determinarse los rasgos de la personalidad del sujeto¹³⁷.

La misma línea argumental se mantiene, con ocasión del análisis de la regulación relativa a la instalación de los dispositivos o medios de geolocalización, conforme a lo autorizado por el artículo art. 588 quinquies b) LECrim, al entender que el régimen jurídico ha de seguir las mismas garantías y requisitos que el establecido para la intervención de las comunicaciones personales. Así, considera que si bien es cierto que *«...a diferencia de lo que acontece con otras medidas de injerencia (arts. 588 ter a) ó 588 quater b))*, la nueva regulación no hace explícito un juicio de proporcionalidad. El legislador no se ocupa de definir parámetros cuantitativos o cualitativos de gravedad del delito que esté siendo objeto de investigación. Este silencio no puede interpretarse, sin embargo, como una relajación de las exigencias constitucionales proclamadas por el art. 588 bis a). Los principios de proporcionalidad, necesidad y excepcionalidad siguen actuando como presupuestos de legitimidad, cuya concurrencia ha de quedar expresamente reflejada en la resolución judicial habilitante. De ahí que lejos de debilitar el deber judicial de motivación de las resoluciones restrictivas de derechos, su necesidad se ve reforzada por esa misma ausencia». Para continuar precisando en rela-

136 STS 141/2020, de 13 de mayo.

137 V. RODRÍGUEZ LAÍN, J.L., «La nueva jurisprudencia sobre dispositivos de seguimiento y localización. (Comentario a la STS, Sala 2ª, 141/2020, de 13 de mayo)» en *La Ley*, número 9650, 2020, La Ley Digital, 22/02/2023

ción a la duración de la medida que «...La utilización de la locución "duración máxima" y el vocablo "excepcionalmente" es una llamada de atención a la importante afectación de la intimidad que estas medidas de geolocalización pueden traer consigo. Una duración prorrogada, de carácter máximo de 18 meses solo puede justificarse a la vista de la gravedad del hecho investigado y de la utilidad de la medida. Y por supuesto, solo es legítima a partir de una resolución judicial motivada que explique, a la vista de los principios de proporcionalidad, excepcionalidad y necesidad, la justificación del sacrificio del derecho a la intimidad»¹³⁸.

La reforma operada en la Ley procesal penal también ha suscitado un pronunciamiento de la Fiscalía General del Estado, en relación con la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, diferenciando entre la instalación de dispositivos que permiten grabar imágenes, y los dispositivos de seguimiento y localización. Así pone de relieve la distinta intensidad de las injerencias en el derecho fundamental a la intimidad. Si bien respecto a la grabación de imágenes, afirma que «...se trata de formas de indagación de la actividad delictiva que van a incidir en el derecho fundamental a la intimidad personal, al invadir reductos de privacidad que pueden llegar a afectar a la esfera más reservada de la vida de los investigados», considera que este tipo de injerencias en el derecho fundamental puede ser cuestionada al tratarse de una afección leve. Continúa señalando la Fiscalía General que «...Es esta una materia que no aparece condicionada en el texto constitucional a la reserva judicial, de ahí que el legislador haya optado por graduar la incidencia en el derecho fundamental de estas dos formas de persecución del delito exigiendo habilitación judicial únicamente para las modalidades más invasivas, los seguimientos a través de dispositivos técnicos, manteniendo, sin embargo, en manos de la Policía Judicial la capacidad de recurrir al empleo de dispositivos técnicos para la captación de imágenes»¹³⁹.

1.2.2. La incidencia en el derecho a la inviolabilidad del domicilio

Otro de los derechos fundamentales que pueden resultar afectados por la utilización de instrumentos tecnológicos relacionados con la inteligencia artificial, es el derecho a la inviolabilidad del domicilio. Si hasta hace algún tiempo la invasión del recinto domiciliario se circunscribía a la entrada física de personas no autorizadas, en este momento la injerencia se puede llevar a

138 STS 291/2021, de 7 de abril. V. también las SSTs 971/2022, de 16 de diciembre; 92/2023, de 11 de septiembre, entre otras.

139 V. Circular de la Fiscalía General del Estado 4/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización.

cabo también, por la intromisión de artefactos técnicos dirigidos por control remoto que proporcionan imágenes y sonidos. Y, además, aun en estos casos, la invasión puede tener lugar con la penetración física del aparato en el domicilio, o con la observación desde el exterior de la vivienda¹⁴⁰.

El uso de artificios técnicos que permiten el acceso al interior de la vivienda de forma no física, ya podía producirse con anterioridad a la utilización de instrumentos relacionados con la inteligencia artificial, a través de instrumentos tan sencillos como los conocidos prismáticos. El Tribunal Supremo se refiere a su utilización por los agentes policiales desde una vivienda situada frente al domicilio del sujeto investigado y posteriormente acusado. La Sala considera que *«...el agente de policía puede narrar como testigo cuanto vio y observó cuando realizaba tareas de vigilancia y seguimiento. Nuestro sistema constitucional no alza ningún obstáculo para llevar a cabo, en el marco de una investigación penal, observaciones y seguimientos en recintos públicos. A juicio de la Sala, sin embargo, la fijación del alcance de la protección constitucional que dispensa el art. 18.2 de la CE sólo puede obtenerse adecuadamente a partir de la idea de que el acto de injerencia domiciliaria puede ser de naturaleza física o virtual. En efecto, la tutela constitucional del derecho proclamado en el apartado 2 del art. 18 de la CE protege, tanto frente la irrupción inconsentida del intruso en el escenario doméstico, como respecto de la observación clandestina de lo que acontece en su interior, si para ello es preciso valerse de un artificio técnico de grabación o aproximación de las imágenes. El Estado no puede adentrarse sin autorización judicial en el espacio de exclusión que cada ciudadano dibuja frente a terceros. Lo proscribía el art. 18.2 de la CE. Y se vulnera esa prohibición cuando sin autorización judicial y para sortear los obstáculos propios de la tarea de fiscalización, se recurre a un utensilio óptico que permite ampliar las imágenes y salvar la distancia entre el observante y lo observado»*¹⁴¹.

De esta forma, la percepción visual del interior de un domicilio sin utilizar instrumentos de ampliación o acercamiento de la imagen, no supone una vulneración del derecho a la inviolabilidad del domicilio. Cuestión distinta, como destaca la anterior resolución, es si para facilitar esta percepción se utilizan este tipo de instrumentos.

Un ejemplo más sofisticado del uso de instrumentos que permiten el acceso virtual al domicilio, lo constituye el uso de drones en la investigación. Con ellos se facilita el acceso virtual a la vivienda, y además pueden proceder a la grabación de imágenes y sonido. En estos casos se afecta indudablemente al derecho a la inviolabilidad del domicilio, pero también al derecho a

140 ARIZA COLMENAREJO, M.J., «Garantías procesales en el uso de drones en la investigación penal», en *Era digital...*, op. cit., pág. 328.

141 STS 329/2016, de 20 de abril.

la intimidad y al secreto de las comunicaciones¹⁴². Por tal motivo, es obligado solicitar autorización judicial conforme a las reglas y garantías previstas en la Ley procesal penal sobre la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, y mucho más cuando estos artefactos se emplean no sólo para la observación, sino también para la grabación de imágenes y conversaciones, en estos casos las garantías serán las previstas en la regulación de la intervención de las comunicaciones orales directas¹⁴³.

Respecto de esta última medida, de la captación de conversaciones orales directas utilizando un dispositivo aéreo que permita la grabación de conversaciones en el interior de un domicilio, o en otros espacios privados o incluso públicos, no cabe duda que el derecho fundamental afectado es, además de la inviolabilidad del domicilio si la conversación se desarrolla en su interior, el derecho al secreto de las comunicaciones.

1.2.3. La incidencia en el derecho al secreto de las comunicaciones

El derecho al secreto de las comunicaciones consagrado constitucionalmente en el tercer apartado del artículo 18 CE, ha sido objeto de muchas consideraciones, sin embargo, es preciso apuntar la doctrina de la conocida sentencia del Tribunal Constitucional 114/1984, de 29 de noviembre, que determina su ámbito de aplicación y protección. Considera el Tribunal que el precepto constitucional garantiza el secreto de la comunicación y su «*impenetrabilidad por terceros (públicos o privados: el derecho posee eficacia erga omnes) ajenos a la comunicación misma*». El secreto no afecta y no puede predicarse frente al que toma parte en la comunicación. Quien graba una conversación propia no incurre en la prohibición del derecho al secreto del artículo 18.3 CE. Cuestión distinta es si se da difusión a la grabación y se entra en la esfera más reservada de la persona, vulnerándose entonces el derecho a la intimidad del primer apartado del citado artículo 18. Las nuevas aplicaciones informáticas facilitan sin duda la intervención de las comunicaciones, que ya no se realiza únicamente por la apertura de cartas y paquetes, o por la intervención de comunicaciones telefónicas. La interceptación y acceso al contenido de comunicaciones orales vis a vis, de correos electrónicos, o de comunicaciones telemáticas, marcan desde hace algunos años una nueva forma de intervención de comunicaciones que ha exigido la regulación de requisitos y procedimientos que garanticen la protección del derecho.

142 V. sobre esta cuestión, ARIZA COLMENAREJO, M.J., «Garantías procesales en el uso de drones en la investigación penal», en *Era digital...*, *op. cit.*, págs. 321-341.

143 Esta cuestión será tratada más ampliamente en el siguiente capítulo.

En el caso de la grabación de conversaciones orales directas, debe respetarse la regulación establecida en los artículos 588 quater y siguientes de la Ley procesal penal. De esta forma, se permite la utilización de este tipo de dispositivos electrónicos para captar las conversaciones orales directas del investigado, tanto en la vía pública, en espacios abiertos, en lugares cerrados, e incluso en su domicilio. En este último caso, la autorización judicial debe comprender, no sólo el acceso al domicilio, sino también la justificación de la medida de injerencia en este otro derecho fundamental. Es preciso apuntar en este sentido, que, con los nuevos dispositivos electrónicos, la entrada en el domicilio no siempre tiene lugar de forma física, la utilización de drones permite la injerencia desde fuera del recinto mediante la grabación de imágenes, al igual que permite también la grabación de las comunicaciones.

El art. 18.3 CE protege las conversaciones privadas, excluyéndose de su ámbito de protección aquellas comunicaciones o conversaciones que tienen vocación de publicidad. El carácter privado de una conversación ha de establecerse por la persona o personas que la mantienen, que de una u otra forman manifiestan su voluntad de no darla a conocer públicamente. Esto implica que cada individuo ostenta una capacidad de control sobre sus propias conversaciones. En atención a ello, cabe plantearse dos cuestiones. La primera, relativa a la determinación del número de personas que han de participar en una conversación para que sea considerada como privada; y la segunda, la necesidad de clarificar si una conversación mantenida en lugar público pierde su carácter privado por esta circunstancia, o su privacidad no depende del lugar donde se efectúe.

En relación con la primera de las cuestiones, una conversación puede ser privada aunque participen varias personas, ya que no sería lógico que esta cualidad dependiera del número de individuos que intervengan en ella¹⁴⁴. El criterio para calificar de privada una conversación en la que participe un grupo numeroso de personas, debe ser la concurrencia de algún hecho que las relacione, o que las una como grupo, configurándose éste, no como la reunión de personas aisladas entre sí, sino con conexiones internas entre ellas. Este sería el caso de reuniones entre miembros de partidos políticos, juntas de accionistas de empresas, etc., donde participan en general varios individuos, pero existiendo entre ellos unos mismos intereses. Lógicamente las conversaciones desarrolladas por estas personas mantienen su carácter privado, pese al número de participantes¹⁴⁵.

Respecto del lugar donde es preciso mantener las conversaciones para que éstas no pierdan su calidad de privadas, no es necesario que se desarro-

144 Esto nos llevaría a conclusiones tan ilógicas como establecer, por ejemplo, que una conversación de cinco personas es privada, pero una de seis ya puede considerarse pública.

145 Cuestión distinta, son los mítines de los partidos políticos, ya que en estos casos lo que se pretende es comunicar con el mayor número de personas, sin relación de ninguna clase entre ellas, convirtiendo la comunicación en pública.

llen en lugares cerrados, o de entrada restringida, pudiendo perfectamente tener lugar en restaurantes, cafeterías, etc., siempre que las personas que hablan utilicen un tono de voz normal, y no den a entender que se trata de una conversación pública. Nadie duda, cuando entra en alguno de estos lugares, que las conversaciones mantenidas por las personas que allí se encuentran son conversaciones privadas y nadie pretende, en principio, acceder a ellas. En este sentido, es conveniente diferenciar entre la escucha de una conversación privada que se mantiene en estos lugares, cuando se percibe de forma natural, y la que se produce utilizando mecanismos de grabación. En estos casos, no cabe duda que se vulnera el derecho al secreto de las comunicaciones¹⁴⁶.

La instalación de dispositivos técnicos de escucha, o la utilización de drones en espacios públicos que permitan el acceso a las conversaciones que se mantienen en estos lugares, debe ir precedida necesariamente de una autorización judicial, en la que el juzgador ha valorado la proporcionalidad de la medida.

La grabación de conversaciones en lugares públicos sin autorización judicial dictada en el seno de un proceso penal, vulnera el derecho al secreto de las comunicaciones del artículo 18.3 CE. Nadie duda que las comunicaciones que dos o más personas mantienen en la vía pública, en plazas, parques, etc., son de carácter privado, en tanto los interlocutores no quieran por el volumen de su conversación, hacerlas públicas. Para su intervención han de cumplirse los requisitos y condiciones previstos en los artículos 588 quater a) y siguientes LECrim.

Cabe en este punto hacer una precisión respecto de la instalación de cámaras móviles previstas en el artículo 17 LOPDP. El citado precepto permite a las autoridades policiales la grabación de imágenes y sonidos con cámaras móviles en lugares públicos, condicionándola a «...*la concurrencia de un peligro o evento concreto*». El legislador debería recoger alguna precisión más, en el sentido que la grabación del sonido, contemplada en el precepto, hace referencia a aquellos que no tienen la consideración de comunicación entre dos o más sujetos. Ya que, en otro caso, debería procederse conforme a lo establecido en los artículos 588 quater a) y siguientes de la Ley procesal penal, que prevé la intervención de las comunicaciones orales directas en el curso de una investigación penal, con autorización judicial previa¹⁴⁷.

146 STEDH de 20 de diciembre de 2005, Caso Wisse c. Francia,

147 V. SSTC 114/1984, de 29 de noviembre; 70/2002, de 3 de abril; 145/2014, de 22 de septiembre, entre otras.

1.3. Especial referencia a los derechos a la protección de datos personales y al entorno virtual como límite en la aplicación de los sistemas de inteligencia artificial

1.3.1. El derecho a la protección de datos

La presencia de la tecnología y de los instrumentos electrónicos en el día a día de la sociedad actual es innegable. Resulta impensable no ligar el desempeño de cualquier trabajo o profesión, con los dispositivos electrónicos que facilitan las relaciones en el mundo laboral e industrial, que se utilizan para agilizar las transacciones comerciales, o las negociaciones, o tratos con los operadores mercantiles. Pero la utilización de estos dispositivos también se extiende a la actividad personal diaria de adultos, jóvenes e incluso niños, interactuando con el entorno, y dando lugar a nuevas formas de relacionarse socialmente. Estas nuevas formas de relaciones sociales y comerciales favorecen la incorporación de datos personales de los ciudadanos que voluntariamente, o incluso de forma involuntaria, alimentan bases de datos, redes y otros tipos de aplicaciones virtuales, dejando un rastro sobre el sujeto, al que pueden acceder tanto los poderes públicos, como entes privados y sujetos con no buenas intenciones¹⁴⁸.

Esta nueva forma de relación y de comunicación, a través de dispositivos electrónicos, favorece la obtención de la información almacenada y facilita, por tanto, la investigación de las conductas delictivas¹⁴⁹.

Considerando que la base fundamental de los sistemas de IA, lo constituye el análisis de una gran cantidad de datos, que, atendiendo a las instrucciones de los algoritmos que se implantan en el sistema, se entrelazan con la finalidad de dar respuesta a las cuestiones planteadas, es necesario realizar un breve análisis del derecho contemplado en el artículo 18.4 CE, que precisamente protege al ciudadano de un uso inadecuado de sus datos personales, al consagrar como derecho fundamental el control de los datos relacionados con su vida privada¹⁵⁰.

148 Sobre el concepto del derecho al entorno digital v. GONZÁLEZ-CUELLAR SERRANO, N., «Garantías constitucionales en la persecución penal en el entorno digital» en *Derecho y Justicia Penal en el Siglo XXI. Liber amicorum* en homenaje al profesor Antonio González-Cuellar García, Colex, Madrid, 2006, págs. 887 y ss.

149 ORTIZ PRADILLO, J.C., «Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos fundamentales en el proceso penal», *La ley digital*, de 25 de enero de 2022, <https://laleydigital-laleynext-es.ezbusc.usc.gal/>, pág. 2.

150 V. ARRABAL PLATERO, P., «El derecho fundamental al propio entorno virtual y su incidencia en el proceso», en *Era digital, sociedad y Derecho* (Fuentes Soriano, dir.), Editorial Tirant lo Blanch, Valencia, 2020, págs. 431 a 442. GALLEGO RODRÍGUEZ, P., «Los registros biométricos y su aplicación al proceso penal desde una perspectiva constitucional», en *Inteligencia artificial legal y Administración de justicia...*, op. cit., págs. 220 y ss.

Es evidente que, en la investigación de los hechos delictivos, la entrada de los poderes públicos en la esfera privada de los ciudadanos tiene como límite el respeto de sus derechos fundamentales. En este contexto se enmarca el límite que la Constitución establece en su artículo 18.4 CE. Advirtiéndose ya los peligros que el uso de las nuevas tecnologías, de la informática como recoge el precepto, podría suponer en una sociedad futura, el constituyente establece que será la ley la encargada de limitar su aplicación, protegiendo así los derechos fundamentales en juego. Así lo expresa el Tribunal Constitucional, al declarar que *«la Ley limitará 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»*. De este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama *«la informática»*¹⁵¹.

Sin embargo, nuestro Tribunal va más allá, y haciendo referencia, en aquel momento, a la ausencia de desarrollo legislativo del precepto, declara que este hecho no puede utilizarse como justificación para no defender su plena efectividad. Así lo declara al señalar que *«...cuando se opera con esa reserva de configuración legal el mandato constitucional puede no tener, hasta que la regulación se produzca, más que un mínimo contenido ..., pero ese mínimo contenido ha de ser protegido, ya que de otro modo el amparo previsto en el art. 53.2 de la Constitución carecería de efectividad y se produciría la negación radical de un derecho que goza de la máxima protección constitucional en nuestro ordenamiento jurídico. La dilación en el cumplimiento del deber que la Constitución impone al legislador no puede lesionar el derecho reconocido en ella»*¹⁵². Para seguir afirmando posteriormente que *«...los derechos y libertades fundamentales vinculan a todos los poderes públicos, y son origen inmediato de derechos y obligaciones, y no meros principios programáticos. Este principio general de aplicabilidad inmediata no sufre más excepciones que las que imponga la propia Constitución, expresamente o bien por la naturaleza misma de la norma»*¹⁵³.

151 STC 254/1993, de 20 de julio. V. también SSTC 11/1998 de 3 de enero; 94/1998, de 4 de mayo; 292/2000, de 30 de noviembre, entre otras.

152 STC 15/1982, de 23 de abril; V. también 16/1982, de 28 de abril

153 STC 254/1993, de 20 de julio

En este sentido, cabe defender la aplicación directa de la Norma constitucional, en relación a los derechos fundamentales, cuando los reconoce y consagra, si bien no se puede decir lo mismo respecto de las posibles restricciones «...*dado que el Texto constitucional no descende a una concreta regulación de los casos y forma en que las injerencias o limitaciones pueden producirse*»¹⁵⁴.

Esta garantía de la regulación legal que desarrolle el contenido y límites del derecho fundamental a la protección de datos, ha sido también objeto de las consideraciones del alto tribunal¹⁵⁵, que haciéndose eco de la doctrina del TEDH, ha considerado que la garantía establecida en el artículo 8 CEDH, relativa a la intimidad individual y familiar, es también aplicable a la protección de datos personales. El Tribunal europeo reconoce que la seguridad nacional, o la investigación delictiva, pueden operar como límites del ejercicio de tales derechos, pero también afirma que dichas limitaciones deben resultar imprescindibles en una sociedad democrática, y han de establecerse en una ley de fácil acceso para el ciudadano, que puede de esta forma conocer las consecuencias de su aplicación¹⁵⁶. Además, como también precisa el Tribunal, tales limitaciones serán necesarias, adecuadas y proporcionadas al fin que se persigue¹⁵⁷.

En este contexto, se aprueba la LO 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, primera Ley de nuestro ordenamiento jurídico sobre esta materia, que crea la Agencia de Protección de Datos, como órgano encargado de controlar su aplicación. Tres años después, se aprueba en la Unión Europea, la Directiva 95/46/CE, del Parlamento europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. Esta Directiva nace con la pretensión de unificar la normativa europea en la materia. En su desarrollo se dicta en nuestro país, la Ley 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, que sustituye a la anterior de 1992¹⁵⁸.

154 MORENO CATENA, V., «Garantía de los derechos fundamentales en la investigación penal» en *Poder Judicial*, número especial II, 1987, pág. 157.

155 V. la importante STC 292/2000, de 30 de noviembre.

156 SSTEDH de 6 de septiembre de 1978 (caso Klass y otros); 25 de marzo de 1983, caso Siver y otros; 27 de octubre de 1983, caso Malone; 26 de marzo de 1987, caso Leander; de 25 de febrero de 1997, casos Z; de 25 de febrero de 1993, caso Funke.

157 SSTEDH de 26 de marzo de 1985, caso X e Y; de 26 de marzo de 1987, caso Leander; de 7 de julio de 1989, caso Gaskin, entre otras.

158 V. más ampliamente, SANTOS SÁNCHEZ, D.J., «Los tratamientos de datos personales para la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales: consideraciones de la AEPD», en *Investigación y proceso penal en el siglo XXI...*, op. cit., págs. 713 y ss.

El desarrollo normativo del derecho a la protección de datos se completa con su incorporación, primero en la Carta de Derechos Fundamentales de la UE, y posteriormente en el Tratado de Funcionamiento de la Unión. Consecuencia de ello es la elaboración, en el ordenamiento de la UE, de una norma general de protección de datos, el Reglamento UE 679/2016, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, y la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE, y en la legislación nacional, la LO 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales, que deroga la anterior LO 15/1999, y que pretende lograr la adaptación del ordenamiento jurídico español al Reglamento citado.

No obstante, con el objetivo de otorgar una protección extraordinaria del derecho a la protección de datos, y de diseñar un sistema de garantías completo que proteja al individuo, aún en aquellos casos en los que los poderes públicos están autorizados al tratamiento de sus datos personales, se dicta la Directiva 2016/680, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, que regula un régimen especial o específico, y que se dirige únicamente a los tratamientos que regula, esto es, el tratamiento de datos, con los fines descritos, en el ámbito judicial y policial. Esta norma se completa con una segunda Directiva, Directiva UE 681/2016, 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 grave¹⁵⁹.

La trasposición a nuestro ordenamiento jurídico de la Directiva 2016/680, se lleva a cabo con la LO 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. Dado el objeto de nuestro trabajo también es importante destacar en este punto, la regulación desarrollada en el Capítulo I bis del Título III del Libro III de la LOPJ, que bajo el rótulo «Protección de datos de carácter personal en el ámbito de la Administración de Justicia» diferencia entre el tratamiento con fines jurisdiccionales o no jurisdiccionales, estableciendo las reglas básicas a tener en cuenta.

159 La citada Directiva se traspone a la legislación nacional con la LO 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. V. GUZMAN FLUJA, V., «Consideraciones sobre el alcance objetivo y subjetivo de la Directiva UE 680/2016» en *Nuevos Postulados de la Cooperación Judicial...*, op. cit., pág. 824; SANTOS SÁNCHEZ, D.J., «Los tratamientos de datos personales para la prevención, investigación...», op. cit., pág. 718.

De las normativas europea y nacional se pueden extraer los principios básicos que rigen y dan sentido a la utilización y tratamiento de datos con fines de investigación penal, y que se fundamentan en el respeto de los derechos fundamentales de los ciudadanos¹⁶⁰. El principio del consentimiento alude a la autorización personal del titular para acceder a sus datos personales, excepción hecha de aquellas situaciones en las que una ley autorice su tratamiento sin consentimiento, y establezca los requisitos y garantías a observar. Relacionado con el anterior, se encuentra el principio de información, que obliga a la identificación del fichero de almacenaje de datos y a su responsable, con el objetivo de que el titular de los datos, conozca la existencia del fichero, su finalidad y el responsable, a efectos de autorizar o denegar futuros tratamientos. El principio de calidad de los datos supone una garantía imprescindible en el tratamiento, que avala su utilización con fines legítimos y adecuados. El principio de conservación exige que los datos tratados puedan cancelarse cuando ya se ha cumplido la finalidad de su obtención. Y en caso contrario, los requisitos y garantías que se deben observar cuando deban ser conservados. Y finalmente, los derechos conocidos como ARCO (acceso, rectificación, cancelación y oposición)¹⁶¹.

El derecho a la protección de datos se integra en el artículo 18 CE, que recoge una serie de derechos fundamentales que tienen en común la protección de la vida privada de los ciudadanos. Así, como ya se ha señalado, pero en este punto es necesario recalcar, el derecho al honor, el derecho a la intimidad, el derecho a la propia imagen, la inviolabilidad del domicilio, el secreto de las comunicaciones personales, y el derecho a la protección de datos, se integran en el citado precepto constitucional, que también ampara al ahora conocido como derecho al entorno virtual, y se convierten en el escudo protector de la esfera privada. Como derechos fundamentales consagrados constitucionalmente, su limitación ha de realizarse por ley orgánica que especifique los supuestos, requisitos, procedimiento y, en definitiva, las garantías que han de rodear una posible injerencia.

Realmente, el cuarto apartado del artículo 18 CE, se puede desdoblar en dos derechos, el derecho a la autodeterminación informativa, o derecho a la protección de datos, y el derecho al entorno virtual. El primero de ellos puede considerarse como un derecho estático, que protege los datos personales que

160 El artículo 4.2 RGPD define el tratamiento como «cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción».

161 RODRÍGUEZ FERNÁNDEZ, R., «Protección de datos personales: normativa europea y nacional (especial referencia a la normativa de protección de datos en la prevención, detección, investigación y enjuiciamiento de infracciones penales)», en *La Ley Penal*, número 157, Julio-Agosto 2022, <https://laleydigital-laleynext-es>, pág. 4.

se encuentran en dispositivos particulares y en la red, y que se lesiona cuando se accede a dichos datos sin respetar la voluntad de su titular. El segundo, con un alcance más amplio, se trata de un derecho dinámico, cuya finalidad es la exclusión de intromisiones en el espacio digital, en el que los titulares dejan huellas, rastros, comunicaciones, etc., de forma consciente o involuntaria¹⁶².

Para el Tribunal Constitucional, el apartado cuarto del artículo 18 CE, incorpora una nueva garantía constitucional, que dará respuesta a las posibles amenazas a la dignidad y a los derechos que protegen la vida privada. Se garantiza así, el derecho al honor y a la intimidad personal, pero también otros derechos relacionados con la vida privada que puedan ponerse en peligro por el uso indebido de la informática, o como recoge expresamente el alto Tribunal «...*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"*»¹⁶³.

Se regula como derecho fundamental, el derecho a controlar el uso de los datos relacionados con la vida privada de los ciudadanos, que podrán oponerse a que sus datos personales puedan ser utilizados para fines distintos a aquel que justificó su obtención¹⁶⁴. Este poder de disposición y control faculta a la persona para decidir, no sólo qué datos quiere proporcionar y con qué finalidad, sino también le habilita para conocer qué tipo de instituciones públicas o privadas detentan esos datos y con qué fin.

Considera el Tribunal, que el artículo 18.4 CE consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona, independientemente de que pertenezcan, o no, al ámbito más reservado de su intimidad¹⁶⁵. Esta precisión sobre el origen de los datos, incluyendo aquellos que son públicos, centra el contenido y alcance de este derecho, que extiende su protección a los datos personales que puedan obtenerse de una exposición pública, atribuyendo a su titular la autorización para su uso, más allá de aquellos ámbitos que ha permitido inicialmente¹⁶⁶.

Y es aquí donde radica uno de los contenidos más importantes de este derecho fundamental, el poder de control y de disposición sobre los datos personales. A través de esta garantía se impone a los poderes públicos la prohibición de facilitar la información sobre los ciudadanos sin la debida autorización y garantías. Pero, como señala expresamente el Tribunal «ese

162 CALAZA LÓPEZ, S., «Protección judicial del derecho a la intimidad informática en su doble dimensión de derecho a la Autodeterminación informativa y derecho al entorno virtual» en Nuevos postulados de la cooperación judicial en la Unión Europea..., *op. cit.*, pág. 1115. V también, SSTs 342/2013, de 17 de abril y 786/2015, de 4 de diciembre.

163 STC 254/1993, de 20 de julio.

164 SSTC 11/1998, de 13 de enero y 94/1998, de 4 de mayo.

165 STC 94/1998, de 4 de mayo.

166 STC 27/2020, de 24 de febrero.

*poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin*¹⁶⁷.

El Tribunal Constitucional se ocupa de diferenciar la protección otorgada por el artículo 18.4 CE, de la reconocida en su primer apartado que recoge el derecho a la intimidad. Así considera 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 terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran»¹⁶⁸.

Como ya se ha apuntado, los derechos recogidos en el artículo 18 CE, tienen en común regular el ámbito de protección de la vida privada de los ciudadanos, considerada en todas las posibles manifestaciones, y diseñando un ámbito objetivo diferente para cada uno de los derechos contemplados, pese a que todos ellos se encuentran estrechamente vinculados entre sí.

Hechas estas consideraciones previas, es evidente que la libre circulación de datos personales y su tratamiento por sistemas de IA supone una ventaja indudable para la prevención, investigación y enjuiciamiento de conductas criminales, pero también resulta obvio que este tipo de actuación debe estar sujeta a un conjunto de garantías que protejan los derechos de los ciudadanos.

En un primer momento, y al vincularse la información y el traspaso de datos al derecho a la intimidad, se facilitaba la libre obtención de dichos datos por parte de las fuerzas de seguridad con la finalidad de la investigación delictiva. Por tal motivo, no siempre era necesaria una autorización judicial expresa. Además, la LO 15/1999, de protección de datos de carácter personal, dero-

167 STC 292/2000, de En este sentido considera el tribunal es esta resolución que «...el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 C.E. otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos».

168 STC 292/2000 de 30 de noviembre.

gada por la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, autorizaba, en su artículo 22, la recogida y tratamiento de datos personales, sin autorización de su titular, siempre que su finalidad fuera la prevención de un peligro real para la seguridad pública, o la represión de infracciones penales¹⁶⁹.

Sin embargo, la revolución tecnológica, y el peligro que supone para la esfera personal de los ciudadanos, la utilización de instrumentos electrónicos de todo tipo para la investigación criminal, provocó que los tribunales iniciasen una jurisprudencia más restrictiva sobre dicha utilización, amparando la vida privada del ciudadano y su control sobre los datos protegidos por el artículo 18.4 CE. Además, también el legislador ha sido consciente del riesgo que conlleva una utilización inadecuada de los dispositivos tecnológicos, regulando nuevos requisitos y garantías en la LO 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. Tal y como ya se ha indicado, el objeto de esta norma, se recoge en su artículo 1, y como se desprende del título se centra en «... establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública». En la misma línea de protección de los derechos fundamentales agrupados en el artículo 18 CE, se enmarca la regulación de la LO 13/2015, de modificación de la Ley procesal penal, estableciendo el marco de actuación en la investigación con medios tecnológicos.

De esta forma, y considerando su aplicación en la investigación de conductas delictivas, han de resultar de aplicación los principios rectores de las medidas de investigación tecnológica, y especialmente los principios de legalidad, jurisdiccionalidad y proporcionalidad. Precisamente, fruto de esa evolución y de la jurisprudencia del Tribunal Europeo de Derechos Humanos, del Tribunal Constitucional y del Tribunal Supremo, son las exigencias relacionadas con la inviolabilidad del domicilio y el secreto de las comunicaciones, que ahora tienen reflejo en la Ley procesal penal. Una muestra de ello es el reconocimiento por el Tribunal Supremo de que la posible captación con instrumentos tecnológicos del interior de un domicilio vulnera el derecho recogido en el artículo 18.2 CE, aunque no haya una entrada física en el mismo¹⁷⁰. De la misma forma, el registro de ordenadores, o de teléfonos móviles, exige también el cumplimiento de las garantías previstas para la injerencia en el secreto de las comunicaciones, o en el derecho a la protección de datos, al

169 ORTIZ PRADILLO, J.C., «Big Data, vigilancias policiales y geolocalización...», *op. cit.*, pág. 6.

170 V. en este sentido la STS 342/2013, de 17 de abril.

considerar que estos elementos electrónicos contienen información que pertenece a la esfera reservada de la persona¹⁷¹.

No puede obviarse, que el tratamiento de los datos proporcionados por instituciones públicas y entidades privadas permite a las unidades policiales reconstruir las actuaciones realizadas por los sujetos investigados, llegando a averiguar con total precisión su actividad pasada, e incluso las personas con las que han contactado¹⁷². Es indudable que con ello se está produciendo una grave injerencia en el derecho a la vida privada de los ciudadanos, no sólo del investigado, sino también de terceros con los que se relaciona¹⁷³.

Atendiendo precisamente a la gravedad de la injerencia en el derecho fundamental citado, el Tribunal Constitucional ha estimado que la protección se extiende a todos «...*aquellos datos que identifiquen o permitan la identificación de la persona y que puedan servir para la confección de su perfil o para cualquier otra utilidad que, en determinadas circunstancias, constituya una amenaza para el individuo*»¹⁷⁴. En el mismo sentido, y en relación con las publicaciones obtenidas de las redes sociales, considera el alto Tribunal que los ciudadanos autorizan su acceso en un determinado momento y ubicación, pero con ello no se está extendiendo la autorización a otras posibles accesos o publicaciones ajenas al ámbito temporal y espacial previsto inicialmente por el titular del derecho¹⁷⁵.

Partiendo de estas consideraciones, será necesario establecer un régimen legal sobre la aplicación de los instrumentos de inteligencia artificial con fines de prevención y de investigación de las conductas delictivas. Si en los supuestos de su utilización en el marco de una investigación penal se han de aplicar los principios rectores previstos por la Ley 13/2015, que regula las medidas de investigación tecnológica, en los casos de actuación preventiva no resulta del todo claro la forma en la que se ha de proceder. Todo dependerá del margen de incidencia en los derechos fundamentales y de la gravedad de la injerencia.

En aquellos casos en que la intromisión en algunos de los derechos contemplados en el artículo 18 CE, y más concretamente en su apartado cuarto, pueda revestir cierta gravedad, sería preciso recabar la autorización judicial para facilitar el juicio de proporcionalidad y establecer el marco de garantías que han de aplicarse en las medidas restrictivas de derechos fundamentales.

171 STC 115/2013, de 9 de mayo.

172 V. RODRÍGUEZ LAINZ, J.L., «Últimos pronunciamientos del Tribunal de Justicia de la Unión Europea sobre cesión de datos de telecomunicaciones para fines de investigación criminal», en *La inteligencia artificial y su aplicación en el sistema de justicia penal* (Noya Ferreiro, dir.), Tirant lo Blanch, Valencia, 2025.

173 ORTIZ PRADILLO, J.C., «Big Data, vigilancias policiales y geolocalización...», *op. cit.*, pág. 5.

174 STC 29/2013, de 11 de febrero.

175 STC 27/2020, de 24 de febrero.

De todas formas, al igual que está previsto para otras medidas de investigación tecnológica, razones de urgencia pueden aconsejar la actuación inmediata de la policía, pero en estas situaciones deberá requerirse, en el más breve plazo posible, la validación judicial de la actuación para preservar el respeto del derecho fundamental que se ha visto afectado.

En este contexto, es necesario precisar que el artículo 18.4 CE supone un límite indudable a la obtención del material probatorio, al considerarse que la vulneración del derecho fundamental previsto al obtener e incorporar datos personales al proceso determinan la ilicitud de la prueba¹⁷⁶.

1.3.2. El derecho al entorno virtual o digital

Tal y como ya se ha indicado al inicio de este epígrafe, junto al derecho a la protección de datos, se protege también en el cuarto apartado del artículo 18.4 CE, el derecho al entorno virtual o digital. Se trata de un derecho fundamental de nueva generación que tiene su origen en el desarrollo de la vida privada de los ciudadanos en el espacio virtual, en el que se exponen diferentes manifestaciones relacionadas con la intimidad, la imagen, el secreto de las comunicaciones. Estas nuevas formas de relación y la capacidad que tienen los instrumentos tecnológicos de entrar en esa esfera privada de los ciudadanos que se expone en los sistemas digitales, poniendo en peligro varios de los derechos fundamentales consagrados en el citado artículo 18 CE, ha resultado determinante para el reconocimiento de este nuevo derecho al entorno virtual. No se trata de la injerencia en el derecho a la intimidad, o en el derecho al secreto de las comunicaciones, o en el derecho a la imagen, o la inviolabilidad del domicilio, sino que la utilización de esta clase de artificios puede poner en peligro todos ellos. En estrecha relación con su protección se parte de una realidad evidente, y es que, en la sociedad actual, los ciudadanos desarrollan parte de su vida privada de forma virtual, y, por tanto, ha de darse protección a esta nueva forma de relacionarse.

Es cierto que la protección de los derechos fundamentales en juego, ya podía realizarse a través de la regulación y amparo de cada uno de ellos, sin embargo, esta protección es más completa cuando se lleva a cabo de forma global, relacionando cada uno de los derechos en juego, ya que de esta forma se da amparo integral a la vida privada¹⁷⁷.

Los datos personales, cuando se consideran individualmente, pueden ser objeto de protección a través del derecho a la intimidad, o a través del derecho a la imagen, o del secreto de las comunicaciones, pero cuando se

176 DELGADO MARTÍN, J., «Protección de datos personales y prueba en el proceso» en *Diario La Ley*, número 9383, 22 de Marzo de 2019, <https://laleydigital-laleynext-es>, pág. 2.

177 ARRABAL PLATERO, P., «El derecho fundamental al propio entorno virtual y su incidencia en el proceso», en *La justicia digital en España...*, op. cit., pág. 432.

accede, por ejemplo, a un ordenador personal, o a un smartphone, se está abriendo una puerta a la vida privada del sujeto, accediendo a datos de la vida más reservada (videos, fotografías, documentos personales...), incidiendo en varios de los derechos fundamentales del artículo 18 CE. Pero, además, esta información se puede obtener también accediendo a las páginas, chats, o las redes sociales en las que interactúa una persona. En este entorno virtual se ponen de manifiesto y se dan a conocer los datos más reservados, pero esa información personal no tiene vocación de publicidad, ni tiene el interesado la intención de compartirla con personas ajenas a su entorno. Señala el Tribunal Constitucional, que todo este cúmulo de informaciones consideradas de forma aislada pueden no tener interés, sin embargo, al relacionarlas, configuran un perfil concreto y descriptivo de la personalidad del individuo, y como tal información global ha de ser protegida¹⁷⁸.

A esta vinculación de la información relacionada con una persona, hace referencia la denominada Teoría del mosaico¹⁷⁹. Para esta teoría, la información parcial del individuo es equiparable a las piezas de un mosaico, individualmente consideradas no aportan nada significativo, pero bien colocadas o, en este caso, enlazadas, configura la personalidad de una persona.

También el Tribunal Supremo se ha ocupado del reconocimiento de este derecho en varias de sus resoluciones, considerando que *«La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso 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*

178 STC 173/2011, de 7 de noviembre.

179 «La teoría del mosaico considera que la información de un individuo en cuanto a lo privado y lo público son datos abiertos y no pertenecientes al 100 % a un apartado determinado. Por ello se puede entender que existe una delgada línea entre los datos que se pueden considerar privados y cuales públicos, puestos que esa clasificación según Madrid Conesa va a depender de quien sea el sujeto receptor de la información y quien el emisor de la misma. Por otro lado, lo que en un principio puede parecer un dato irrelevante, como el sexo de una persona, el nombre, la fecha de nacimiento, sus inclinaciones políticas, sus datos de renta, etc si se presentan aislados; si los mismos en lugar de verlos de forma aislada los unimos, todo cambia. Los datos que a priori pueden parecer no importantes y que no afectan al derecho a la intimidad si los conectamos con otros que quizás tampoco parezcan irrelevantes, pero que pertenezcan al mismo individuo, podemos llegar a conseguir una composición exacta de dicho individuo sin que éste tenga conocimiento de ello». V. en este sentido, NISA ÁVILA, J.A., «Teoría del Mosaico y Data Mining: análisis jurídico del estado actual en comparativa con la Theory Modular Data Privacy», en *ElDerecho.com. Noticias Jurídicas y Actualidad*. <https://elderecho.com/teoria-del-mosaico-y-data-mining-analisis-juridico-del-estado-actual-en-comparativa-con-la-theory-modular-data-privacy> V. también GIMENO SENDRA, V., «Libertad de expresión, honor e intimidad personal», *Economist & Jurist*, volumen 17, número 136, 2010, págs. 40 y ss.

*de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital*¹⁸⁰.

Por tanto, la protección constitucional del derecho al entorno virtual en el que se integra «*toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos*»¹⁸¹, requiere una autorización judicial previa, como así lo exigen expresamente, para alguno de los derechos fundamentales integrados (derecho al secreto de las comunicaciones), la propia Norma constitucional¹⁸².

Ahora bien, este derecho al entorno virtual puede moldearse por su titular, que tiene la facultad de preservar su vida privada de toda intromisión ajena, o compartir parte de esta esfera personal. A esta cuestión también alude el Tribunal Supremo, haciendo incluso referencia a la reducción de la protección del entorno virtual cuando se comparte el uso de un ordenador. En este sentido, considera que «*...frente a lo que sucede respecto del contenido material de otros derechos, el derecho a la intimidad o, si se quiere, el espacio de exclusión que frente a otros protege el derecho al entorno virtual, es susceptible de ampliación o reducción por el propio titular. Quien incorpora fotografías o documentos digitales a un dispositivo de almacenamiento masivo compartido por varios es consciente de que la frontera que define los límites entre lo íntimo y lo susceptible de conocimiento por terceros, se difumina de forma inevitable*». Las expectativas de mantener la privacidad

180 STS 342/2013, de 17 de abril. V. también las SSTS 97/2015, de 24 de febrero; 786/2015, de 4 de diciembre; 204/2016, de 10 de marzo; 426/2016, de 19 de mayo; 489/2018, de 23 de octubre; 723/2018, de 23 de enero; 462/2019, de 14 de octubre

181 STS 204/2016, de 10 de marzo.

182 V. ARRABAL PLATERO. P., El derecho fundamental al propio entorno virtual y su incidencia en el proceso, en «*La justicia digital en España...*», *op. cit.*, págs., 135 y ss.; LÓPEZ-BARAJAS PEREA I., El derecho a la protección del entorno virtual y sus límites: el registro de los sistemas informáticos» en *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas* (Díaz Martínez/López-Barajas Perea, dirs), Tirant lo Blanch, Valencia 2018, pág. 137 y ss; entre otros.

en estos casos se ven reducidas. De todas formas, en el caso apuntado en la resolución citada, lo que se comparte es la utilización de un mismo ordenador, por lo que se puede prever que otras personas que dispongan de la misma contraseña, puedan acceder a los contenidos propios. Sin embargo, esta situación no hace previsible que los poderes públicos accedan a esos contenidos, por lo que la autorización judicial para el acceso seguiría siendo necesaria¹⁸³.

Teniendo en cuenta que el derecho al entorno virtual protege al ciudadano respecto de todas aquellas manifestaciones de su vida privada que comparte en el espacio digital, podría pensarse que la injerencia en este ámbito de la vida privada vulnera el derecho al secreto de las comunicaciones. Sin embargo, este derecho protege la comunicación cuando está en curso, esto es, cuando se está produciendo el procedimiento comunicativo, no cuando ya ha finalizado y los datos permanecen en los dispositivos. Así lo pone de relieve el Tribunal Supremo, cuando se pronuncia sobre la captación y lectura de correos electrónicos y considera que no se trata de una intromisión en el derecho al secreto de las comunicaciones. Afirma el Tribunal que «...el correo electrónico y los programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato telemático, el derecho a la libre comunicación entre dos o más personas. Es opinión generalizada que los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por su destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito que sería propio de la inviolabilidad de las comunicaciones. La comunicación ha visto ya culminado su ciclo y la información contenida en el mensaje es, a partir de entonces, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad, cuya tutela constitucional es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad de las comunicaciones... Más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual»¹⁸⁴.

183 No obstante, es preciso matizar en este aspecto, que la resolución citada hace referencia a la entrega a la policía del ordenador de uso familiar, entrega que se realiza por la madre de una menor en relación a una investigación por abusos sexuales del padre. Obviamente, el supuesto es diferente al examen de un ordenador sin que medie esa entrega, y sin que el usuario tenga la condición de menor. En este caso, es uno de los usuarios el que pone a disposición de la policía el dispositivo y lo hace como titular de la patria potestad y en protección de un menor.

184 STS 342/2013, de 17 de abril. V. también, 786/2015, de 4 de diciembre, 462/2019, de 14 de octubre, entre otras.

2. La incidencia de la inteligencia artificial en los derechos fundamentales de naturaleza procesal

Es evidente, y ya se ha señalado anteriormente, que la utilización de las nuevas tecnologías y de los sistemas relacionados con la inteligencia artificial facilita la investigación penal, pero al mismo tiempo, cuando su uso no se rodea de las garantías necesarias, puede poner en peligro los derechos vinculados a la vida privada de las personas, pero también los derechos fundamentales de naturaleza procesal previstos en el artículo 24 CE.

Desde luego, la justicia tiene muy presente las grandes ventajas que proporcionan los instrumentos de inteligencia artificial, prueba de ello es el Convenio suscrito en 2017 entre el CGPJ y la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital. El citado convenio permite a los profesionales adscritos a los órganos jurisdiccionales utilizar aplicaciones de inteligencia artificial que puedan facilitar su trabajo. Dichas aplicaciones se utilizan principalmente para el tratamiento jurisprudencial y análisis de documentos¹⁸⁵.

También ha sido un importante antecedente, por su innovación para la tramitación procesal y en la digitalización de la Administración de justicia, la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia¹⁸⁶, derogada por Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo.

La vieja ley recogía la implantación del expediente electrónico, lo que exigiría la digitalización de los procedimientos desarrollados ante los tribunales, para lo que resultaba imprescindible que los actos de comunicación y presentación de escritos fueran realizados de forma electrónica, tal y como lo ha regulado en su momento la Ley 42/2015, de 5 de octubre, de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. En el mismo año se dicta el Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia, y por el que se regula el sistema LexNET.

185 MARTÍN DÍZ, F., «Inteligencia artificial y proceso: garantías frente a eficiencia en el entorno de los derechos procesales fundamentales», en *Justicia: ¿Garantías versus Eficiencia?*, (Llopis Nadal/Bellido Penadés/Jiménez Conde/De Luis García, coords.), <http://www.tiranonline.com>, 21 de enero 2020 pág. 2.

186 Dicha Ley fijaba un plazo de cinco años para que las Administraciones competentes dotasen a las oficinas judiciales y fiscalías de sistemas de gestión procesal que permitan la tramitación electrónica de los procedimientos.

En el mismo sentido, el RD 6/2023, supone, como ya indica el texto normativo, «...la consolidación en nuestra sociedad de las nuevas tecnologías, la evolución cultural de una ciudadanía consciente de los retos que comporta la digitalización y, sobre todo, la utilidad de los nuevos instrumentos y herramientas tecnológicas al servicio de una mejor y más eficiente gestión de los recursos públicos, también en el marco de la Administración de Justicia, implica para los poderes públicos el imperativo de abordar correctamente este nuevo marco relacional y, con él, delimitar y potenciar el entorno digital con el propósito de favorecer una más eficiente potestad jurisdiccional».

No cabe duda que el acceso a las bases de datos y documentación jurídica a través de los instrumentos de IA es un avance importante, tanto para la agilización de la tramitación procesal, como para el buen funcionamiento de la organización judicial¹⁸⁷. Pero con este tipo de instrumentos lo que se proporciona al órgano jurisdiccional, y al personal que lo compone, son sistemas que facilitan su trabajo, pero que en ningún caso sustituyen al sujeto en la toma de decisiones. No cabe olvidar que la aplicación de los sistemas de IA para la resolución de conflictos, requiere que la decisión adoptada por el sistema pueda ser revisada por la persona que lo controla, apartándose incluso de ella cuando se cuestione el resultado¹⁸⁸. Con ello no se pretende mantener que los sistemas de inteligencia artificial no puedan evolucionar hasta el punto de que la actividad humana en el proceso pueda ser sustituida, lo que realmente se defiende es que, desde el respeto a la propia naturaleza de la función jurisdiccional y la protección de los derechos fundamentales en un Estado de Derecho, sea esta la opción la más apropiada¹⁸⁹.

Por tanto, como cabe colegir de las consideraciones anteriores, a la hora de analizar la implantación de los sistemas de IA en la Administración de justicia, sin poner en duda su utilidad, también deben tenerse en cuenta los graves peligros que este tipo de recursos pueden generar en el respeto a la dignidad de la persona y a los derechos fundamentales, y en el correcto fun-

187 V. sobre esta cuestión BARONA VILAR, S., *Algoritmización del derecho y de la justicia...*, op. cit., 2021, págs. 554-556.

188 En este sentido, ya el Reglamento del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, por el que se deroga la Directiva 95/46/CE, establece en su artículo 22 que «1.Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar».

189 GUZMÁN FLUJA, V., «Automated justice. La preocupante tendencia hacia la justicia penal automatizada» en *Derecho procesal. Retos y transformaciones* (Bujosa Vadell, dir.), Editorial Atelier, Barcelona, 2021, pág. 366. V. también GÓMEZ COLOMER, J.L., V. también GÓMEZ COLOMER, J.L., «Unas reflexiones sobre el llamado «juez-robot», al hilo del principio de la independencia judicial» en *Justicia algorítmica...*, op. cit., pág. 253.

cionamiento de un proceso penal conforme a los principios constitucionales propios del Estado de Derecho¹⁹⁰.

Con carácter previo, y antes de abordar el análisis de la incidencia de la aplicación de los sistemas de IA en los derechos fundamentales de naturaleza procesal, es necesario precisar que los citados derechos se recogen en el artículo 24 CE que, en sus dos apartados, los regula con diferente contenido, pero que se integran en el marco de garantías del proceso. En este sentido, el Tribunal Constitucional se ha pronunciado considerando que *«El artículo 24 de la Constitución, en sus dos epígrafes, previene dos supuestos íntimamente relacionados entre sí, pero que merecen un tratamiento diferenciado, ya que el segundo de ellos apunta preferentemente a las llamadas «garantías procesales»-así el derecho al juez ordinario predeterminado por la ley, asistencia letrada, información de la acusación, proceso público, utilización de los medios de prueba pertinentes y presunción de inocencia—, mientras que el primero, al proclamar el derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de los derechos e intereses legítimos previniendo que nunca pueda producirse indefensión, establece una garantía, previa al proceso, que lo asegura, cuando se dan las circunstancias requeridas al efecto. Dicho de otro modo, el artículo 24.1 también asegura la «tutela efectiva», pero lo hace a través del concreto juego de los instrumentos procesales, mientras que el 24.2 asegura la tutela efectiva mediante el acceso al mismo proceso»*¹⁹¹.

2.1. Derecho a la tutela judicial efectiva e Inteligencia artificial

Dejando a un lado las ventajas de la aplicación de los instrumentos tecnológicos en el campo procedimental, que sin duda va a reportar una tramitación más ágil y eficaz, reduciendo tiempo y trabajo, lo que desde luego ha de valorarse de forma muy positiva, los mayores inconvenientes en la aplicación de estos instrumentos se encuentran vinculados al ejercicio de los derechos fundamentales de contenido procesal, y a las garantías del proceso debido.

En una primera aproximación, el derecho a la tutela judicial efectiva, consagrado como derecho fundamental en el primer apartado del artículo 24 CE, integra en su contenido esencial el derecho de acceso a los tribunales, el derecho a la obtención de una sentencia de fondo jurídicamente fundada, y el derecho a la ejecución de la sentencia. Así se pone de relieve en una dilatada jurisprudencia constitucional al considerar el alto Tribunal que *«El derecho a la tutela efectiva que dicho artículo consagra no agota su contenido en la exi-*

190 GUZMÁN FLUJA, V., «Automated justice. La preocupante tendencia hacia la justicia penal...», *op. cit.*, pág. 344.

191 STC 46/1982 de 12 de julio.

gencia de que el interesado tenga acceso a los Tribunales de Justicia, pueda ante ellos manifestar y defender su pretensión jurídica en igualdad con las otras partes y goce de la libertad de aportar todas aquellas pruebas que procesalmente fueran oportunas y admisibles, ni se limita a garantizar la obtención de una resolución de fondo fundada en derecho, sea o no favorable a la pretensión formulada, si concurren todos los requisitos procesales para ello. Exige también que el fallo judicial se cumpla y que el recurrente sea repuesto en su derecho y compensado, si hubiere lugar a ello, por el daño sufrido: lo contrario sería convertir las decisiones judiciales y el reconocimiento de los derechos que ellas comportan en favor de alguna de las partes, en meras declaraciones de intenciones¹⁹².

Sin embargo, es notorio que la resolución de los conflictos puede derivarse a instancias distintas de la judicial. El arbitraje y la mediación han reclamado su lugar entre los métodos de resolución de conflictos, pero la LO 1/2025, de 2 de enero, de medidas en materia de eficiencia del Servicio Público de Justicia, que convierte la mediación en un presupuesto del acceso a la vía jurisdiccional, se refiere ya a otras formas de solución, como la negociación, o la opinión neutral de una persona independiente¹⁹³. No es esta la ocasión para detenerse en esta cuestión, que, al tratarse de un derecho fundamental de tanta trascendencia, exigiría un estudio reflexivo y riguroso, pero sí para apuntar que hay voces que reclaman la posible evolución del derecho regulado en el artículo 24.1 CE, que parece exigir una nueva configuración en cuanto a su contenido¹⁹⁴.

En relación con el acceso a los tribunales, como primer paso en el ejercicio del derecho a la tutela judicial efectiva, resulta evidente que los sistemas de IA no pueden privar al ciudadano del acceso a los órganos jurisdiccionales. Atribuir la resolución de los conflictos a los sistemas de IA, y más concretamente a los hoy denominados jueces-robots, supondría un cambio sustancial de la potestad jurisdiccional, alejada de la función de los órganos jurisdiccional de juzgar y hacer ejecutar lo juzgado¹⁹⁵.

En este sentido, la Carta ética europea sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno, adoptada por la Comisión Europea

192 STC 32/1982, de 7 de junio; 26/1983, de 13 de abril. V. CARRASCO DURÁN, M., «La definición constitucional del derecho a la tutela judicial efectiva» en *UNED. Revista de Derecho político* número 107, 2020, pág. 13 y ss.

193 V. en este sentido el artículo 5 de la LO 1/2025, de 2 de enero, de medidas en materia de eficiencia del servicio público de justicia.

194 MARTÍN DÍZ, F., «Del derecho a la tutela judicial efectiva hacia el derecho a una tutela efectiva de la justicia» en *Revista Europea de Derechos Fundamentales*, primer semestre 2014, número 23, págs. 161-176; BARONA VILAR, S., *Solución extrajurisdiccional de conflictos. Alternative Dispute Resolution (ADR) y Derecho Procesal*, Tirant lo Blanch, Valencia, 1999.

195 BUENO DE MATA, F., «Macrodatos, inteligencia artificial y proceso: luces y sombras», *Revista General de Derecho Procesal*, número 51, 2020, pág. 18.

para la Eficiencia de la Justicia (CEPEJ), en diciembre de 2018, ya señalaba que «cuando se utilizan herramientas de inteligencia artificial para resolver una disputa o como una herramienta para ayudar en la toma de decisiones judiciales o para brindar orientación al público, es esencial asegurarse de que no socaven las garantías del derecho de acceso al juez y el derecho a un juicio justo».

Ello implica que ha de garantizarse en todo caso el derecho de acceso a los tribunales, y que los sistemas predictivos relacionados con el éxito en la contienda, no puede suponer en ningún caso un obstáculo, o incluso una prohibición, para que el ciudadano pueda recabar el pronunciamiento de los órganos jurisdiccionales¹⁹⁶.

No es posible dejar de hacer un comentario sobre la designación de los sistemas de IA destinados a resolver conflictos, como «jueces-robots». La propia denominación ya es un sin sentido, porque implica por sí misma una ofensa a la labor desarrollada por los jueces y magistrados, que va mucho más allá del análisis de los datos obrantes en un proceso¹⁹⁷. En este sentido, la labor jurisdiccional no se limita al conocimiento de las normas jurídicas y de la jurisprudencia, se integran también en la función jurisdiccional la supervisión de los derechos de las partes, y del cumplimiento de las garantías del proceso y requisitos del procedimiento¹⁹⁸. De esta forma, «decidir» no es lo mismo que ejecutar programas. La «resolución» electrónica de asuntos que pueden automatizarse no es una «decisión». Si todo estuviera programado no habría nada que decidir. La decisión propiamente dicha no es aplicación mecánica de un programa. El jurista decide en la medida en que su actividad no está programada¹⁹⁹.

La decisión judicial se obtiene a partir del estudio del caso concreto, del material fáctico obrante en autos, y de la actividad probatoria practicada en el proceso²⁰⁰. En función de las alegaciones de las partes y de la actividad desplegada en el proceso, el juez realiza un pronunciamiento jurisdiccional aplicando la ley. Es obvio, a pesar de lo que popularmente se dice, que no

196 MARTÍN DÍZ, F., «Modelos de aplicación de Inteligencia Artificial en justicia: asistencial o predictiva versus decisoria», en *Justicia algorítmica y Neuroderecho...*, op. cit., pág. 75

197 Un importante estudio sobre el juez robot puede encontrarse en GÓMEZ COLOMER, J.L. *El juez robot. La independencia judicial en peligro*, Tirant lo Blanch, Valencia, 2023.

198 SAN MIGUEL DEL CASO, C., «Inteligencia artificial y algoritmos: la controvertida evolución de la tutela judicial efectiva en el proceso penal» en *Estudios Penales...*, op. cit., <https://doi.org/10.15304/epc.44.8859>, pág. 9.

199 MARTÍNEZ GARCÍA, J.I., «Inteligencia y derechos humanos en la sociedad digital», en *Cuadernos electrónicos de Filosofía del Derecho*, número 40, 2019, pág. 171. V. también MARCHENA GÓMEZ, M., «Inteligencia artificial y jurisdicción penal», *Discurso leído por el Excmo. Sr. Dr. D. Manuel Marchena Gómez en el acto de su recepción como Académico de número de la Real Academia de Doctores de España*, <https://confilegal.com/wp-content/uploads/2023/03/INTELIGENCIA-ARTIFICIAL-INGRESO-MARCHENA-REAL-ACADEMIA-DE-DOCTORES-.pdf>, pág. 47.

200 V. más ampliamente GÓMEZ COLOMER, J.L., *El juez robot...*, op. cit., págs. 261-268.

hay dos casos exactamente iguales. Los escritos de alegaciones de las partes, la aportación del material fáctico, la actividad investigadora desarrollada en la fase de instrucción, la introducción del material probatorio, y un largo etcétera, condicionan indudablemente el pronunciamiento judicial²⁰¹. A todos estos factores ha de atender el juzgador en su pronunciamiento jurisdiccional, aplicando la ley al caso concreto con todos los condicionantes que le rodean, dejando al margen, en la medida de lo posible, otro tipo de influencias personales, o de carácter subjetivo. Para garantizar que esta actividad jurisdiccional no se encuentre condicionada por elementos subjetivos o externos a la labor jurisdiccional, se arbitran legalmente las conocidas causas de abstención y recusación. ¿Podrían arbitrase mecanismos similares respecto de los sistemas de inteligencia artificial?²⁰². Obviamente, no con la intención de recusar al «juez robot», sino a los técnicos o personas que han decidido sobre la introducción de los datos que han de servir de base en la ejecución del programa.

Además, la norma exige su interpretación que, partiendo del artículo 3 CC, deberá atender al «*sentido propio de sus palabras, en relación con el contexto, los antecedentes históricos y legislativos y la realidad social del tiempo en que han de ser aplicadas, atendiendo fundamentalmente al espíritu y finalidad de aquellas*». Parece complicado que un sistema de IA pueda llevar a cabo una interpretación legal en el sentido descrito, y mucho más cuando la realidad social es cambiante y sus variaciones su producen, cada vez, en un espacio más corto de tiempo²⁰³. Aunque el razonamiento lógico se encuentra en la base de la toma de decisiones judiciales, no puede atribuírsele todo el peso del juicio, ya que en la valoración de los hechos y la interpretación del material probatorio entran en juego diferentes factores a los que el juzgador ha de enfrentarse utilizando la empatía, la experiencia, el sentido común, etc...²⁰⁴. El juez también ha de valorar la realidad de los hechos aportados en el proceso, y en esa labor del convencimiento judicial que persigue la actividad probatoria, tienen una influencia no poco considerable las emociones, percepciones, intuiciones y lo que se conoce como sensibilidades subjetivas, lo que, en definitiva, está lejos de integrarse en un sistema de expertos de IA²⁰⁵.

201 V. más ampliamente MARCHENA GÓMEZ, M., «Inteligencia artificial y jurisdicción penal...» *op. cit.*, págs. 48-56.

202 Sobre esta cuestión v ampliamente GÓMEZ COLOMER, J.L., «Unas reflexiones sobre el llamado «juez-robot...», *op. cit.*, pág. 250 y ss.

203 V. ARMENTA DEU, T. «El proceso en la Europa digital: entre recuperar liderazgos y proteger derechos», en *Uso de la información y de los datos personales en los procesos: los cambios en la era digital*, (Colomer Hernández, Dir.), Aranzadi, Cizur Menor, 2022.

204 SOLAR CAYÓN, J.I., «Reflexiones sobre la aplicación de la Inteligencia artificial en la Administración de justicia», en *Teoría jurídica contemporánea*, volumen 6, 2021, pág. 9.

205 BARONA VILAR, S. «Una justicia «digital» y «algorítmica» para una sociedad en estado de mudanza» en *Justicia algorítmica...*, *op. cit.*, pág. 47. V. también FAGGIANI, V., «El derecho

Tampoco puede argumentarse que la decisión adoptada por un sistema de inteligencia artificial resulta desprovista de subjetivismo, o de valoraciones individuales o ideológicas²⁰⁶. Una vez más ha de precisarse, que su programación parte de los datos proporcionados, que se nutren de hechos y situaciones del pasado. La información con la que se dota al algoritmo es consecuencia de datos derivados de decisiones humanas anteriores, que, como tales, están cargadas de valoraciones subjetivas, sesgos ideológicos y factores procedentes de una valoración humana anterior. Como ya se ha apuntado con anterioridad, los hechos y situaciones pasadas, al igual que la interpretación normativa de épocas anteriores, no pueden condicionar la evolución normativa, y la interpretación de las leyes conforme a la sociedad en la que la que se están aplicando²⁰⁷.

Es importante poner de relieve el grave perjuicio que se causaría a la evolución en la interpretación de las normas jurídicas. La interpretación de la norma conforme a la realidad social del tiempo en el que han de aplicarse, se vería en peligro al acudir a decisiones pasadas. La resolución de casos anteriores, más o menos similares, cerrarían el paso a argumentaciones más actuales y conformes con la realidad actual²⁰⁸.

La motivación de las resoluciones dictadas también forma parte del contenido esencial del derecho a la tutela judicial efectiva²⁰⁹. En el caso de la utilización de sistemas de expertos, el juez podrá motivar en su resolución la influencia que ha tenido dicho sistema en la toma de la decisión, tanto si ha seguido su indicación, como si se ha apartado de ella²¹⁰. Sin embargo, no puede concluirse lo mismo si lo que se pretende es que el sistema de experto dicte la resolución. En este caso, la motivación corresponderá siempre al ser humano, porque la IA no puede actualmente incorporar todas aquellas percepciones y premisas que exige la motivación y la argumentación jurídica. En la motivación de las resoluciones judiciales se integran elementos de valora-

a un proceso con todas las garantías ante los cambios de paradigma de la inteligencia artificial», en *UNED. Teoría y Realidad Constitucional*, número 50, 2022, pág. 526; GÓMEZ COLOMER, J.L., «Unas reflexiones sobre el llamado «juez-robot»...», *op. cit.*, pág. 253.

206 MIRÓ LLINARES, F., «Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots», *Revista de Derecho Penal y Criminología*, 3.ª Época, número 20 (julio de 2018), pág. 121.

207 BORGES BLAZQUEZ, R., «La inteligencia artificial en el proceso penal y el ¿regreso? de Lombroso» en *Justicia algorítmica...*, *op. cit.*, pág. 180-

208 V. MARCHENA GÓMEZ, M., «Inteligencia artificial y jurisdicción penal...», *op. cit.*, pág. 48.

209 Sobre la argumentación jurídica y la motivación v. BARONA VILAR, S., «Argumentación jurídica, prueba, judicial decisión y robotización judicial: hacia la smart justice», en *Algoritmización de la justicia...*, *op. cit.*, pág. 543 y ss.

210 MARTÍN DIZ, F., «Modelos de aplicación de Inteligencia Artificial...», *op. cit.*, pág. 78.

ción probatoria y de la percepción del juez en la práctica de la prueba, para eso se ha regulado la exigencia de la inmediación²¹¹.

Sería complicado que la motivación de las resoluciones del «juez-robot» puedan atribuirse a los jueces o magistrados que las supervisan, principalmente por el desconocimiento del funcionamiento interno del sistema inteligente. Como es sabido, uno de los principales inconvenientes que se predicen de la IA, es la falta de transparencia en su funcionamiento, lo que provoca, en muchas ocasiones, que el resultado propuesto por la máquina no pueda ser explicado, y por tanto no pueda ser motivado²¹². No puede el juzgador humano explicar la decisión tomada por el juzgador robot, cuando desconoce las causas que la han propiciado, ni las «valoraciones» que ha realizado para dar certeza a unos hechos y negar la realidad de otros. ¿Cómo explicar o justificar una decisión en la que no se ha participado, y que parte de un procedimiento en el que no se ha estado presente, y en una valoración de pruebas cuya práctica ha sido ajena?²¹³

2.2. Derecho de defensa e Inteligencia artificial

El derecho de defensa se configura como uno de los derechos fundamentales más relevantes, sin cuya observancia no se puede garantizar una justicia propia de un Estado de Derecho²¹⁴. Su respeto y valor fundamental constituye una de las premisas sobre las que se asienta nuestro proceso penal, que se erige en el instrumento necesario para la aplicación del Derecho penal y el ejercicio del *ius puniendi* del Estado. Sirve para garantizar la seguridad pública, pero también ha de preservar o garantizar los derechos de la persona investigada.

El ordenamiento jurídico ha rodeado al «imputado»²¹⁵ de un conjunto de garantías que configuran un *status* procesal ya asentado en la cultura jurí-

211 GÓMEZ COLOMER, J.L., «Unas reflexiones sobre el llamado “juez-robot...”», *op. cit.*, pág. 257.

212 SAN MIGUEL DEL CASO, C., «Inteligencia artificial y algoritmos...», *op. cit.*, pág. 12.

213 Sobre la motivación y argumentación jurídica ver el importante estudio de BARONA VILAR, S., *Algoritmización del derecho y de la justicia...*, *op. cit.*, 2021, págs. 550 y ss.

214 Sobre el origen de la defensa y su evolución v. GONZÁLEZ-CUELLAR SERRANO, N., «El derecho de defensa y la marca de Caín», en *Nuevos debates en torno a la justicia española* (Castillejo Manzanares, dir.), Editorial Tirant lo Blanca, Valencia, 2017, págs. 289 y ss.

215 El término «imputado», utilizado para designar a aquella persona que estaba siendo objeto de una investigación judicial, ha sido sustituido por «investigado». La ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, en su exposición de motivos explica las razones para este cambio, señalando que «tiene por objeto adaptar el lenguaje de la Ley de Enjuiciamiento Criminal a los tiempos actuales y, en particular, eliminar determinadas expresiones usadas de modo indiscriminado en la ley, sin ningún tipo de rigor conceptual, tales como imputado, con la

dica occidental, que nuestra Constitución consagra en su art. 24²¹⁶. La mera imputación le confiere una pluralidad de derechos instrumentales de carácter constitucional que se engarzan en el contenido del derecho de defensa y que deben ser escrupulosamente respetados²¹⁷.

Este conjunto de garantías, o derechos que conforman el derecho de defensa se encuentran estrechamente vinculados al principio de contradicción que impera en el proceso penal, que precisa de un justo equilibrio entre las partes, y por tanto del respeto al principio de igualdad de armas²¹⁸.

La contradicción, calificada como una de las garantías esenciales del proceso penal del Estado de Derecho²¹⁹, es consustancial a la idea misma de proceso y constituye un principio general de la justicia penal²²⁰, tal y como

que se alude a la persona sobre la que tan sólo recaen meras sospechas y por ello resulta investigado, pero respecto de la cual no existen suficientes indicios para que se le atribuya judicial y formalmente la comisión de un hecho punible». Conforme a ello el término investigado «...servirá para identificar a la persona sometida a investigación por su relación con un delito; mientras que con el término encausado se designará, de manera general, a aquél a quien la autoridad judicial, una vez concluida la instrucción de la causa, imputa formalmente el haber participado en la comisión de un hecho delictivo concreto». Así, conforme a las modificaciones introducidas, el sujeto sometido a un proceso penal recibirá la denominación de «investigado» cuando todavía no se ha dictado una resolución judicial que le atribuya indiciariamente el hecho delictivo; se llamará «encausado» desde el momento en que se dicte esta resolución. En los procesos ordinarios que se instruyen mediante el sumario, en este momento de atribución judicial del hecho se les denomina «procesados». Finalmente, una vez que se produce la calificación provisional de la acusación en su contra se les denomina «acusados».

- 216 V. SSTC 205/1989, de 11 de diciembre, 161/1994, de 23 de mayo, y 277/1994, de 17 de octubre, entre otras.
- 217 MORENO CATENA, V., «La garantía de los derechos fundamentales durante la investigación penal» en *Cuadernos penales* José María Lidón, número 7, 2010, págs. 18-19.
- 218 V. en este sentido GIMENO SENDRA, V., «El derecho de defensa», en *Constitución y proceso*, Editorial Tecnos, Madrid, 1988, pág. 88. En este sentido considera el Tribunal Supremo que «...el derecho a un proceso público con todas las garantías, de acuerdo con los arts. 11 de la Declaración Universal de Derechos Humanos, 14 del Pacto Internacional de Nueva York de 1966 y 6 del Convenio de Roma de 1950, implica que para evitar el desequilibrio entre las partes, ambas dispongan de las mismas posibilidades en cuanto a alegaciones, pruebas e impugnaciones, lo que cobra singular relevancia en el juicio oral y en lo que es propiamente dicho la actividad probatoria, derecho que se conecta con las garantías en general contenidas en el art. 24 constitucional». V. SSTs de 15 abril 1996 y 1686/1997 de 10 septiembre.
- 219 Así lo señala DE URBANO CASTRILLO, E., «El principio de contradicción en el proceso penal», en *Diario La Ley*, número 5474, 4 Feb. 2002, pág. 1712, cuando afirma que «...una concepción propia de un Estado de Derecho social que propugna la consecución real y efectiva de la igualdad y demás derechos y libertades fundamentales, sólo puede operar, por lo que a la cuestión que tratamos se refiere, si de la audiencia como garantía del proceso se pasa a la contradicción como esencia del mismo...».
- 220 V. CALAMANDREI, P., *Proceso y democracia*, Editoriales jurídicas Europa-América, Buenos Aires, 1960, pág. 147. DE LA OLIVA SANTOS, A., *Derecho procesal* (con Díez-Picazo Giménez y Vegas Torres); MORENO CATENA, V., «Algunos problemas del derecho de defensa» en *Justicia*,

se pone de relieve en numerosas resoluciones judiciales²²¹. Su efectividad supone que las partes puedan hacer valer sus pretensiones a través de la introducción de hechos y pruebas, conociendo el material obrante en el proceso, e interviniendo en su desarrollo con el ánimo de influir en la resolución judicial²²². En este sentido, la contradicción se identifica con la igualdad de las partes en el proceso, y con la facultad de reconocerles la posibilidad de oponerse a la pretensión del adversario²²³. Se trata pues de facilitar la oposición, y el debate o discusión sobre la pretensión, a través de la comparecencia en el proceso y la introducción de hechos y pruebas²²⁴.

No hay en la Constitución una referencia expresa al principio de contradicción, pero su reconocimiento se entiende implícito en el art. 24, tanto en su primer apartado, que al declarar el derecho a la tutela judicial efectiva pro-

número 3, 1990, pág. 562; MONTERO AROCA, J., *Principios del proceso penal. Una explicación basada en la razón*. Tirant lo Blanch, Valencia, 1997, pág. 139, entre otros.

- 221 A título de ejemplo la sentencia 49/2008, de 25 de febrero, en la que el Tribunal Supremo considera que «...la importación de un acto procesal generado en un marco jurídico distinto, no debe hacerse con quiebra de uno de los principios estructurales del proceso penal, el principio de contradicción, ni puede menoscabar el derecho de defensa. La Sala, en fin, no puede considerar desplazada la presunción de inocencia que ampara a cualquier imputado cuando la condena se basa en la declaración de un testigo presencial de los hechos que nunca ha visto al acusado y que, además, nunca ha podido ser interrogado por el Letrado de la defensa del imputado».
- 222 V. PLANCHADELL GARGALLO, A., *El derecho fundamental a ser informado de la acusación*, Tirant lo Blanch, Valencia, 1999, pág., 77.
- 223 V. GUTIERREZ ALVIZ CONRRADI, F., *El derecho de defensa y la profesión de abogado*, Atelier, 2012, pág. 20; V. también CARNELUTTI, *Derecho y proceso* (traducido por Sentis Melendo), Buenos Aires, 1971, págs. 112 y ss.; GUASP DELGADO, J., *Derecho Procesal Civil*, Madrid, 1968, pág. 171.
- 224 Así lo pone de relieve el Tribunal Constitucional al considerar que del derecho a «...intervenir en el debate procesal en condiciones que respeten la contradicción, con todas las garantías (art. 24.2 C.E.), sólo son titulares del mismo las partes personadas en el momento oportuno, sin que corresponda a quienes carezcan de legitimación pasiva necesaria o lleguen tardíamente, por su negligencia, a las actuaciones. Como ya dijimos en la STC 109/1985, la indefensión, o falta de garantías, derivadas de la ausencia de contradicción no deben apreciarse cuando «la parte que pudo defender sus derechos e intereses legítimos, a través de los medios que ofrece el ordenamiento jurídico, no usó de ellos con la pericia técnica suficiente —Sentencias de 7 de julio de 1983 y 11 de julio de 1985—, o cuando la parte que invoca la indefensión colabora con su conducta a su producción —Sentencia de 11 de junio de 1984—, pues en ella no ha de tener actuación quien se sienta agraviado y la invoca, ya que si la lesión se debe de manera relevante a la inactividad o negligencia, por falta de la diligencia procesal exigible al lesionado, o se genera por la voluntaria actuación desacertada, equívoca o errónea de dicha parte —Sentencias de 11 de junio de 1984 y de 17 de julio de 1985, y autos de la Sala Segunda de 7 y 21 de noviembre de 1984—, la indefensión resulta absolutamente irrelevante a efectos constitucionales, porque al causante de ella le es imputable su presencia, no pudiendo reunir a la vez la doble condición de autor y de perjudicado, y si la creó con su comportamiento doloso o negligente, no es posible beneficiarle con su reconocimiento y consecuencias»». V. STC 155/1995, de 24 de octubre.

híbe la indefensión, como en el segundo, al regular el derecho de defensa y el derecho a un proceso con todas las garantías²²⁵.

Para el Tribunal Constitucional, «...entre las garantías que comprende el art. 24 CE para todo proceso penal destacan, por ser principios consustanciales al mismo, las de contradicción e igualdad. Según una constante y reiterada doctrina de este Tribunal, el art. 24 CE, en cuanto reconoce los derechos a la tutela judicial efectiva con interdicción de indefensión, a un proceso con todas las garantías y a la defensa, ha consagrado, entre otros, los citados principios de contradicción e igualdad, garantizando el libre acceso de las partes al proceso en defensa de sus derechos e intereses legítimos. Ello impone, entre otras exigencias, la necesidad de que todo proceso penal esté presidido por la posibilidad de una efectiva y equilibrada contradicción entre las partes a fin de que puedan defender sus derechos, así como la obligación de que los órganos judiciales promuevan el debate procesal en condiciones que respeten la contradicción e igualdad entre acusación y defensa»²²⁶. El alto Tribunal vincula la exigencia de contradicción al derecho a un proceso con todas las garantías, que requiere para su efectividad el compromiso de los órganos jurisdiccionales²²⁷.

En el mismo sentido se pronuncia el Tribunal Supremo, al señalar que «entre las garantías que comprende el art. 24 CE para todo proceso penal destaca, por ser principios consustanciales del mismo, los de contradicción e igualdad. El principio de contradicción en el proceso penal hace posible el enfrentamiento dialéctico entre las partes, permitiendo así el conocimiento de los argumentos de la contraria y la manifestación ante el Juez o Tribunal de los propios, constituye una exigencia ineludible vinculada al derecho a un

225 V. MORENO CATENA, V., *La defensa penal*, Editorial Civitas, Madrid, 1982, pág. 25; CORTÉS DOMÍNGUEZ, V., *Introducción al Derecho Procesal*, (con Moreno Catena), Editorial Tirant lo Blanch, Valencia, 2016, pág. 242; GIMENO SENDRA, V., *Introducción al Derecho Procesal*, Editorial Colex, Madrid, 2014, pág. 276; MONTERO AROCA, J., *Derecho Jurisdiccional I. Parte general* (con Gómez Colomer, Montón Redondo y Barona Vilar), Editorial Tirant lo Blanch, Valencia 2014, pág. 246.

226 V. SSTC 53/1987, de 7 de mayo; 66/1989, de 17 de abril; 186/1990, de 15 de noviembre.

227 Como señala el Tribunal en la sentencia 178/2001, de 17 de septiembre, «...en el proceso penal, además, la necesidad de contradicción y equilibrio entre las partes está reforzada por la vigencia del principio acusatorio —que también forma parte de las garantías sustanciales del proceso— el cual, entre otras consecuencias, impone la necesidad de que la función de la acusación sea acometida por un sujeto distinto al órgano decisor (nemo iudex sin accusatore) y de que el objeto procesal sea resuelto por un órgano judicial independiente e imparcial, para lo cual es imprescindible disponer de la posibilidad de conocer los argumentos de la otra parte y manifestar ante el Juez los propios, así como poder acreditar los elementos fácticos y jurídicos que fundamentan las respectivas pretensiones». V. en el mismo sentido las SSTC 179/2002, de 14 de octubre, 8/2003, de 20 de enero, 143/2004, de 13 de septiembre, 182/2009 de 7 septiembre; y 53/1987, de 7 de mayo; 18/1995 de 24 enero; 162/1997, de 3 de octubre; 16/2000, de 31 de enero; 79/2000, de 27 de marzo; 93/2000, de 10 de abril; 101/2001, de 23 de abril.

proceso público con todas las garantías, para cuya observancia se requiere el deber de los órganos judiciales de posibilitarlo. Y se vulnera el derecho a la tutela judicial efectiva del art. 24.1 CE, produciendo indefensión, cuando el sujeto, sin haber tenido oportunidad de alegar y probar sus derechos en el proceso, los ve finalmente afectados por las resoluciones recaídas en el mismo. Del principio de igualdad de armas, lógico corolario del principio de contradicción, se deriva asimismo la necesidad de que las partes cuenten con los mismos medios de ataque y defensa e idénticas posibilidades y cargas de alegación, prueba e impugnación, a efectos de evitar desequilibrios entre sus respectivas posiciones procesales, ni que sean admisibles limitaciones a dicho principio, fuera de las modulaciones o excepciones que puedan establecerse en fase de instrucción (o sumarial) por razón de la propia naturaleza de la actividad investigadora que en ella se desarrolla encaminada a asegurar el éxito de la investigación y en definitiva, la protección del valor constitucional de la justicia»²²⁸

Doctrina y jurisprudencia destacan el carácter poliédrico del derecho de defensa en el que se incluyen un conjunto de derechos instrumentales que conforman las garantías procesales consustanciales al Estado de Derecho, y que se recogen en el segundo apartado del art. 24 CE²²⁹. Los derechos a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, y a no confesarse culpables, conforman el contenido

228 STS 806/2012, de 23 octubre. Así considera el Tribunal Supremo en la STS 974/2012, de 5 diciembre que «La efectiva realización de los principios de igualdad de las partes y contradicción que imponen a los órganos judiciales el deber positivo de evitar desequilibrios entre la respectiva posición procesal de las partes y evitar limitaciones en la defensa que puedan generar indefensión, prohibida por el art. 24.1CE, lo que reclama un cuidadoso esfuerzo del órgano jurisdiccional para garantizar la plena efectividad de los derechos de defensa en las distintas fases e instancias del proceso». V. también la STC 178/2001, de 17 de septiembre. En el mismo sentido las SSTs 1080/2006, de 2 de noviembre; 1238/2009, de 11 de diciembre; 383/2010, de 5 de mayo; 365/2012, de 15 de mayo; 775/2012, de 17 de octubre; 125/2012, de 29 de diciembre.

229 V. en este sentido MORENO CATENA, V., *La defensa penal*, op. cit., págs. 24-25; GÓMEZ COLOMER, J.L., *Derecho Jurisdiccional III. Proceso Penal*, Editorial Tirant lo Blanch, Valencia, 2012, pág. 247; GIMENO SENDRA, V., en *Los procesos penales* (con Conde-Pumpido Tourón y Garberí Llobregat.), tomo II, Editorial Bosch, Barcelona 2000, pág. 166; DE URBANO CASTRILLO, E., «El principio de contradicción en el proceso penal», en *Diario La Ley*, número 5474, 4 Feb. 2002, pág. 1172; LÓPEZ YAGÜE, V., «La condición de imputado en el proceso penal español. Formas de adquisición y status jurídico que conlleva. Ideas para su reforma», en *La reforma del proceso penal*, Editorial LA LEY, Madrid, 2011; PLANCHADELL GARGALLO, A., *El derecho fundamental...*, op. cit., pág. 82; RUIZ VADILLO, E., «Algunas breves consideraciones sobre el sistema acusatorio y la interdicción constitucional de toda indefensión en el proceso penal», en *Diario La Ley*, tomo 4, 1987, pág. 874; SERRANO RUIZ-CALDERÓN, J.M., «El derecho de defensa según la sentencia 79/2012 de la Sala de lo Penal del Tribunal Supremo» en *Diario La Ley*, número 7850, 3 mayo 2012, pág. 5.

esencial del derecho de defensa, y se integran, además, en el contenido esencial del derecho a un proceso con todas las garantías, o al debido proceso²³⁰.

Partiendo de estas consideraciones, en un proceso penal en el que se utilicen sistemas de inteligencia artificial, el derecho de defensa puede verse gravemente afectado, y ello puede comprobarse fácilmente con la simple referencia a las siguientes cuestiones. Estos sistemas de IA van a suponer un alto coste para los despachos de abogados que quieran disponer de ellos, porque desde luego no se trata de sistemas de fácil acceso para la gran mayoría de los despachos. Este simple hecho va a provocar que algunos sujetos puedan acceder a estos sistemas de apoyo a la estrategia procesal de defensa, mientras que otros, con menos recursos económicos, no se pueden beneficiar de su aplicación, lo que indirectamente va a provocar que la posición de partida de las partes en el proceso resulte ya muy desigual²³¹.

Una segunda cuestión de interés, es la aplicación de los sistemas predictivos para elaborar una estrategia de defensa, e incluso para que dicha defensa se asuma por un abogado o despacho concreto. En este sentido, el acceso a este tipo de instrumentos y al análisis que se extraiga del sistema, puede influir de forma definitiva sobre la viabilidad del caso y la decisión de aceptar la defensa. La complejidad del tema, y, desde luego, la predicción de un mal resultado, puede llevar al profesional a rechazar la defensa, colocando al sujeto investigado en una difícil situación, afectando al derecho a la defensa, pero también a la igualdad de armas y al derecho a la tutela judicial efectiva²³².

De todos es conocida la utilización del sistema COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), que se basa en un algoritmo diseñado por una empresa privada norteamericana para medir el riesgo de reincidencia de los acusados. Su evaluación parte de una serie de variables, o factores de riesgo que se introducen en el sistema, centrándose la labor del algoritmo en determinar el grado de probabilidad de reincidencia

230 Este derecho aparece recogido en los arts. 10 y 11 de la Declaración Universal de Derechos Humanos de 1948, el art. 6 del Convenio Europeo de Derechos Humanos de 1950, y el art. 14 del Pacto Internacional de Derechos Civiles y Políticos de 1966. Sobre su contenido es necesario precisar que el Tribunal Constitucional ha realizado una interpretación excesivamente amplia del primer apartado del art. 24 CE, tutela judicial efectiva, integrando en su contenido los múltiples derechos que se recogen en el segundo apartado, y que hacen referencia a los instrumentos procesales que se ponen a disposición del ciudadano reclamante de tutela. Esta interpretación se encuentra directamente relacionada con la prohibición de indefensión que prevé el primer apartado del precepto citado, pero lo cierto es que prácticamente ha vaciado de contenido el derecho al debido proceso. V. en este sentido MORENO CATENA, V., *Introducción al Derecho Procesal* (con Cortés Domínguez), Editorial Tirant lo Blanch, Valencia, 2012, pág. 201.

231 MARTÍN DIZ, F., «Inteligencia artificial y proceso...», *op. cit.*, pág. 5; SAN MIGUEL CASO, C., «La aplicación de la Inteligencia Artificial...», *op. cit.*, pág. 292

232 SAN MIGUEL CASO, C., «La aplicación de la Inteligencia Artificial...», *op. cit.*, pág. 292.

en función del peso de cada variable. Las variables introducidas en el sistema se basan en el origen, raza, entorno familiar y social, historial delictivo, adicción a sustancias estupefacientes y al alcohol, situación laboral y económica, y, en definitiva, toda una serie de factores introducidos sin control oficial alguno y que, sin embargo, pueden influir decisivamente en una resolución judicial sobre la prisión provisional u otras medidas cautelares²³³.

No cabe duda que la utilización de este tipo de sistemas en el proceso penal incide en el derecho de defensa. La introducción de los factores de riesgo se realiza sin contradicción, por parte de sujetos que tampoco están vinculados a ningún control oficial. Su dependencia profesional de una empresa privada y su obligación hacia el secreto empresarial, impide en principio conocer su estructura y funcionamiento, por lo que hace imposible impugnar su fiabilidad²³⁴. Este problema puede solucionarse condicionando legalmente su aplicación en el proceso, a que se facilite el acceso a la información y al funcionamiento del sistema, aunque, como ya se ha apuntado, en algunas ocasiones el cruce de datos del sistema escapa incluso al entendimiento de su programador, lo que representa un serio problema²³⁵.

Por tanto, la opacidad del sistema, tanta veces criticada y atacada, pero a la que no se le ha puesto remedio, supone un grave inconveniente para el ejercicio del derecho de defensa. No sólo afecta a la posibilidad de recurrir la resolución, al desconocerse el modo en el que se ha obtenido, sino que, por el mismo motivo, también impide la proposición de medios o pruebas que la contradigan.

En el mismo orden de consideraciones, tampoco se puede obviar la entrada en el proceso penal de informes policiales basados en técnicas de IA, que adquieren la categoría de prueba pericial especial o «*sui generis*»²³⁶, al estar basada en conocimientos técnicos y especializados, pero cuya introducción en el proceso penal conlleva un grave problema para los derechos de defensa y la contradicción²³⁷. No puede mantenerse que tales informes estén exentos del debate contradictorio, pero al realizarse por técnicos de alto nivel, con

233 V. BORGES BLAZQUEZ, R., «El sesgo de la máquina en la toma de decisiones en el proceso penal», en *Ius Et Scientia*, volumen 6, número 2, 2020, págs. 61 y ss.; GASCÓN INCHAUSTI, F., «Desafíos para el proceso penal...», *op. cit.*, pág. 202; MIRÓ LLINARES, F., «Inteligencia artificial y justicia penal...», *op. cit.*, págs. 108 y ss.

234 GASCÓN INCHAUSTI, F., «Desafíos para el proceso penal...», *op. cit.*, pág. 203.

235 PÉREZ ESTRADA, M.J. *Fundamentos jurídicos para el uso de la inteligencia artificial en los órganos judiciales*, Tirant lo Blanch, Valencia, 2022, pág. 139.

236 V. STS 783/2007, de 1 de octubre; V. también la STS 124/2009, de 13 de febrero; 290/2010, de 31 de marzo.

237 V. BUENO DE MATA, F., *Investigación y prueba de delitos de odio en Redes Sociales: Técnicas Osint e inteligencia policial*, Tirant lo Blanch, Valencia, 2023, págs. 241 y ss-

instrumentos complejos y en condiciones específicas, va a resultar muy complicado elaborar un contrainforme, e incluso rebatir el aportado²³⁸.

Además, en este campo, es preciso diferenciar los informes encargados en el marco de una investigación penal, que, realizados por unidades policiales se incorporan al proceso y deben cumplir ya de partida con el marco de garantías del proceso penal, de aquellos otros llevados a cabo por los servicios de inteligencia del Estado, al margen del proceso, y cuya incorporación se pretende con posterioridad. Habrá que analizar, en este caso, si el procedimiento de elaboración y de tratamiento de este tipo de informes puede ser contrastada en el proceso, o al elaborarse por estos servicios especiales, quedan al margen de su control. En este último caso, su incorporación al proceso ofrece serias dudas al incidir en el derecho a un proceso con todas las garantías y en el derecho de defensa²³⁹.

Otra cuestión a tener en cuenta, que se encuentra estrechamente ligada al ejercicio efectivo de la defensa, está vinculada al derecho a la información, que constituye un presupuesto básico del principio de contradicción y del derecho de defensa. Es cierto que este derecho se centra ahora en la información de la acusación y de los hechos que se imputan²⁴⁰. Pero, también es cierto que, el primero investigado, y después acusado, ha de conocer las diligencias de investigación practicadas y las fuentes de prueba que pueden tener acceso al proceso. Y es precisamente en esta cuestión en la que pueden derivarse problemas en la aplicación de sistemas inteligentes.

Como ya se ha apuntado en más de una ocasión, la opacidad de los instrumentos de IA constituye una de las principales dificultades que plantea su aplicación en el sistema de justicia, y más concretamente en el sistema de justicia penal. El desconocimiento sobre el funcionamiento de los algoritmos, cada vez más complejos, y de su evolución impide trasladar la información a la defensa, colocando al acusado en una muy difícil situación, no solo a la hora de rebatir y contradecir la información facilitada por el sistema inteligente, sino también en dos campos más: el de proponer pruebas que puedan rebatir lo afirmado por la IA, y el de convencer al juzgador de la posible inexactitud en la valoración de la máquina.

A esta dificultad contribuye la estrategia en la que puede colocarse la empresa diseñadora, al no facilitar toda la información sobre el funciona-

238 GUERRERO PALOMARES, S., «La denominada «prueba de inteligencia policial» o «pericial de inteligencia», en *Revista Aranzadi de Derecho y Proceso Penal*, número 25, 2011, página 13.

239 BARONA VILAR, S. *Algoritmización del Derecho y de la justicia*, op. cit., pág. 509.

240 STC 44/1983, de 24 de mayo. V. también las SSTC 54/1985, de 18 de abril; 141/1986, de 12 de noviembre; 17/1989, de 30 de enero; 277/1994, de 17 de octubre; 95/1995, de 19 de junio; 123/1995, de 18 de julio y 36/1996, de 11 de marzo; 19/2000, de 31 de enero; 278/2000, de 27 de noviembre y 182/2001 de 17 septiembre, entre otras. En el mismo sentido las SSTS de 4 de noviembre de 1986, 21 de abril de 1987 y 1232/2001 de 22 junio, entre otras.

miento del algoritmo amparándose en el secreto industrial, lo que podría evitarse con el diseño de algoritmos públicos controlados por la Administración²⁴¹.

Precisamente, es la dificultad de la información sobre el funcionamiento de los sistemas o aplicaciones de inteligencia artificial, lo que genera mayores dificultades. Las partes de un proceso penal, han de conocer el número de decisiones o casos que se han suministrado para que se pueda llevar a cabo su procesamiento cara a obtener una respuesta viable; se ha de conocer el origen de esas decisiones y cómo se han elegido, y que representatividad suponen entre todas las posibles; en definitiva ha de proporcionarse el material que se ha suministrado al sistema²⁴². Pero yendo más allá, sin conocer los datos de los que se nutre el sistema ni su funcionamiento, no sólo es complicado diseñar una estrategia de defensa y ponerla en marcha en un proceso, sino que, ante una resolución basada en soluciones aportadas por la IA sin la debida motivación, ya que el desconocimiento impide una justificación adecuada, su impugnación se convierte en una tarea prácticamente imposible.

Desde otra perspectiva, pero también tomando como punto de partida el ejercicio del derecho de defensa, otra de las cuestiones a la que ha de hacerse referencia es la relativa a las garantías que han de rodear la entrada en el proceso de la información derivada de la vigilancia policial utilizando instrumentos de IA. No es extraño que la policía realice labores de prevención a través de actuaciones de vigilancia genérica. En este contexto puede almacenarse información vinculada a una persona, sobre la que en ese momento no existe causa penal alguna²⁴³. Sin embargo, cuando se produce la *notitia criminis*, y se da inicio a la fase de investigación del proceso, la pregunta que cabe hacerse es si ese material derivado de una vigilancia genérica anterior puede ser introducido en el proceso. Ante esta situación cabe también preguntarse ¿qué líneas de actuación puede ejercer el sujeto ante la introducción de datos obtenidos de una vigilancia preprocesal, sin ninguna autorización judicial, ni vinculada a ninguna causa abierta? ¿Puede ser utilizada esta información, obtenida en una labor de prevención policial, y trasladarse, sin más, a una causa penal abierta posteriormente sobre el citado sujeto?²⁴⁴.

241 DE LUIS GARCÍA, E., «Justicia, inteligencia artificial y derecho de defense», en *Revista de internet, Derecho y política, Monográfico: «Digitalización y algoritmización de la justicia»* (coord.: Miró LLinares, coord.) <https://idp.uoc.edu/> pág. 6.

242 GÓMEZ COLOMER, J.L., «Derechos fundamentales, proceso e Inteligencia Artificial...», *op. cit.*, pág. 277

243 V. sobre esta cuestión COLOMER HERNÁNDEZ, I., «Control y límites en el uso de la información y los datos personales por parte de la Inteligencia Artificial en los procesos penales» en *Justicia algorítmica y neuroderecho...*, *op. cit.*, págs. 301 y ss.

244 V. GUZMÁN FLUJA, V., «Ideas para un debate sobre la predicción del crimen» en *Inteligencia artificial y Administración de Justicia...*, pág. 333.

Estas cuestiones exigen una regulación específica sobre la utilización de la información policial obtenida a través de sistemas de IA en labores de prevención, de igual forma a la que, en su momento, se reguló por la Ley 13/2015, en relación a los descubrimientos casuales. Para ello, el legislador deberá rodear de garantías su incorporación a un proceso penal incoado posteriormente, diseñando un procedimiento que, desde la defensa de los derechos fundamentales, y, más concretamente, del derecho de defensa, pueda validar la actuación policial para que los resultados obtenidos puedan ser tratados como fuentes de prueba.

2.3. Derecho a la presunción de inocencia e Inteligencia artificial

La consagración de la presunción de inocencia como derecho fundamental tiene lugar en el artículo 24 de la Constitución, dando así inicio a una regulación del proceso penal informado por principios y garantías derivados de la proclamación del Estado social y democrático de Derecho. Este reconocimiento trae causa de los tratados internacionales ratificados por España una vez constituido como Estado democrático²⁴⁵. Representa una de las principales garantías sobre la que gira el enjuiciamiento penal, erigiéndose en uno de los pilares sobre los que se apoya el derecho al proceso debido. La puesta en peligro del derecho a la presunción de inocencia implica el desconocimiento de los principios esenciales del proceso penal. Su relevancia en el proceso constitucional también es puesta de relieve en la Directiva (UE) 2016/343, del Parlamento europeo y del Consejo, de 9 de marzo de 2016 (LA LEY 3261/2016), por la que se refuerzan determinados aspectos de la presunción de inocencia y el derecho a estar presente en el juicio.

El contenido del derecho fundamental a la presunción de inocencia ha de determinarse desde una doble perspectiva. Se trata en primer lugar de una regla de tratamiento, al imponer que el investigado y encausado será considerado inocente hasta que se produzca su condena por sentencia firme. En segundo lugar, ha de considerarse como regla de juicio, al operar sobre el juzgador que fundamentará la condena en una actividad probatoria desarro-

245 Una vez ratificado en noviembre de 1977, el Tratado de Roma de 1950, se produce como consecuencia inmediata el reconocimiento de este derecho fundamental, regulado en diversos documentos internacionales que toman como referencia el artículo 9 de la Declaración de los Derechos del Hombre y del Ciudadano de 1789. Así se reconoce la presunción de inocencia en el artículo 11.1 de la Declaración Universal de los Derechos Humanos aprobada por la ONU en diciembre de 1948, en el artículo 6.2 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Públicas, de noviembre de 1950, el artículo 14.2 del Pacto Internacional para los Derechos Civiles y Políticos de 1966, y en el artículo 48.1 de la Carta de los Derechos Fundamentales de la Unión Europea de diciembre de 2000.

llada en el proceso penal, en su fase de juicio oral, con respeto a los principios de contradicción e igualdad de armas²⁴⁶.

Los sistemas de inteligencia artificial, que parten de los datos proporcionados previamente, podrán afectar a la presunción de inocencia cuando dichos datos se hayan introducido en función de estudios sesgados, o de patrones pasados discriminatorios, atendiendo a factores relacionados con el origen, la raza, la realidad socioeconómica anterior, etcétera²⁴⁷, que van a incidir notablemente en el juzgador, poniendo en peligro su imparcialidad y la presunción de inocencia del acusado²⁴⁸. En estos casos, la regla de tratamiento aparece desvirtuada al suministrar datos que tienden a dirigir el funcionamiento del sistema en una determinada dirección. En este contexto, se ofrecerán unos resultados que aparecen ya viciados en su inicio, por lo que su introducción en el proceso pondrá en peligro la imparcialidad judicial, afectando a la regla de juicio²⁴⁹.

Se trata de datos que pertenecen al origen y al pasado del sujeto, que, sin embargo, pueden resultar determinantes para decidir sobre su futuro. Se está aceptando, que el origen, circunstancias familiares y personales, entorno familiar y otros datos sobre la personalidad del investigado pueden condicionar en gran medida la decisión judicial. Con ello, la aplicación de la ley al caso concreto puede encontrarse condicionada por la evaluación anterior del sujeto investigado, lo que desde luego va a incidir en la interpretación de la norma y en una justicia de autor, que tendrá en cuenta no sólo las circunstancias actuales del acusado, sino también sus pasado personal, familiar y social²⁵⁰.

En este sentido el Reglamento Europeo de Inteligencia Artificial, precisa en su considerando 42 que «...en consonancia con la presunción de inocencia, las personas físicas de la Unión siempre deben ser juzgadas basándose en su comportamiento real. Las personas físicas nunca deben ser juzgadas a partir de comportamientos predichos por una IA basados únicamente en la elaboración de sus perfiles, en los rasgos o características de su personalidad, como la nacionalidad, el lugar de nacimiento, el lugar de residencia, el número de hijos, el nivel de endeudamiento o el tipo de vehículo, sin una valoración humana y sin que exista una sospecha razonable, basada en hechos

246 V. sobre la presunción de inocencia, FERNÁNDEZ LÓPEZ, M., *Prueba y presunción de inocencia*, Editorial Iustel, Madrid, 2005; MARTÍN DÍZ, F., «Presunción de inocencia en procesos penales por violencia de género», *Ius et Praxis*, vol. 24, núm. 3, 2018, pág. 26 y ss., entre otros

247 SOLAR CAYÓN, J.I., «Inteligencia artificial en la justicia penal...», *op. cit.*, pág. 169.

248 MARTÍN DÍZ, F., «Modelos de aplicación de Inteligencia Artificial en justicia...», *op. cit.*, pág. 79.

249 MARTÍN DÍZ, F., «Modelos de aplicación de Inteligencia Artificial en justicia...», *op. cit.*, pág. 79.

250 Sobre esta cuestión puede consultarse ARMENTA DEU, T. *Derivas de la justicia. Tutela de los derechos y solución de controversias en tiempos de cambio*. Editorial Marcial Pons, Madrid 2021.

objetivos comprobables, de que dicha persona está implicada en una actividad delictiva. Por lo tanto, deben prohibirse las evaluaciones de riesgos realizadas con respecto a personas físicas para evaluar la probabilidad de que cometan un delito o para predecir la comisión de un delito real o potencial basándose únicamente en la elaboración de perfiles de esas personas físicas o la evaluación de los rasgos y características de su personalidad».

Es importante destacar en este punto algunos elementos esenciales relativos al contenido de la presunción de inocencia como son «...*que el acusado debe ser tratado como si no hubiera cometido ninguna infracción hasta que el Estado, a través de las autoridades responsables del ejercicio de la acción penal, presente pruebas suficientes para que un tribunal independiente e imparcial lo declare culpable; o que la presunción de inocencia requiere que los miembros del tribunal no tengan una idea preconcebida de que el acusado ha cometido la infracción de la que se le acusa*²⁵¹.

Una de las cuestiones más complejas relativas a la presunción de inocencia y su alcance como derecho fundamental, es la de determinar si ha de aplicarse dicha presunción antes de la incoación de un proceso penal, como parámetro delimitador de las investigaciones policiales. No se pretende, en este caso, un estudio exhaustivo sobre el alcance de la presunción de inocencia, y menos si se tiene en cuenta que las posiciones doctrinales sobre esta cuestión no son unánimes, por lo que habría que dedicarle un análisis riguroso y detallado de su naturaleza y extensión, pero sí ha de realizarse alguna reflexión.

Como ya es sabido, la actividad policial de investigación de los hechos delictivos y de las conductas criminales suele ser anterior a la incoación del proceso penal. Las actuaciones policiales de prevención, con la finalidad de evitar la comisión de conductas delictivas, marcan el día a día del trabajo policial, en el que obviamente, y cada vez con mayor frecuencia, se utilizan instrumentos de IA. En este marco, la actividad policial puede centrarse en averiguar los lugares en los que se pueden realizar conductas delictivas, y en los tipos delictivos que se pueden perpetrar, lo que en una primera aproximación no representa problema alguno en relación con la protección de la presunción de inocencia. Sin embargo, cuando las investigaciones policiales tratan de determinar personas, o grupos de personas que pueden ser posibles autores de hechos delictivos concretos, la incidencia en la presunción de inocencia parece probable.

Cabe deducir, y ello es lógico, que los datos derivados de esa actuación preprocesal puedan ser introducidos en el proceso una vez iniciado, y que se pretenda convertirlos en material probatorio con la finalidad de desvirtuar la presunción de inocencia. Sin embargo, ha de tenerse en cuenta que la obten-

251 V. MORENO CATENA, V., *Fiscalía europea y derechos fundamentales*, Tirant lo Blanch, Valencia, 2014, pág. 112.

ción de estas fuentes ha podido tener lugar al margen del control judicial, por lo que la limitación de derechos fundamentales de alta relevancia, como el derecho a la intimidad, a la privacidad, o a la protección de datos, se ha producido al margen de todo control judicial, y sin efectuar el necesario juicio de proporcionalidad²⁵².

Como ya se ha apuntado, la doctrina no es unánime respecto de la extensión o del alcance de la presunción de inocencia en la fase de investigación preprocesal, pero lo que resulta evidente es que, de un lado, no se puede impedir la necesaria función preventiva de la policía, y, de otro, que esta función no puede llevarse a cabo con vulneración de los derechos fundamentales. Será determinante, por tanto, fijar los parámetros o los mecanismos de control para que los datos obtenidos de estas investigaciones puedan acceder al proceso rodeados de las garantías necesarias que eviten la prohibición probatoria.

Como se comprobará en el siguiente capítulo, es innegable que, teniendo en cuenta ciertos requisitos y condiciones, y siempre atendiendo a razones de prevención, los agentes policiales están autorizados para el tratamiento de datos personales de aquellas personas que resulten sospechosas de cometer un hecho delictivo. Así lo permite la Directiva UE 680/2016, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, que en el artículo 6.1 recoge entre los destinatarios o «interesados» en este tratamiento a las *«personas respecto de las cuales existan motivos fundados para presumir que han cometido o van a cometer una infracción penal»*.

Igual sentido se desprende del artículo 1 de la LO 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 al establecer el ámbito de aplicación de la citada ley, incluye expresamente la protección de los datos personales de las personas físicas en las actuaciones a prevención realizadas por las autoridades competentes, básicamente por los miembros y fuerzas de la seguridad del Estado.

A la hora de establecer las reglas de control que deberían tomarse en consideración para validar una actuación policial desarrollada en el marco de una investigación preprocesal, habrá que partir de las garantías que se exigen cuando esa actuación policial se lleva a cabo en la instrucción penal, bajo control judicial. De esta forma, la investigación desarrollada por la policía en

252 GUZMÁN FLUJA, V., «Ideas para un debate sobre la predicción del crimen» en *Inteligencia artificial y Administración de Justicia...*, pág. 334.

la fase de instrucción del proceso penal esta supervisada y controlada judicialmente, por lo que en aquellos casos en que se procede a la limitación de derechos fundamentales, dicha actuación se hace desde el juicio de la proporcionalidad y con el control judicial correspondiente. Y aun en estos casos se protege la presunción de inocencia y el derecho de defensa mediante la oportuna contradicción.

Sin embargo, en los supuestos en que se pretenden introducir datos obtenidos preprocesalmente, estos controles judiciales no se han producido. Por tal motivo, lo primero que habrá que llevar a cabo es un control judicial sobre el material obtenido. El juzgador ha de realizar una supervisión sobre la obtención de los datos y las condiciones en las que se ha producido, además de valorar, y aquí entraría en juego el juicio de proporcionalidad, las circunstancias personales del investigado y la gravedad del hecho investigado²⁵³.

253 MORENO CATENA, V., *Fiscalía europea...*, op. cit., págs. 135-137

CAPÍTULO III

LA ACTUACIÓN POLICIAL COMO PUNTO DE PARTIDA EN LA INVESTIGACIÓN PENAL

1. Reflexiones previas

Como ya se ha puesto de relieve en capítulos anteriores, cada vez con mayor frecuencia los instrumentos relacionados con la inteligencia artificial se abren camino, no sólo como apoyo en la realización de actuaciones judiciales, sino también en el campo de la investigación de hechos delictivos y en la toma de decisiones en el proceso.

Para su aplicación en la fase de investigación y enjuiciamiento del proceso penal ha de partirse necesariamente de la búsqueda del equilibrio entre los diferentes derechos que pueden verse afectados en su desarrollo. De esta forma, ha de tenerse en cuenta que *«El proceso penal representa probablemente el principal campo de tensión entre la exigencia ciudadana de seguridad y el derecho a la libertad de quien se ve sometido al proceso..., sirve para garantizar la seguridad pública, como un valor digno de protección..., pero también debe salvaguardar los derechos de la persona»*²⁵⁴.

En la sociedad actual, el papel de las Fuerzas y Cuerpos de la Seguridad del Estado en la investigación delictiva cobra especial relevancia. Los avances tecnológicos y, en los últimos tiempos, la utilización de instrumentos de inteligencia artificial conlleva mayores facilidades para la investigación. Aunque la actividad policial relacionada con la investigación penal, se puede iniciar en el momento en que se incoa el proceso penal, y se encarga a las unidades de policía la investigación del hecho delictivo, lo cierto es que, en realidad, esta función investigadora de la policía ya se lleva a cabo con anterioridad.

254 MORENO CATENA, V., «La garantía de los derechos fundamentales durante la investigación penal» en *Cuadernos penales...*, op. cit., pág. 13.

En este contexto, dos son los escenarios en los que se desarrolla la intervención policial. De un lado, dicha investigación puede comenzar con las instrucciones dadas por el juez o magistrado, o por el Ministerio fiscal, cuando se ha interpuesto una denuncia o querella incoándose el proceso penal. De esta forma, abiertas diligencias penales, de oficio o instancia de parte, se pueden adoptar diligencias de investigación que, en la mayoría de los casos, se ejecutan por las unidades de policía. De otro, los agentes de policía, de oficio, cuando tiene conocimiento de la comisión de algún hecho con apariencia delictiva, ponen en marcha una serie de actuaciones cuya finalidad es esclarecer las circunstancias de la comisión del delito y averiguar los sujetos implicados en el mismo. Una vez practicadas, estas diligencias se trasladan al órgano jurisdiccional para que se incoe, si es el caso, el correspondiente proceso penal. Habitualmente estas actuaciones responden a denuncias en sede policial, o a la constancia de una *notitia criminis* por algún otro conducto.

Si hasta hace pocos años, la investigación penal se desarrollaba partiendo de algunas de estas dos situaciones, en la actualidad el papel policial en su relación con las actuaciones delictivas comienza con anterioridad incluso a la realización de la actividad criminal. En los últimos años, se han incrementado notablemente una serie de funciones policiales relacionadas con la llamada policía predictiva y policía de prevención, que tiene como finalidad evitar, en la medida de lo posible, la comisión de hechos delictivos²⁵⁵.

Con esto no se quiere negar la existencia de funciones preventivas de la policía en etapas anteriores, que, como norma general, tenían como objetivo actuaciones relacionados con el aseguramiento del sospechoso de la actuación delictiva y de las fuentes de prueba. En este sentido, el artículo 282 LECrim, ya encomienda a la policía judicial, en su función de averiguación de la actividad delictiva «...recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la autoridad judicial...». Estas funciones se completan con las recogidas en los artículos 771 y 772 de la Ley procesal penal.

Sin embargo, a día de hoy, es obligada la referencia a las actuaciones predictivas que dan lugar a la adopción de medidas de prevención, que cobran mayor importancia desde la utilización policial de instrumentos tecnológicos y sistemas relacionados con la inteligencia artificial. Las labores policiales se centran ahora, con mayor intensidad, en prevenir la comisión delictiva, o, si ello no es posible, en frustrar en sus etapas iniciales la ejecución del delito.

No se puede negar que, en la sociedad actual, se está produciendo una evolución hacia un mayor control sobre los ciudadanos, justificado bajo el

255 MIRÓ LLINARES, F./SANTISTEBAN GALARZA, M., «La regulación de los sistemas policiales predictivos en el Reglamento Inteligencia Artificial» en *Tratado sobre el Reglamento de Inteligencia Artificial...*, op. cit., págs. 315 y ss.

paraguas de la seguridad. A ello ha contribuido notablemente el incremento de las actuaciones criminales relacionadas con el terrorismo, la trata de personas, el tráfico de drogas, la ciberdelincuencia, y, en general, todos aquellos delitos cometidos por bandas organizadas. El empeño de los Estados en tratar de evitar, en la medida de lo posible, la comisión de este tipo de actos criminales, que pueden afectar a una gran parte de la ciudadanía, poniendo incluso en peligro la seguridad nacional, ha llevado a modificar normativas policiales, penales y procesales, proporcionando a las fuerzas policiales instrumentos más acordes para la lucha contra estas nuevas formas de criminalidad. De esta forma, las fuerzas policiales no sólo van a reaccionar ante la comisión de un hecho delictivo, sino que van a desplegar su actividad antes de la comisión de la actividad criminal, atendiendo para ello a riesgos y amenazas²⁵⁶.

Si la utilización de los nuevos instrumentos tecnológicos y de sistemas de IA supone destacados avances en la lucha contra la delincuencia, es necesario precisar también, como ya se ha hecho en páginas anteriores, su incidencia en los derechos de los ciudadanos y en sus libertades fundamentales. Por ello, es importante poner ya de relieve que dicha actuación policial, dirigida a prevenir la comisión de hechos delictivos, ha de rodearse de las mismas garantías que se aplican cuando se está investigando el delito, una vez incoado el proceso penal. No se puede obviar que los derechos en juego, son los mismos en uno y otro caso, por lo que las garantías en la investigación también deben ser iguales, y con más razón cuando en estas actuaciones a prevención, la autoridad judicial no desempeña la función de control que sí realiza en la fase de instrucción del proceso penal.

Como ya se ha indicado al inicio de este capítulo, en el proceso penal confluyen dos derechos importantes para los ciudadanos, de un lado el derecho de la sociedad a la seguridad pública y a la defensa de sus derechos, no sólo individuales, sino como colectivo. De otro, el derecho de los individuos que se ven sometidos a la investigación penal a que, en dicha investigación, se garanticen sus derechos fundamentales, practicándose las diligencias acordadas garantizando su derecho de defensa y su derecho al proceso debido. Estas mismas garantías que se propugnan para la fase de instrucción, han de observarse en fases preprocesales, dado que con su ejecución se pretenden obtener resultados que, en su caso, puedan ser útiles en un futuro proceso, lo que va a exigir que se observen los presupuestos y requisitos para la protección de los derechos fundamentales. O dicho de otra forma, las garantías propias del proceso penal constitucional no pueden ponerse en peligro, o incluso anularse, alegando la defensa de la democracia y de la seguridad,

256 BARONA VILAR, S., *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, Valencia, 2021, pág. 501.

porque entonces sí, el proceso que ahora conocemos empezaría a dejar de ser el proceso garantista regulado constitucionalmente²⁵⁷.

La comprobación de la comisión del delito, y la búsqueda de su autor y de las personas que han participado en la preparación y ejecución de la actividad delictiva, constituyen el núcleo central de las investigaciones delictivas. Para ello, y de acuerdo con lo establecido en el artículo 282 LECrim, la policía judicial podrá adoptar «...*las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la autoridad judicial*».

Son estas tareas de aseguramiento, que tienen lugar en la primera fase del proceso penal, las que pueden generar fuentes de prueba que después podrán incorporarse al juicio oral. Es esta precisamente la razón que justifica la exigencia de garantías estrictas y respeto a los derechos fundamentales en la realización de diligencias de investigación policiales. En consecuencia, cuando en el ejercicio de labores a prevención desarrolladas con anterioridad al inicio del proceso penal, se obtengan resultados que puedan resultar de utilidad una vez incoado el proceso, y se pretenda que adquieran eficacia convirtiéndose primero en fuentes de prueba y después en material probatorio, será imprescindible rodear las diligencias practicadas de las garantías necesarias para evitar la exclusión probatoria²⁵⁸. En este sentido, ya se pronuncia, como se ha podido comprobar, la Directiva 60/2016, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, en la que ya se delimita el ámbito objetivo de aplicación, precisando que también resulta de aplicación a las actuaciones con fines de prevención²⁵⁹.

Si bien es cierto que la actuación policial predictiva y a prevención cobra ahora nuevo protagonismo, no quiere decir que sea una novedad de los últimos años. Lo que ocurre es que este tipo de tareas se lleva ahora a cabo valiéndose de instrumentos tecnológicos y de inteligencia artificial, que pueden causar mayores perjuicios en los derechos de los ciudadanos, fruto de la complejidad de su funcionamiento y de su difícil detección. En este sentido,

257 GÓMEZ COLOMER, J.L., «El aumento de intervencionismo público en la investigación del delito. Una reflexión al hilo del acto de investigación criminal de registro remoto de equipos informáticos (coloquialmente llamado “del gusano informático”)», en *Derecho Probatorio y otros estudios procesales. Liber amicorum* Vicente Gimeno Sendra (Asencio Mellado, dir.), editorial Castillo de Luna Ediciones Jurídicas, Madrid, 2020, pág. 819.

258 BARONA VILAR, S., «Algoritmización del Derecho...», *op. cit.*, pág. 504.

259 V GUZMÁN FLUJA, V., «Consideraciones sobre el alcance objetivo y subjetivo de la Directiva 680/2016», en *Nuevos Postulados de la Cooperación Judicial...*, *op. cit.*, pág. 840.

ya la Constitución, en su artículo 104, encomienda a las Fuerzas y Cuerpos de la seguridad del Estado la función de «...*proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana*». Obviamente, en esta función se integran todas las actuaciones relacionadas con la averiguación de los hechos delictivos y de sus autores, valiéndose lógicamente de los instrumentos disponibles en cada momento. El encargo constitucional, se desarrolla en la LOPJ, y concretamente en su artículo 549, que encomienda a la policía «...*a) La averiguación acerca de los responsables y circunstancias de los hechos delictivos y la detención de los primeros, dando cuenta seguidamente a la autoridad judicial y fiscal, conforme a lo dispuesto en las leyes*».

Aunque la regulación de la actividad policial se encuentra dispersa en distintos textos normativos no pueden dejar de mencionarse las normas más relevantes. Así, cabe destacar la LO 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, el RD 769/1987 de 19 de junio, sobre regulación de la Policía Judicial²⁶⁰, y la LO 4/2015, de protección de la seguridad ciudadana. De igual forma, es preciso mencionar los artículos 282 y siguientes y 769 y siguientes de la Ley de Enjuiciamiento Criminal, que se ocupan de regular las funciones policiales en la investigación de los hechos delictivos, tanto con carácter general, como en el ámbito del proceso abreviado. También resulta obligada la referencia a las disposiciones introducidas por la Ley 13/2015, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, que dan cobertura legal a las nuevas diligencias derivadas de los avances tecnológicos de los últimos años y de la inteligencia artificial. Finalmente, por su especial relevancia en el objeto de estudio, es preciso citar 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.

260 El artículo 547 LOPJ parece diferenciar entre una policía judicial genérica a la que pertenecen todos los miembros de las Fuerzas de Seguridad «...tanto si dependen del Gobierno central como de las comunidades autónomas o de los entes locales, dentro del ámbito de sus respectivas competencias», de la policía judicial en sentido estricto, a la que se hace referencia en el artículo 548, integrándolas en unidades de policía judicial, cuya composición se establece en el artículo 7 del citado Real Decreto, que están integradas por la policía nacional y la guardia civil: «Constituyen la Policía Judicial en sentido estricto las Unidades Orgánicas previstas en el artículo 30.1 de la Ley Orgánica de Fuerzas y Cuerpos de Seguridad integradas por miembros del Cuerpo Nacional de Policía y de la Guardia Civil.». V. en este sentido, NACARINO LORENTE, J.M., «La prevención del delito por las Fuerzas y Cuerpos de Seguridad y su relación con el adelanto de las barreras penales. ¿Dichas actuaciones permiten prevenir el delito y asimismo contribuir a tipificar conductas preparatorias?» (1), *Diario La Ley*, número 9740, Sección Tribuna, 20 de Noviembre de 2020, <https://laleydigital-laleynext-es.ezbusc.usc.gal/>, pág. 2.

2. Consideraciones puntuales sobre las actuaciones policiales a prevención

2.1. Una primera aproximación

Centrando la actividad policial en su faceta de persecución de las actividades delictivas y de la investigación criminal, no cabe duda que las actuaciones predictivas y a prevención cobran especial importancia desde la irrupción de la tecnología y de los instrumentos de IA.

Es preciso dejar constancia, en primer lugar, que los problemas derivados de estas funciones policiales, respecto de la protección de los derechos fundamentales y de las garantías del proceso debido, no derivan de su papel, o de la actividad desarrollada cuando ya se ha incoado el proceso penal. En este caso, las condiciones y forma de actuación de la policía se encuentran ya previstos, y las reglas y límites de sus funciones se recogen fundamentalmente en la Ley de Enjuiciamiento Criminal, cuya regulación se ha completado con la ya citada Ley 13/2015, que ha introducido un amplio desarrollo de la investigación con medios tecnológicos. Es por ello, que no van a ser objeto de un tratamiento específico, aunque sí se hará alguna alusión con motivo del tratamiento de estas funciones en las actuaciones a prevención.

En el sentido apuntado, la Ley procesal penal se ocupa, en los artículos 579 y siguientes, de las denominadas diligencias de investigación tecnológicas, y contempla una regulación completa de los presupuestos, requisitos y efectos de estas medidas. Por lo que aquí interesa, el Capítulo IV recoge las disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos. Es obvio que en todas estas diligencias de investigación se utilizan sistemas de IA, y es este cuerpo legal el que establece los requisitos y garantías para su válida aplicación en la fase de investigación del proceso penal. La salvaguarda de los derechos fundamentales queda garantizada con esta regulación, que combina la necesaria actividad instructora, con su protección.

Sin embargo, no puede decirse lo mismo de las funciones policiales practicadas con anterioridad a la incoación del proceso penal, con ánimo de predecir y, en consecuencia, evitar futuras acciones delictivas²⁶¹.

261 En este punto ha de realizarse una precisión relativa a la regulación de la actuación policial para la identificación de un usuario de equipo informático que esté cometiendo un hecho delictivo. Es necesario precisar que, en este caso, se trata de actuaciones policiales llevadas a cabo a prevención para el descubrimiento de actividades delictivas cometidas en

Cuando las actuaciones policiales y las diligencias adoptadas derivan de la puesta en marcha de mecanismos predictivos, y de actuaciones a prevención que han dado como resultado la sospecha sobre la comisión de una actuación delictiva, es preciso determinar con claridad cuáles son los requisitos y garantías que han de observarse en esta fase preprocesal de la investigación. En este sentido, ha de tenerse presente que los barridos informáticos realizados por la policía, los resultados derivados de las imágenes captadas con las tan conocidas cámaras de videovigilancia, la utilización de drones de vigilancia policial en los puntos calientes, la interceptación de mensajes en redes sociales, etc., pueden centrar futuras actuaciones policiales más concretas, dirigidas sobre conductas sospechosas, con posibles autores en el foco de atención²⁶². En estos casos, la investigación policial se desarrolla al margen de la actividad jurisdiccional, porque todavía no se ha iniciado el proceso penal, por lo que, de no respetarse las garantías propias de la fase de instrucción, se está privando a los ciudadanos del necesario control que jueces y magistrados han de desarrollar en su función protectora de los derechos fundamentales.

Entre las herramientas de IA, que se ponen al servicio de la policía, destacan aquellas que permiten prevenir la comisión de hechos delictivos mediante la denominada evaluación de riesgos, son las conocidas como herramientas de predicción. Las actuaciones policiales predictivas han supuesto un importante cambio en las actuaciones policiales. Se trata de la «...*aplicación de técnicas cuantitativas para identificar objetivos de interés policial con el propósito de reducir el riesgo delictivo mediante la prevención de delitos futuros o la resolución de delitos pasados*»²⁶³. Se supera así el modelo policial reactivo, consistente en la actuación policial *a posteriori*, como respuesta a la actividad criminal, para transitar hacia un modelo mixto, en el que adquiere especial importancia la predicción de futuras acciones delictivas con la finalidad de adoptar la medidas necesarias para prevenir su ejecución²⁶⁴.

Las actuaciones policiales con finalidad predictiva ya se han desarrollado en etapas anteriores, si bien es importante destacar que, en aquel momento, la evaluación se centraba casi exclusivamente en la peligrosidad del sujeto y en sus tendencias delictivas. Así, se recogían datos sobre los delitos come-

internet, y que será el juez de instrucción el que autorice la actuación policial para identificar al sujeto concreto sospechoso de cometer la actuación criminal, tal y como se prevé en el que la Ley de Enjuiciamiento Criminal en su artículo 588 ter k).

262 GUZMÁN FLUJA, V., «Ideas para un debate sobre la predicción del crimen...», en *Inteligencia artificial legal...*, op. cit., pág. 304.

263 MIRÓ LLINARES, F., «Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots», *Revista de Derecho Penal y Criminología*, 3.ª Época, número 20 (julio de 2018), pág. 100.

264 LAFONT NICUESA, L., «La policía predictiva más allá de Minority Report (1)», en *Diario LA LEY*, número 10687, 9 de Marzo de 2025, pág. 4.

tidos y sus autores incorporándolos a las bases de datos de la policía. En la actualidad, los elementos a evaluar son variados, y no sólo tienen que ver con la personalidad y condiciones del sujeto, sino que entran en consideración otros factores como sus circunstancias familiares, laborales o ambientales, que se tienen en cuenta para determinar la probabilidad de actuación delictiva²⁶⁵.

Precisamente, la utilización de instrumentos de inteligencia artificial permite ahora el análisis de gran variedad de datos, optimizando resultados, lo que provoca tanto la obtención de mejores modelos de previsión, como la adopción de medidas que permitan prevenir actuaciones criminales, detectando no sólo formas de ejecución sino también los posibles autores²⁶⁶.

El análisis de un volumen abundante de datos, extraídos de expedientes policiales pasados, informaciones estadísticas, grabaciones y rastreos, permiten fijar un hilo conductor derivado de las relaciones entre ellos, y de la coincidencia de diversos factores, deduciéndose un nivel de riesgo concreto en lugares también concretos, e incluso en individuos determinados²⁶⁷. Así, los sistemas de policía predictiva establecen patrones de conducta derivados de actuaciones pasadas que se extrapolan hacia posibles actuaciones futuras, con el objetivo de predecir comportamientos delictivos²⁶⁸. A través de estos instrumentos se trata de predecir la comisión de futuros hechos delictivos, con el fin de adoptar las medidas necesarias para evitarlos²⁶⁹.

265 MONTESINOS GARCÍA, A., «Los algoritmos que valoran el riesgo de reincidencia. En especial, el sistema Viogen» en *Revista Aranzadi de Derecho y Proceso Penal*, número 64, 2021, cuarto trimestre, Aranzadi Digital, pág. 2

266 Este tipo de instrumentos de predicción permiten también detectar e identificar a sujetos vulnerables y posibles víctimas, facilitando la adopción de medidas de protección. No obstante, al no ser objeto de este trabajo, las consideraciones desde esta perspectiva no van a ser objeto de estudio.

267 SOLAR CAYÓN, J.I., «Inteligencia artificial en la justicia penal: los sistemas algorítmicos» en *Dimensiones éticas y jurídicas de la Inteligencia artificial en el marco del Estado de Derecho. Cuadernos de la Cátedra de Democracia y Derechos Humanos*, 16, Universidad de Alcalá. Defensor del Pueblo, 2020, pág. 130.

268 Los patrones delictivos se basan en tendencias de actuación o comportamientos que se relacionan con actividades delictivas. De esta forma, se puede realizar un análisis de las características comunes entre ellas, y utilizarlo para prevenir futuras actuaciones. Con ellos se pueden identificar los tipos de conductas, su ubicación y horarios y los métodos que se utilizan.

269 Es importante tener en cuenta la regulación de la Directiva 2016/680 sobre la elaboración de perfiles y patrones de comportamiento, que protege a los posibles afectados por decisiones que evalúen aspectos personales y que se basen únicamente en un tratamiento automatizado de los datos, siempre que tales decisiones tengan efectos jurídicos adversos que le afecten significativamente. En el mismo sentido se pronuncia el artículo 14 de la LO 7/2021, si bien prevé una excepción que habilita al tratamiento con datos personales siempre que lo autorice una norma legal

Desde la perspectiva de la seguridad pública, la utilización de técnicas predictivas beneficia a la sociedad en una doble dirección. De un lado, puede facilitar la adopción de las medidas necesarias para evitar la comisión delictiva, permitiendo a los cuerpos de seguridad del Estado la puesta en marcha de los recursos necesarios para prevenir actuaciones criminales²⁷⁰. De otro lado, también parece indudable, que, en aquellos casos o situaciones en los que no se puede evitar la actuación delictiva, los resultados obtenidos a través de los sistemas «inteligentes», podrán servir de base o de ayuda en la investigación del delito cometido. Sin embargo, en este segundo aspecto, se ha de poner de relieve lo dicho anteriormente en relación con las consecuencias derivadas de actuaciones que no se han llevado a cabo con el debido respeto a los derechos fundamentales, y se han desarrollado con ausencia absoluta de control judicial²⁷¹.

Hechas estas consideraciones, y constatando las ventajas incuestionables del uso de sistemas predictivos y de prevención, no puede obviarse que se trata de sistemas computacionales que trabajan con datos acumulados relacionados con el pasado de los sujetos, para, en función de los resultados proporcionados, establecer una presunción de culpabilidad futura. Varios son los factores a tener en cuenta para asegurar, en la medida de lo posible, la credibilidad de los resultados. De esta forma, en estas operaciones es fundamental comprobar la formación y las competencias de los técnicos que deciden los datos de entrenamiento, y los criterios que se han de proporcionar al sistema, y en función de los cuales se lleva a cabo el análisis algorítmico. Esto es, considerando todos los datos que se pueden proporcionar al sistema, cómo se realiza la elección, o mejor, qué criterios se tienen en cuenta para abordar la selección de los que se introducen. Y como consecuencia de ello, entender que el acierto y fiabilidad de los resultados propuestos va a depender de la cantidad y de la calidad de la información disponible, y de la elección de los datos proporcionados²⁷². En todo caso, la utilización de este tipo de sistemas ha de supervisarse por una autoridad que deberá confrontar los resultados obtenidos y relacionarlos con otro tipo de indicios que permitan asegurar la predicción ofrecida por el sistema²⁷³.

270 CUATRECASAS MONFORTE, C., «IA: herramienta de investigación criminal» en *La Ley digital*, 24 enero 2024, pág. 11.

271 GUZMÁN FLUJA, V., «Ideas para un debate sobre la predicción del crimen» en *Inteligencia artificial legal y Administración de Justicia*, dirigido por Calaza López y Llorente Sánchez-Arjona, Aranzadi, 2022, pág. 302.

272 SUAREZ XAVIER, P.R., «Policía predictiva: entre seguridad y garantías fundamentales» en *Investigación y proceso penal en el siglo XXI: ..., op. cit.*, pág. 579.

273 BARONA VILAR, S., «Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia» en *Revista Jurídica Digital UANDES*, número 3, 2019, pág. 11.

2.2. Garantías frente a la actividad policial de prevención

Pese a que pueda resultar reiterativo, al haberse puesto de manifiesto anteriormente, se considera conveniente insistir en que es precisamente esta labor predictiva y de prevención, realizada con sistemas de IA, la que genera más incertidumbre y puede poner en peligro el sistema garantista de la justicia penal. La utilización por las unidades policiales de los instrumentos tecnológicos para predecir futuras actuaciones delictivas, que permiten valorar el riesgo de comisión de un hecho delictivo, centrando incluso la vigilancia en sujetos determinados, pueden relacionarse con el hallazgo de fuentes de prueba que, posteriormente, han de ser introducidas en el proceso para someterse a contradicción en el juicio oral. Si en este *iter* procedimental no se respeta la protección de los derechos fundamentales a través de la supervisión judicial, se pondrá en peligro la eficacia de la prueba, lo que conllevará la exclusión probatoria²⁷⁴. Admitir lo contrario pondría en peligro el proceso penal del Estado de Derecho²⁷⁵.

Partiendo de la especial relevancia que ha de predicarse respecto de la función policial, establecer el control de su actuación, fijando límites a las diligencias que puedan afectar a derechos fundamentales, se convierte en una tarea de suma importancia para preservar la investigación y la instrucción²⁷⁶. Así lo afirma el Tribunal Constitucional al considerar que «...la ley que autorice injerencias en los derechos fundamentales debe indicar con claridad el alcance de la discrecionalidad conferida a las autoridades competentes, así como la manera de su ejercicio, no admitiéndose interpretaciones analógicas»²⁷⁷.

Llegados a este punto, resulta evidente que, en el proceso penal constitucional, el respeto a las garantías y los derechos fundamentales marcan el camino en la investigación penal, por lo que la Constitución y la Ley procesal penal se convierten en las primeras normas delimitadoras y de referencia en la actuación de los poderes públicos, y de las autoridades encargadas de la instrucción de los hechos delictivos. En esta línea han de entenderse las garantías que se recogen en la Ley 13/2015, de reforma de la Ley de Enjuicia-

274 ARRABAL PLATERO, P., «El binomio Derecho procesal y nuevas tecnologías: de las pruebas tecnológicas al uso de la inteligencia artificial en la Administración de Justicia» en *El Derecho de la encrucijada tecnológica. Estudios sobre derechos fundamentales, nuevas tecnologías e inteligencia artificial*, (Martín Ríos/Villegas Delgado, coords), Tirant lo Blanch, Valencia, 2022, pág. 186.

275 BARONA VILAR, S., *Algoritmización del Derecho...*, op. cit., pág. 503.

276 BARONA VILAR, S., *Algoritmización del Derecho y de la justicia...*, op. cit., pág. 502.

277 STC 92/2023, de 11 de septiembre. V. también las SSTC 49/1999, de 5 de abril; 169/2001, de 16 de julio; 233/2005, de 26 de septiembre; 145/2014, de 22 de septiembre, y 99/2021, de 10 de mayo, entre otras

miento Criminal, que regula la investigación por medios tecnológicos, y que marca un antes y un después en los requisitos que se han de observar en la investigación que utilice este tipo de instrumentos.

De igual forma, el Reglamento Europeo de Inteligencia Artificial (REIA), o con más precisión 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, establece también una serie de requisitos que han de cumplirse cuando se trata de aplicar instrumentos de IA en la investigación.

Con anterioridad, y respondiendo a las directrices marcadas por la Directiva 2016/680, la LO 7/2021, se ocupa también de regular un sistema de garantías en el tratamiento de datos personales con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales, estableciendo condiciones y requisitos, tanto en relación a su utilización, como para su transmisión. Pese a que esta norma ha sido objeto de un amplio tratamiento en el primer capítulo, se considera oportuno realizar en este punto una serie de precisiones.

El tratamiento de datos personales de carácter sensible se condiciona, en el artículo 13 de la citada Ley orgánica, a su previsión en una norma con rango de ley, o en el Derecho de la UE, a que resulte necesario para proteger los intereses vitales, o los derechos y libertades fundamentales del interesado, y a que el tratamiento se refiera a datos personales hechos públicos por el propio interesado. Además, su artículo 14 prohíbe el tratamiento de este tipo de datos cuando no esté permitido por una norma con rango legal que prevea también las medidas de protección que el interesado pueda ejercitar, incluyendo la intervención humana para su revisión.

No obstante, estas garantías se ven ensombrecidas por la regulación del artículo 15 de la norma, que, en el marco del tratamiento de datos derivados de la grabación de imágenes y sonidos por las Fuerzas de seguridad, no las considera intromisiones ilegítimas en los derechos relacionados con la vida privada protegidos por la LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen²⁷⁸.

En este contexto, es necesario precisar, que el tratamiento de esos datos personales no se considera intromisiones ilegítimas en los derechos regulados en el artículo 18 CE, a efectos de su protección civil, como expresamente señala el artículo 15. No obstante, ello no quiere decir que se esté permitiendo dicho tratamiento para que el resultado obtenido pueda tener efectos en un proceso penal posterior, si no se ha rodeado de las garantías previstas para las diligencias de investigación acordadas en la fase de instrucción.

278 V. SUAREZ XAVIER, P.R., «Policía predictiva: entre seguridad y garantías fundamentales...», *op. cit.*, pág. 581.

En este sentido, el Tribunal Supremo se ha ocupado de fijar las pautas a seguir en diligencias policiales de investigación en las que se utilizan instrumentos de IA, con la finalidad de garantizar la protección de los derechos fundamentales y libertades públicas, preservando al mismo tiempo la investigación policial preprocesal, y la desarrollada en la fase de instrucción. En sus últimas resoluciones trata de acotar las injerencias en derechos que protegen la vida privada de las personas, restringiendo o limitando las actuaciones policiales que puedan considerarse una vulneración de estos derechos fundamentales²⁷⁹.

Esta preocupación constante por la protección de los derechos y libertades de los ciudadanos en la investigación penal, se ha compartido también por el Tribunal Constitucional, que se ha pronunciado sobre la eficacia y legalidad de las diligencias policiales preprocesales, al hilo de determinar la licitud de las pruebas obtenidas a partir de las imágenes procedentes de la instalación de cámaras de videovigilancia sin control judicial, ni comunicación alguna a la autoridad judicial. La actuación de la policía se lleva a cabo en el marco de una investigación policial sobre tráfico de drogas. En el inicio de la investigación, y después de un seguimiento a los sospechosos, se procede a la instalación de cámaras de videovigilancia en un garaje privado, a efectos de comprobar la actuación de las personas implicadas. Todo ello sin poner el hecho en conocimiento de la autoridad judicial, ni iniciarse diligencias previas. De esas cámaras se extraen una serie de imágenes en las que se puede comprobar la carga y descarga de bultos que resultan sospechosos. Son estas imágenes las que llevan a la policía a solicitar una autorización judicial de entrada y registro en el domicilio, y en el vehículo de uno de los investigados. Consecuencia de esta diligencia es la obtención de sustancia estupefacientes y de instrumentos delictivos relacionados con el tráfico de drogas.

El Tribunal Constitucional no entra a considerar la legalidad de la entrada y registro domiciliario, toda vez que se produce con autorización judicial, una vez se han iniciado ya la instrucción judicial, señalando que corresponde al juez ordinario determinar el alcance de la información obtenida respecto del derecho fundamental a la presunción de inocencia. Lo que cuestiona la defensa, y aborda el Tribunal, es la legalidad de la instalación de las cámaras de videovigilancia antes de iniciarse la instrucción, y sin dar cuenta de ello a la autoridad judicial. En este sentido considera que «...*el derecho fundamental concernido en este caso es el derecho fundamental a la intimidad personal, pues la Guardia Urbana de Barcelona se sirvió en su investigación de unas imágenes obtenidas sin el conocimiento del recurrente mediante una cámara instalada en un lugar en el que aquel mantenía una legítima expectativa de privacidad, como es el garaje de una comunidad de vecinos. Sin necesidad de entrar a dilucidar si ese garaje tiene la condición de domicilio a*

279 STS 610/2016, de 7 de julio; 489/2018, de 23 de octubre; 141/2020, de 13 de mayo; 835/2022, de 21 de octubre, entre otras.

los efectos del art. 18.2 CE, pues el derecho a la inviolabilidad del domicilio no se invoca en el presente recurso de amparo, es notorio que, conforme al referido criterio de expectativa razonable de privacidad, ese espacio pertenece al ámbito de la intimidad protegida por el art. 18.1 CE, pues se trata de un lugar cerrado que es, además, una propiedad privada de acceso restringido (a los titulares de las plazas de aparcamiento y a terceros a los que aquellos permitan la entrada) y por tanto es patente que se trata de un lugar en el que el recurrente tenía una expectativa razonable de no ser escuchado u observado subrepticamente por terceras personas»²⁸⁰.

Atendiendo a esta resolución se puede entrar a valorar si las actuaciones policiales a través de instrumentos de IA practicadas sobre sujetos ya identificados y fuera de la supervisión judicial, pueden incorporarse al proceso, o si la afectación de derechos fundamentales como la intimidad, el secreto de las comunicaciones, o la libertad de movimientos pueden cuestionar este tipo de fuentes de prueba²⁸¹.

A este respecto, cabe recordar que las limitaciones impuestas por el Reglamento Europeo de IA, la Constitución y la Ley de Enjuiciamiento Criminal, y la LO 7/2021, de protección de datos, deben marcar el camino de futuras actuaciones que permitan una investigación delictiva desde el respeto a los derechos fundamentales y al sistema garantista que ha marcado la regulación de nuestro proceso penal. La gran utilidad de los sistemas de IA y su eficacia en la investigación de la criminalidad, no puede verse empañada por el olvido de las reglas más básicas de protección de los derechos fundamentales, y mucho menos cuando el ordenamiento jurídico tiene instrumentos suficientes para protegerlos, favoreciendo que la actuación de los poderes públicos se desarrolle dentro del marco de garantías que rodea el proceso penal.

3. La vigilancia policial

3.1. Consideraciones iniciales

Los sistemas predictivos relacionados con los adelantos tecnológicos y de inteligencia artificial, que permiten a las unidades de policía arbitrar medidas de prevención delictiva, o en su caso, investigar las actuaciones criminales, son muy variados y resulta del todo imposible hacer referencia a todos

280 STC 92/2023, de 11 de septiembre.

281 V. ORTIZ PRADILLO, J.C., «Big Data, vigilancias policiales y...», *op. cit.*; RICHARD GONZÁLEZ, M., «Investigación policial en lugares públicos y privados atendiendo al derecho a la intimidad de los ciudadanos investigados. Comentario de la STC 92/2023 de 11 de septiembre, sobre la categoría de los garajes comunitarios respecto del derecho a la intimidad» en *LA LEY Probática*, número14, 2023.

ellos²⁸², por lo que se ha optado por centrar este estudio en determinados instrumentos y aplicaciones que están relacionados con la vigilancia policial preprocesal, por considerar que las actuaciones practicadas en esta etapa, carecen en muchos casos de una regulación clara y precisa que aleje todo tipos de dudas sobre su correcta ejecución.

Lo primero que cabe apuntar es que estos sistemas pueden agruparse en función de los objetivos perseguidos. Así, puede recurrirse a los sistemas que buscan la determinación de los lugares y el tiempo en los que resulta más probable que se cometan hechos delictivos, son los denominados mapas delictivos digitales, o puntos calientes (hotspot); Esta ubicación física y temporal de la actividad criminal va a permitir a la policía diseñar una estrategia de prevención y actuación. Otro tipo de sistemas pretenden la determinación de qué tipos delictivos son más probables en lugares determinados. En relación con este segundo grupo es necesario precisar que su acierto está directamente relacionado con aquellos tipos penales que parten o derivan de actuaciones objetivas, que como tales son predecibles, y tienen una incidencia menor en aquellos otros que responden más a la impulsividad y ausencia de premeditación. Un tercer grupo trata de fijar los sujetos, o grupos de sujetos, que tienen mayor probabilidad de cometer un delito, o de ser víctimas de delitos. Finalmente, en otro grupo se pueden integrar aquellos sistemas cuyo objetivo es determinar personas concretas que pueden convertirse en víctimas de un delito, o fijar las características que tendrá el autor de un delito ya cometido. En estos últimos supuestos la incidencia en los derechos fundamentales de las personas sobre las que produce la actuación policial es significativa, por lo que sería necesario establecer límites concretos y un control sobre la actuación policial²⁸³.

De esta forma, los sistemas predictivos pueden clasificarse atendiendo a la predicción de actividades delictivas, enfocando su utilización en determinar los lugares en los que hay una alta probabilidad de actuaciones criminales; atendiendo a la predicción de identidades delictivas, con la finalidad de acotar a los autores que pueden cometer esas actuaciones; y atendiendo a la predicción de identidades vulnerables con la finalidad de identificar a aquellas persona que tienen más probabilidades de convertirse en víctimas de hechos delictivos.

Es indudable que una de las actuaciones policiales más relevantes, y que proporcionan indudables éxitos tanto en la adopción de medidas preventivas, como en el descubrimiento de los autores de los hechos delictivos, es la vigilancia policial. Se trata de una actividad cuya finalidad es garantizar la

282 V. CUATRECASAS MONFORTE, C., «IA: herramienta de investigación criminal...», *op. cit.*, págs. 17 y ss.

283 GUZMÁN FLUJA, V., «Ideas para un debate sobre la predicción del crimen...», *op. cit.*, pág. 308.

seguridad ciudadana, el orden público, y evitar u obstaculizar la comisión de hechos delictivos. Si en su inicio se llevaba a cabo a través de la observación personal realizada por los agentes de la policía, hoy adquiere una mayor relevancia debido a la utilización de herramientas de inteligencia artificial.

La revolución tecnológica ha propiciado el desarrollo de nuevos instrumentos que avanzan en las funciones de vigilancia, con datos más precisos y acertados. La instalación de videocámaras, el rastreo de redes, las balizas de seguimiento y otros instrumentos de geolocalización, se incorporan a esta actividad de seguimiento, facilitando la localización de sospechosos y su ubicación espacio temporal²⁸⁴.

Un primer paso en la vigilancia policial orientada a la prevención delictiva, está estrechamente relacionada con la conocida como criminología ambiental. Partiendo de la instalación de cámaras de videovigilancia en lugares especialmente sensibles, se pueden obtener datos que, utilizados y relacionados con otros, procedentes de otras formas de vigilancia, faciliten la actuación policial.

En este sentido, cabe apuntar que cuando se hace referencia a la vigilancia policial, no se está identificando esta actuación de la policía con una técnica concreta, sino que se pone el foco de atención en una combinación de sistemas que, una vez relacionados, proporcionan un importante número de datos que, combinados entre sí, ofrecen óptimos resultados, tanto para la actuación preventiva como para la investigación criminal.

Así, se parte del análisis de los datos obtenidos de cámaras de videovigilancia, de intercambio de la información en redes, de datos estadísticos, de fotografías y videos realizados por drones²⁸⁵. En definitiva, de la utilización de aplicaciones y sistemas de inteligencia artificial, que analizan posibles localizaciones de actuaciones delictivas, tomando como referencia el entorno y las condiciones sociales. Pero, además, el análisis efectuado propicia, al mismo tiempo, el estudio del comportamiento de determinados sujetos que pueden considerarse como sospechosos, por lo que de una misma actuación pueden derivar distintas medidas de prevención de actuaciones criminales, si bien no todas ellas inciden de igual forma en los derechos fundamentales y en las libertades individuales²⁸⁶. Obviamente, no es lo mismo, ni tiene los mismos efectos, determinar o fijar lugares en los que se pueden desarrollar habitualmente conductas delictivas, que analizar el comportamiento de sujetos concretos que desenvuelven sus actuaciones en esos lugares previamente identificados. En este segundo caso, se ven afectados derechos fundamentales

284 CUATRECASAS MONFORTE, C., «IA: herramienta de investigación criminal...», *op. cit.*, pág. 17.

285 MIRÓ LLINARES, F., «Inteligencia artificial y justicia penal...», *op. cit.*, pág. 99.

286 Aunque es este trabajo no es objeto de estudio, la utilización de los instrumentos de IA también facilita la protección de las víctimas de determinados hechos delictivos, en especial, los relacionados con la violencia de género y la violencia doméstica.

relacionados con la vida privada de personas concretas, por lo que han de respetarse las garantías de protección de dichos derechos.

El tratamiento de los datos obtenidos permite diferenciar a los sujetos, a través de sus costumbres y hábitos, preferencias, características físicas personales, etc., lo que, puesto en relación con el lugar de comisión del hecho delictivo, reduce el círculo de personas sobre las que centrar las actuaciones a prevención, o la investigación de la actuación criminal. A través del cruce de datos, el sistema inteligente proporciona ciertas predicciones sobre el comportamiento humano y los riesgos que pueden suponer cara a actuaciones futuras²⁸⁷.

De esta forma, la información facilitada por los dispositivos electrónicos permite la elaboración de patrones de conducta y determinar el riesgo de reiteración delictiva y, en definitiva, adoptar las medidas más adecuadas para reducir, e incluso evitar posibles actuaciones criminales²⁸⁸. Sin embargo, hay que tener en cuenta que, conforme a la doctrina del Tribunal de Justicia de la Unión Europea, el Tribunal Constitucional y el Tribunal Supremo, aquellas actuaciones de las que puedan derivar conclusiones sobre la vida privada, costumbres o hábitos, relaciones sociales, etc., representan una injerencia en el derecho a la intimidad y a la protección de datos, y en el derecho al entorno virtual, por lo que resulta imprescindible la existencia de control jurisdiccional²⁸⁹.

En este mismo sentido, como se ha comprobado en epígrafes anteriores, se decanta la regulación del Reglamento Europeo de Inteligencia Artificial y las leyes estatales que regulan estas actuaciones. En el considerando 42 REIA, se señala que el respeto a la presunción de inocencia, exige que las personas físicas de la Unión siempre deben ser juzgadas basándose en su comportamiento real. Por tanto, *«...deben prohibirse las evaluaciones de riesgos realizadas con respecto a personas físicas para evaluar la probabilidad de que cometan un delito o para predecir la comisión de un delito real o potencial basándose únicamente en la elaboración de perfiles de esas personas físicas o la evaluación de los rasgos y características de su personalidad»*.

Así, el legislador europeo de Inteligencia Artificial, consciente del grave peligro que la utilización de este tipo de herramientas conlleva para el Estado de Derecho, y para los derechos fundamentales, vincula su incorrecta utilización con el desequilibrio de poder y la afectación de derechos fundamentales

287 MORENO CATENA, V., «Los datos en el sistema de justicia y la propuesta de reglamento UE sobre inteligencia artificial», en *Uso de la información y de los datos personales... op. cit.*, pág. 62

288 MIRÓ LLINARES, F., «Inteligencia artificial y justicia penal...» *op. cit.*, pág. 100.

289 V. MONTORO SÁNCHEZ, J.A., La obtención y tratamiento de datos de carácter personal con fines penales por la policía judicial» en *Uso de la información y de los datos personales...*, *op. cit.*, pág. 652. V. también la sentencia del TJUE de 8 de abril de 2014, caso Digital Rights; STC 292/2000, de 30 de noviembre; STS 434/2021, de 20 de mayo.

como el derecho a la libertad, o derechos fundamentales de contenido procesal, como la presunción de inocencia, la tutela judicial efectiva y el derecho de defensa entre otros²⁹⁰.

En el caso de su utilización para las actuaciones de prevención, lo preocupante es que, en muchos casos, no se parte de la sospecha de una actuación delictiva concreta. La policía no sólo recurre a estos instrumentos cuando está investigando la comisión de un delito, también lo hace sin que exista una investigación previa. Es el análisis de los datos que se van obteniendo, lo que lleva a la policía a la creencia de que un determinado sujeto, o grupo de sujetos, pueden resultar sospechosos de la futura comisión de un acto criminal²⁹¹. A partir de este momento, cuando la investigación preprocesal se centra ya en personas concretas y determinadas, habrá que dar traslado a la autoridad judicial, para que se inicie el proceso penal, en su caso, y rodear la investigación policial de todas las garantías previstas en la Ley procesal penal.

Como es evidente, para que la utilización de las aplicaciones e instrumentos de IA resulte eficaz, se requiere obviamente un tratamiento de los datos con los que trabaja el sistema «inteligente»²⁹². El tratamiento de datos personales relativos a un sujeto concreto en relación a la investigación de un hecho delictivo, se somete a las disposiciones de la LO 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 penales²⁹³. Esto es así porque se aprecia la concurrencia de los tres presupuestos que la propia Ley establece para su aplicación en su artículo 2. Los datos personales se someten a un tratamiento para obtener un resultado sobre su peligrosidad o sospecha de reiteración delictiva²⁹⁴. El tra-

290 Considerando 59 REIA.

291 GUZMÁN FLUJA, V., «Ideas para un debate sobre la predicción del crimen...», *op. cit.*, pág. 315.

292 V. LÓPEZ JIMÉNEZ, R., «La videovigilancia por las Fuerzas y Cuerpos de Seguridad del Estado: tratamiento de los datos personales» en *Uso de la información y de los datos personales...*, *op. cit.*, págs. 587 y ss. PÉREZ GIL, J./GONZÁLEZ PÉREZ, J.J., «La videovigilancia como diligencia de recogida de datos de carácter personal: una reflexión sobre sus repercusiones procesales» en *Videovigilancia. Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de datos personales* (Etxeberria Guridi/Ordeñana Gezuraga, coords.), Tirant lo Blanch, Valencia, 2011.

293 V. MONTORO SÁNCHEZ, J.A., «La obtención y tratamiento de datos de carácter personal con fines penales...» *op. cit.*, págs. 621 y ss.

294 El concepto de «tratamiento de datos» es amplio, y comprende una serie de operaciones que permiten ofrecer un resultado que, en su caso, pueda ser útil en una investigación delictiva. Se define en el artículo 5 de la LO 7/2021, que considera «tratamiento» a «cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción»

tamiento de los datos se realiza por la policía judicial con la finalidad prevista en el artículo 1 de la norma²⁹⁵. Y dicho tratamiento se lleva a cabo por una autoridad competente a los efectos de esta ley²⁹⁶.

La citada Ley Orgánica 7/2021, regula en sus artículos 15 y siguientes, la utilización de instrumentos de grabación de imagen y sonido, que deberán ser expresamente autorizados, atendiendo al principio de proporcionalidad, idoneidad e intervención mínima²⁹⁷.

Como ya se ha indicado en el primer capítulo, la instalación de cámaras fijas se realizará conforme a lo establecido en la LO 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos y su Reglamento de desarrollo, siendo también de aplicación el artículo 16.3 LO 7/2021. Por su parte, la instalación de dispositivos móviles se llevará a cabo conforme a lo dispuesto en el artículo 17.1 de la citada LO 7/2021. Su autorización no tendrá carácter indefinido y dependerá de las circunstancias concretas del evento, o del peligro que se intenta evitar, estableciendo el segundo apartado del precepto el límite de un mes prorrogable por otro.

3.2. Captación de imágenes. Videovigilancia; una breve referencia a los drones como instrumentos de vigilancia policial

3.2.1. Cámaras de videovigilancia

La captación de imágenes por la policía con la finalidad de investigación policial, se produce a través de las conocidas cámaras de videovigilancia instaladas en lugares públicos, o a través de instrumentos más modernos, los denominados sistemas de aeronaves no tripuladas (UAS), más conocidos como drones.

295 Los fines recogidos en el precepto hacen referencia a la «...prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública».

296 El artículo 4.1 de la LO 7/2021, considera autoridad competente a los Fuerzas y Cuerpos de Seguridad del Estado.

297 En este punto es obligado hacer una breve referencia a la instalación de cámaras de videovigilancia no policiales y la posible utilización de sus grabaciones. Ya la LO 7/2021 contempla esta cuestión en el artículo 16.2, al otorgar eficacia a este tipo de grabaciones, pero condicionada a que exista un control policial y una dirección del proceso completo de tratamiento. V. DE LEMUS VARA, F.J. «Límites para el tratamiento de los datos no investigados en el proceso penal», en *Uso de la información y de los datos personales...*, op. cit., pág. 561. Se trata de una colaboración entre la seguridad pública y la seguridad privada, que para que pueda tener eficacia exige el cumplimiento de los requisitos derivados de la protección de los derechos fundamentales.

Si en un capítulo anterior se ha tratado de forma genérica la instalación de cámaras para el uso policial, analizando los tipos de cámaras y su regulación, se abordarán ahora cuestiones más concretas sobre su utilización y los efectos de las imágenes obtenidas.

Como se ha indicado, la instalación de las videocámaras por los agentes de la policía ha de realizarse de acuerdo con lo establecido en la LO 4/1997, de 4 de agosto. Ya se ha hecho referencia a la finalidad preventiva que cumplen estos instrumentos, y también a que pueden ser utilizados, junto con otros indicadores, para llevar a cabo una función predictiva. En este sentido, cabe recordar lo puesto ya de relieve cuando se ha analizado la regulación de la LO 7/2021, de 26 de mayo, de protección de datos personales, y, concretamente de sus artículos 15 a 19. En lo que atañe al objeto de estas consideraciones, cuando con ocasión de la revisión de las imágenes captadas, los agentes policiales tengan conocimiento de un hecho que se considere delictivo, se pondrá la grabación a disposición de la autoridad judicial en el plazo máximo de 72 horas. Se puede deducir de ello que, durante este tiempo, la ley permite a la policía realizar una serie de diligencias complementarias que tendrán como finalidad corroborar la comisión delictiva. Dichas diligencias no podrán comprometer la eficacia de los derechos fundamentales. Conforme a lo dicho, se permite legalmente que la policía pueda grabar imágenes en lugares públicos sin autorización judicial previa.

Cabe precisar que la autorización prevista en la Ley 4/1997, hace referencia a la utilización de cámaras en lugares públicos y su posterior tratamiento, con la finalidad de «...asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública». En el mismo sentido, se ha de entender la regulación del artículo 15.2, de la LO 7/2021, de tratamiento de datos personales, que condiciona la instalación, entre otros criterios: «...a prevenir, detectar o investigar la comisión de infracciones penales y la protección y prevención frente a las amenazas contra la seguridad pública». En ambos supuestos, el legislador centra la utilización de las videograbaciones en relación con las funciones de prevención e investigación, ya sea para la obtención de las imágenes, o para su tratamiento. En ninguno de los dos casos se hace mención alguna de la previa existencia de un proceso penal ya iniciado, lo que lleva a considerar que las actuaciones policiales podrán tener lugar con anterioridad al inicio de la fase de instrucción.

Cuestión distinta es la regulada en el artículo 588 quinquies a) LECrim, ya que en este caso la ley procesal penal se refiere expresamente a la obtención de imágenes de la «persona investigada», de lo que se deduce que ya se ha incoado el proceso penal. Al no exigir el precepto autorización judicial previa, el legislador limita esta actuación a su necesidad para «...facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos». En estos casos, será de

aplicación el régimen jurídico previsto en el citado artículo 588 quinquies a) y siguientes de la Ley procesal penal. No obstante, también habrán de tenerse en cuenta, en su caso, las disposiciones comunes previstas en el Capítulo IV, y especialmente las relativas al principio de necesidad y proporcionalidad de la medida, que deberá valorarse por el juzgador en el control judicial que se realice en el momento en que las grabaciones se introduzcan en la causa.

Es necesario precisar en este punto, que, al no requerir autorización judicial, no se facilita resolución alguna que recoja la modalidad de la medida, aunque el alcance ya se encuentra delimitado en el artículo citado. En consecuencia, el control judicial se produce a posteriori, una vez que se han entregado las grabaciones al juzgador²⁹⁸. Sobre dicho control ya se ha pronunciado el Tribunal Supremo años atrás en una resolución que marca los elementos a tener en cuenta: «...*La incorporación a los autos de la filmación videográfica, deberá efectuarse bajo el control de la Autoridad judicial, enunciado éste que engloba las siguientes garantías: 1.º) Control judicial de la legitimidad de la filmación, que implica el que el juez instructor supervise que la captación de las imágenes se efectuó con el debido respeto a la intimidad personal y a la inviolabilidad domiciliaria, pues si la filmación merece un juicio desfavorable notoriamente a la luz de los citados derechos fundamentales debería negarse la incorporación a los autos de la filmación «ex» artículo 11 de la Ley Orgánica del Poder Judicial. 2.º) Comunicación y puesta a disposición judicial del material videográfico, en términos relativamente breves, por cuanto que la aportación mientras más rápida sea, constituye una garantía en favor de su autenticidad, por cuanto que ella, va en detrimento de su posible manipulación. 3.º) Aportación de los soportes originales a los que se incorporan a las imágenes captadas. 4.º) Aportación íntegra de lo filmado, a fin de posibilitar la selección judicial de las imágenes relevantes para la causa»*²⁹⁹.

Un paso más allá en la utilización de dispositivos de captación de imagen, se produce con la regulación de la captación de imágenes y sonidos, que sólo se permite con autorización judicial previa, tal y como se desprende de la regulación del artículo 588 quater a), LECrim, cuando establece que «*podrá autorizarse la colocación y utilización de dispositivos electrónicos que permitan la captación y grabación de las comunicaciones orales directas...*» del investigado, para precisar en su tercer apartado que «*La escucha y grabación de las conversaciones privadas se podrá complementar con la obtención de imágenes cuando expresamente lo autorice la resolución judicial que*

298 V. en esta cuestión la Circular 4/2019, FGE, en la que se señala esta diferencia temporal del control judicial. Mientras que en las otras medidas de investigación tecnológica el control se produce con anterioridad a la resolución judicial, por tanto, la autorización del juez de instrucción se otorga previo análisis de los principios de proporcionalidad, idoneidad y necesidad de la medida. En el caso de la captación de imágenes en lugares públicos, el control judicial tiene lugar a posteriori, una vez realizada la grabación.

299 Por todas, STS 968/1998, de 17 julio.

la acuerde». No sólo se hace referencia a la «autorización», si no que en el artículo 588 quater c) se recoge el contenido de la resolución judicial autorizante³⁰⁰.

En este contexto, cabe colegir que si la captación de imágenes ha de producirse en lugares no públicos será necesario recabar la autorización judicial, de acuerdo con lo dispuesto en el artículo 588 bis b) LECrim, que regula el capítulo IV, las Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.

Resulta conveniente precisar, a efectos de aclarar la aplicación de una u otra normativa, lo que se entiende por lugar público. La consideración de un lugar determinado como público o privado no depende de su titularidad³⁰¹, sino que se encuentra en estrecha relación con el ámbito de protección del derecho a la inviolabilidad del domicilio y del derecho a la intimidad³⁰². En este sentido, cabe señalar, que el recinto domiciliario, o cualquier espacio cerrado en el que de forma habitual se pueda desarrollar la vida privada de la persona y que, por tanto, genera una expectativa de privacidad, cuenta con la protección del artículo 18.1 y 2 CE³⁰³. A este respecto se ha pronunciado el Tribunal Supremo en numerosas resoluciones, defendiendo el recinto domiciliario de intromisiones ajenas, incluso en aquellos casos en los que no se produce una entrada física en el domicilio. Así, ha manifestado que «...*la tutela constitucional del derecho proclamado en el apartado 2 del art. 18 de la CE protege, tanto frente la irrupción inconsentida del intruso en el escenario doméstico, como respecto de la observación clandestina de lo que acontece en su interior, si para ello es preciso valerse de un artificio técnico de grabación o aproximación de las imágenes*»³⁰⁴.

300 MARCHENA GÓMEZ, M./GONZÁLEZ-CUELLAR SERRANO, N., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Editorial Castillo de Luna, Madrid, 2015, pág. 360.

301 MARCOS AYJÓN, M., «Captación de imágenes por la policía en el garaje de una comunidad de vecinos. Análisis de la STC 92/2023» en *LA LEY Penal*, número 164, 2023, <https://legal-teca-aranzadilaley-es.ezbusc.usc.gal>, pág. 6.

302 V. SSTC 231/1988, de 2 de diciembre; 237/2007, de 7 de noviembre. V. SSTs 7 de julio de 1988; 485/2013, de 5 de junio; 124/2014, de 3 de febrero; 67/2014, de 28 de enero; 569/2020, de 30 de octubre

303 V. SSTC 231/1988, de 2 de diciembre; 134/1999, de 15 de julio; 144/1999, de 22 de julio; 14/2003, de 28 de enero; 127/2003, de 30 de junio; 196/2004, de 15 de noviembre; 89/2006, de 27 de marzo; 206/2007, de 24 de septiembre; 236/2007, de 7 de noviembre; 70/2009, de 23 de marzo; 60/2010, de 7 de octubre; 173/2011, de 7 de noviembre; 93/2013, de 23 de abril, entre otras.

304 SSTs 354/2003, de 13 de marzo; 329/2016, de 20 de abril, entre otras.

Sin embargo, es necesario poner de relieve, que el desarrollo de la intimidad puede realizarse también en espacios no considerados como domicilio³⁰⁵. Así, podrán tener la consideración de espacio no público, aquellos lugares fuera del domicilio, en los que las personas tengan expectativas de preservarlos del acceso de terceros, y en los que puedan desenvolver su intimidad³⁰⁶. Ya se ha hecho referencia en páginas anteriores a la postura del Tribunal Constitucional, al afirmar que el garaje de una comunidad de vecinos, sin tener la consideración de domicilio, se puede rodear de una *expectativa razonable de privacidad*, que se encuentra protegida por el artículo 18.1 CE, al tratarse de un lugar cerrado integrado en una propiedad privada de acceso restringido³⁰⁷.

3.2.2. Vigilancia policial con drones

Junto a la información proporcionada por las cámaras de videovigilancia, cobra ahora mayor protagonismo la información facilitada por los conocidos drones. Se trata de pequeñas aeronaves pilotadas por control remoto, o con funcionamiento autónomo, que tienen incorporadas cámaras y dispositivos que permiten obtener imágenes y sonidos³⁰⁸. El tipo de diseño del dron condicionará la mayor o menor distancia en la que pueden desempeñar sus funciones.

La circulación de drones por el espacio aéreo se regula en el Real Decreto 517/2024, de 4 de junio, por el que se desarrolla el régimen jurídico para la utilización civil de sistemas de aeronaves no tripuladas (UAS)³⁰⁹, y se modifican diversas normas reglamentarias. Esta norma se dicta con la finalidad de adaptar la normativa española al Reglamento (UE) 2018/1139, del Parlamento Europeo y del Consejo, de 4 de julio de 2018, sobre normas comunes en el ámbito de la aviación civil, conocido como Reglamento base, por el que se crea una Agencia de la Unión Europea para la Seguridad Aérea, y se modi-

305 V. STS STC 92/2023, de 11 de septiembre. V. también las SSTC 12/2012, de 30 de enero, 18/2015, de 16 de febrero; 25/2019, de 25 de febrero, entre otras.

306 MARCHENA GÓMEZ, M./GONZÁLEZ-CUELLAR SERRANO, N., *La reforma de la Ley de Enjuiciamiento Criminal en 2015...*, op. cit., pág. 356.

307 STC 92/2023, de 11 de septiembre.

308 V. más ampliamente MARTÍNEZ AYUSO, M.A., «Drones: limitaciones de vuelo y tratamiento de datos personales» en *El Consultor de los Ayuntamientos*, número 8, agosto 2021.

309 Inicialmente se parte de la Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia, por la que se modificaba la Ley de Navegación Aérea de 1960, para introducir la normativa sobre aeronaves civiles pilotadas por control remoto. Posteriormente y ante las lagunas de la citada regulación se dicta el R.D. 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto. Al que se añade el R.D. 1180/2018, de 21 de septiembre, de desarrollo reglamentario del aire y otras disposiciones sobre servicios y procedimientos de navegación aérea.

fican otros Reglamentos³¹⁰. El artículo 3.30 de dicho Reglamento, ofrece una definición de «aeronave no tripulada», integrando en su concepto tanto aquellas que están diseñadas para ser pilotadas a distancia, como las que pueden operar de forma autónoma³¹¹.

El artículo 1 del citado RD 517/2024, de 4 de junio, en su primer apartado, letra b), señala entre sus objetivos *«Establecer el régimen jurídico aplicable a las aeronaves no tripuladas y sus motores, hélices, componentes, equipos no instalados y equipos para controlar la aeronave a distancia, cuando lleven a cabo actividades o servicios civiles de aduanas, policía, búsqueda y salvamento, lucha contra incendios, control fronterizo, vigilancia costera o similares, emprendidas en el interés general por un organismo investido de autoridad pública o en nombre de este, así como al personal y a las organizaciones que participen en las actividades y los servicios desarrollados por dichas aeronaves (en lo sucesivo, «actividades o servicios no EASA»)...*». Precisa también el precepto que *«A estos efectos se entiende por actividades de policía, en sentido estricto, las realizadas por las fuerzas y cuerpos de seguridad regulados en la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad...»*.

Lo importante de estos dispositivos respecto de este estudio, es que proporcionan imágenes y sonidos a la policía, que le permite adoptar medidas preventivas, o bien diligencias de investigación en el marco del proceso penal. Si bien en este último caso la Ley procesal penal no ofrece una regulación específica en la que se mencione, o se haga referencia expresa a los drones, sí es cierto, como ya se ha comprobado, que el artículo 588 quinquies a) permite a la Policía Judicial la captación de imágenes de la persona investigada en lugares públicos a través de su grabación *«...por cualquier medio técnico»*. Cabe así integrar la grabación de imágenes con los drones en este precepto, cuando la policía está realizando una actividad investigadora vinculada a un proceso penal en curso.

No obstante, en aquellos casos en los que se pretenda la grabación de imágenes y sonidos no podrá aplicarse dicho precepto, que hace referencia

310 Se modifican los Reglamentos (CE) n.º 2111/2005, (CE) n.º 1008/2008, (UE) n.º 996/2010, (CE) n.º 376/2014 y las Directivas 2014/30/UE y 2014/53/UE del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) n.º 552/2004 y (CE) n.º 216/2008 del Parlamento Europeo y del Consejo y el Reglamento (CEE) n.º 3922/91 del Consejo,

311 La Unión Europea ha venido a extender su competencia sobre todas las aeronaves no tripuladas civiles, independientemente de su masa operativa, excepto, sobre aquellas utilizadas para llevar a cabo actividades o servicios de aduanas, policía, búsqueda y salvamento, lucha contra incendios, control fronterizo, vigilancia costera o similares, entre las que se incluyen las de vigilancia y disciplina del tráfico en todo el territorio nacional, bajo el control y la responsabilidad de un Estado miembro, emprendidas en el interés general por un organismo investido de autoridad pública o en nombre de este (en adelante «actividades o servicios no EASA»), y aquellas aeronaves no tripuladas cuya explotación suponga un bajo riesgo para la seguridad aérea, según lo indicado en el anexo I, del Reglamento Base.

exclusivamente a la captación de imágenes. El régimen jurídico aplicable en estos casos sería el establecido en el artículo 588 quater a) LECrim, que se ocupa de la grabación de las comunicaciones orales directas, estableciendo en su tercer apartado la posibilidad de que dicha grabación se pueda completar con la captación de imágenes, autorizándola expresamente en la resolución por la que se adopta la medida. Se trata de una medida que puede resultar enormemente invasiva. En algunas ocasiones, la utilización de un dron puede suponer la incidencia en el derecho a la inviolabilidad del domicilio, en el derecho al secreto de las comunicaciones y en el derecho a la intimidad³¹².

Teniendo en cuenta, por tanto, el abanico de derechos fundamentales afectados, no cabe únicamente aplicar las disposiciones comunes a la investigación con medidas tecnológica, previstas en el Capítulo IV de la Ley de Enjuiciamiento Criminal. Antes, al contrario, sería adecuado una combinación de las normas que regulan la incidencia en cada uno de los derechos fundamentales afectados. De esta forma, partiendo de la aplicación de los artículos 588 quater a), y siguientes, que regulan la intervención de las comunicaciones orales directas, y permite la captación complementaria de imágenes, cuando resulte necesario penetrar en el domicilio, o lugar en el que las personas puedan desarrollar su privacidad, con expectativas de preservarla del acceso de terceros, serán también de aplicación las disposiciones relativas a la entrada domiciliaria, delimitando así las garantías que han de observarse al utilizar una herramienta, muy útil para la investigación delictiva, pero también muy restrictiva de la esfera privada de las personas. En este sentido, cabe resaltar que el artículo 488 quater a), 2 LECrim, señala expresamente que «...*En el supuesto en que fuera necesaria la entrada en el domicilio o en alguno de los espacios destinados al ejercicio de la privacidad, la resolución habilitante habrá de extender su motivación a la procedencia del acceso a dichos lugares*», lo que lleva a relacionar dicha regulación con la prevista para la entrada en el domicilio.

Volviendo a la investigación policial preprocesal, el artículo 17, LO 7/2021, permite la utilización de dispositivos móviles de captación de imágenes y sonido, si bien la condiciona a «...*la concurrencia de un peligro o evento concreto*». Desde una perspectiva constitucional resulta sorprendente la regulación de este precepto, dada la referencia genérica a la grabación de sonidos, sin precisar que no deben incluirse en esta autorización las comunicaciones orales. La grabación de sonidos a través de dispositivos móviles puede incidir en el derecho al secreto de las comunicaciones privadas, ya que en lugares públicos también se desarrollan este tipo de conversaciones entre particulares, que, en principio no tienen intención de hacerlas públicas, como ya se ha indicado anteriormente. Es conveniente traer a colación la doctrina del Tribu-

312 ARIZA COLMENAREJO, M.J., «Garantías procesales en el uso de drones en la investigación penal», en *Era digital...*, op. cit., pág. 341.

nal Constitucional sobre la protección del derecho al secreto de las comunicaciones, recogida en la célebre sentencia 114/1984, de 29 de noviembre, «... *la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros (públicos o privados: el derecho posee eficacia erga omnes) ajenos a la comunicación misma. La presencia de un elemento ajeno a aquellos entre los que media el proceso de comunicación, es indispensable para configurar el ilícito constitucional aquí perfilado*».

Partiendo de la propia redacción del precepto constitucional, el artículo 18.3 CE garantiza el secreto de las comunicaciones, especialmente las postales, telegráficas y telefónicas, salvo resolución judicial. De esta forma, el Tribunal Constitucional condiciona la injerencia el derecho protegido a la existencia de una resolución judicial autorizante. «...*El art. 18.3 CE contiene una especial protección de las comunicaciones, cualquiera que sea el sistema empleado para realizarlas, que se declara indemne frente a cualquier interferencia no autorizada judicialmente*»³¹³. La integración de las comunicaciones orales directas entre dos o más sujetos en el ámbito de protección del derecho al secreto de las comunicaciones ya se ha puesto de relieve por numerosas sentencias del Tribunal Constitucional. Si bien en un principio se dudaba entre su inclusión en el derecho a la intimidad, o en el derecho al secreto de las comunicaciones³¹⁴, esta postura se ha modificado hasta integrarlas en el derecho regulado en el artículo 18.3 CE³¹⁵.

También el Tribunal Europeo de Derechos Humanos se ha preocupado de garantizar el secreto de las comunicaciones privadas realizadas de forma oral y directa, al afirmar que la interceptación de una comunicación personal, cualquiera que sea el medio utilizado por el tercero, incluido el medio oral o medioambiental, infringe el artículo 8 CEDH. Basta para ello, que la interceptación se realice con cualquier instrumento técnico que exceda de la simple audición habitual de un sujeto mediante los sentidos³¹⁶.

En este contexto, una regulación más acorde con la protección del derecho fundamental al secreto de las comunicaciones, debería condicionar la utilización de dispositivos móviles de grabación de imágenes y sonidos, conforme al artículo 17 citado, a que los sonidos de referencia no puedan encuadrarse en el concepto de comunicación, ya que, en este caso, se estaría produciendo una intervención de comunicaciones personales, que exigiría la resolución judicial previa, y su ejecución con las garantías previstas en la Ley de Enjuiciamiento Criminal.

313 STC 70/2002, de 3 de abril.

314 SSTC 98/2000, de 10 de abril; 123/2002, de 20 de mayo; 170/2012, de 7 de octubre, entre otras.

315 STC 145/2014, de 22 de septiembre.

316 STEDH de 20 de diciembre de 2005, Wisse c. Francia,

3.3. Dispositivos de geolocalización y seguimiento: una aproximación a su estudio

3.3.1. Instrumentos vinculados al investigado

Entre los variados instrumentos de vigilancia que la tecnología pone al servicio de las Fuerzas y Cuerpos de la Seguridad del Estado, se ha de hacer mención a los dispositivos técnicos de seguimiento y geolocalización. Su relevancia para la investigación policial, tanto la desarrollada con carácter preventivo, como la que se inicia una vez incoado el proceso penal, es indudable. Como también lo es, que con su despliegue se pueden poner en peligro derechos fundamentales, por lo que se requiere de nuevo, establecer los requisitos y garantías que permitan que los resultados obtenidos puedan ser tenidos en cuenta en el material probatorio del proceso penal.

Es conveniente advertir que los requisitos para la instalación de este tipo de dispositivos han sido modificados como consecuencia de la entrada en vigor de la Ley 13/2015, que rodea esta diligencia de mayores garantías que las requeridas con anterioridad. Por tal motivo, se ha considerado necesario hacer referencia a la regulación que la Ley procesal penal recoge para la ejecución de esta diligencia.

Precisamente, sobre su legítima utilización se pronuncia el Tribunal Constitucional, cuando afirma que tienen una «...*incidencia directa en el círculo de exclusión que cada ciudadano define frente a terceros y frente a los poderes públicos, siendo que la afectación de la intimidad es incuestionable, más allá de que, conforme a la jurisprudencia constitucional y de esta Sala, existan actos de injerencia que, sin estar expresamente reservados a la autorización judicial, pueden ser plenamente validos al perseguir un fin constitucionalmente legítimo en una sociedad democrática*»³¹⁷.

No obstante, como se ha señalado en el capítulo anterior, ésta no ha sido siempre la postura de nuestros tribunales. La doctrina jurisprudencial anterior a la entrada en vigor de la Ley 13/2015, era más permisiva, y defendía una interpretación más flexible en relación con la protección del derecho a la intimidad. De esta forma, consideraba el Tribunal Supremo en su sentencia 562/2007, de 22 de junio, que «...*el artificio colocado permitió a los agentes de investigación el seguimiento por mar de la embarcación respecto a la que existían fundadas sospechas de su dedicación al tráfico de drogas. La colocación de esa baliza permitió realizar el seguimiento de la embarcación, ubicarla en alta mar y para su colocación, en los exteriores del barco, no se precisó ninguna injerencia en ámbitos de intimidad constitucionalmente protegidos. Se trata, en definitiva, de una diligencia de investigación, legítima desde la función constitucional que tiene la policía judicial, sin que en su*

317 STS 141/2020, de 13 de mayo.

colocación se interfiriera en un derecho fundamental que requeriría la intervención judicial»³¹⁸. Esta postura jurisprudencial también era defendida por el TEDH, que si bien consideraba que la instalación de los denominados GPS podía suponer una injerencia en la vida privada de las personas, protegida por el artículo 8 CEDH, también afirmaba que el control judicial posterior de la medida podía validar su utilización³¹⁹.

La doctrina del Tribunal Supremo se modifica sustancialmente como consecuencia de la entrada en vigor de la Ley 13/2015, y es la sentencia 141/2020, de 13 de mayo, la que recoge de forma exhaustiva los requisitos y garantías que, a partir de dicha regulación, habrán de observarse para la instalación de dispositivos de localización³²⁰. También la Circular 4/2019, de 6 de marzo, de la Fiscalía General del Estado, se pronuncia sobre la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, que además destaca la incidencia en otro derecho fundamental, el derecho a la protección de datos. Afirma la Fiscalía que *«...La recopilación sistemática de datos de posicionamiento afecta también al derecho a la protección de datos personales del investigado (art. 18.4 CE), con una incidencia directa, además, en el derecho a la intimidad. De este modo, el conocimiento de un solo dato de geolocalización (como, por ejemplo, la visita a un templo), puede afectar a la intimidad del investigado; pero la recopilación sistemática de estos datos y su tratamiento informático puede proporcionar información precisa sobre los hábitos de una persona, lo que supone una intromisión mucho más intensa en la intimidad del investigado»*.

La citada Circular hace referencia a dos modalidades de sistemas de geolocalización y seguimiento. Una primera, en la que se integran los conocidos como balizas de seguimiento, que son dispositivos técnicos basados en sis-

318 V. igualmente las SSTS 523/2008, de 11 de julio; 906/2008, de 19 de diciembre; 798/2013, de 5 de noviembre; 619/2026, de 7 de julio.

319 Considera el Tribunal en la sentencia de 2 de septiembre de 2010, Caso Uzun contra Alemania, que «la vigilancia por GPS por su propia naturaleza puede distinguirse de otros métodos de vigilancia visual o acústica que son, por regla general, más susceptibles de interferir en el respeto al derecho a la vida privada porque revelan más información sobre la conducta, opiniones o sentimiento de una persona. Teniendo en cuenta los principios establecidos en la jurisprudencia, los factores anteriormente mencionados son suficientes para concluir que la observación del solicitante a través del GPS, y el uso de datos obtenidos de este modo de la manera anteriormente descrita, equivalen a una injerencia en la vida privada según lo protegido por el art. 8 CEDH...» pero la «...revisión judicial y la posibilidad de excluir las pruebas obtenidas de una vigilancia GPS ilegal constituyeron una salvaguarda importante, ya que disuadió a las autoridades investigadoras de recopilar pruebas por medios ilegales. En vista de hecho de que se debe considerar que la vigilancia por GPS interfiere menos con la vida privada de una persona que, por ejemplo, las escuchas telefónicas (...), el Tribunal considera que la revisión judicial posterior de la vigilancia de una persona por parte de GPS ofrece una protección suficiente contra la arbitrariedad».

320 V. también las STS 291/2021, de 7 de abril. V. también las SSTS 971/2022, de 16 de diciembre; 92/2023, de 11 de septiembre, entre otras.

temas de posicionamiento global, también denominados GPS (entre otros). La segunda modalidad, que se incluiría en la denominación de medios técnicos de geolocalización y seguimiento, deriva de los datos electrónicos asociados a sistemas de comunicación telefónica³²¹.

Las balizas y los GPS son dispositivos colocados en un sujeto o en un objeto, que emiten una señal constante y permiten un seguimiento continuado, proporcionando su localización continua. En el caso de la localización y seguimiento facilitados por las señales asociadas a la telefonía móvil, resulta posible gracias a los datos facilitados por las compañías telefónicas que permiten ubicar el terminal en una localización. Tal y como recoge la Circular 4/2019, se trata de datos asociados a las comunicaciones, y no de datos de tráfico, ya que es posible captarlos con independencia del mantenimiento de una comunicación³²². Dicha captación se puede producir en tiempo real, utilizando para ello el sistema SISTEL, o bien con posterioridad, recabando «...los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación...» conforme a lo establecido en el artículo 588 ter j) LECrim. En uno y otro caso es preciso poner de relieve el deber de colaboración de estas compañías y empresas, de acuerdo con lo establecido en el artículo 588 ter e) LECrim³²³. El régimen jurídico general aplicable para los dos tipos de geolocalización se regula en los artículos 588 quinquies b) y siguientes de la Ley procesal penal.

Respecto de la instalación de un dispositivo localizador en un objeto, se ha de poner de relieve que la Ley procesal penal, al regular el régimen jurídico es esta medida, la vincula a la vulneración de alguno de los derechos que se recogen en el artículo 18 CE. Así lo titula en su Título VIII «De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución». Por tanto, cuando la medida no afecte a los derechos previstos en el citado artículo podrá llevarse a cabo sin autorización judicial. Así lo declara la Fiscalía General del Estado al hacer referencia a la instalación de

321 Sobre las modalidades de dispositivos de seguimiento v. también DELGADO MARTÍN, J., «Dispositivos de localización y seguimiento en la investigación penal, en «Logos». *Revista Científica del Centro Universitario de la Guardia Civil*, número especial, febrero, 2023, pág. 86; GARCÍA MARCOS, J., «Geolocalización y derechos fundamentales» en *El Derecho.com*. Noticias jurídicas y de actualidad, 29 noviembre 2011, <https://elderecho.com/geolocalizacion-y-derechos-fundamentales>, pág. 2.

322 En este sentido se permite en el artículo 599 ter b) 2, LECrim., cuando establece que «La intervención judicialmente acordada podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario».

323 V. la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

estos dispositivos en paquetes postales³²⁴. Lo verdaderamente determinante de la necesidad de autorización judicial previa, no es el emplazamiento del dispositivo, sino si, con su ubicación, puede ponerse en peligro el derecho a la intimidad o el derecho a la protección de datos.

A partir de la Ley 13/2015, en ningún caso se permite la adopción de esta medida sin autorización judicial, ya que la vigilancia y seguimiento se realiza sobre personas concretas. No obstante, por razones de urgencia, la policía pueda acudir a estos dispositivos sin autorización judicial, cuando existan motivos para temer que el retraso en la instalación pueda frustrar la investigación. Dado el caso, esta actuación deberá ponerse en conocimiento del juez de instrucción en el menor plazo posible y, en todo caso, en el plazo máximo de veinticuatro horas³²⁵. El juzgador deberá validar la medida y, en caso contrario, no podrá surtir efectos en el proceso.

Los artículos 588 quinquies b) y siguientes LECrim, hacen referencia a la necesidad y proporcionalidad de la medida y a su excepcionalidad. Se requiere autorización para su instalación y control judicial en su ejecución, estableciéndose además un plazo inicial máximo de tres meses, que puede prorrogarse hasta 18 meses, con autorización judicial debidamente motivada. También se contempla que la policía pueda acudir a estos dispositivos sin autorización judicial por razones de urgencia, tal y como se ha puesto ya de relieve. En todo caso, ha de tenerse en cuenta la regulación establecida en las disposiciones comunes recogidas en el Capítulo IV LECrim, en lo que hace referencia al ámbito de aplicación, contenido de la resolución judicial, aplicación de los principios rectores...³²⁶.

En el caso de la geolocalización y seguimiento vinculada a datos asociados a la telefonía móvil, se trata de servicios proporcionados por las empresas de telecomunicaciones que permite determinar la posición aproximada de un teléfono móvil gracias a su constante conexión con las estaciones BTS.

El régimen jurídico aplicable sería el ya descrito de los artículos 588 quinquies y siguientes, completándose con las disposiciones comunes del citado Capítulo IV. Sin embargo, es necesario tener en cuenta que si los datos de geolocalización que se requieren son de fechas anteriores a la resolución autorizante, se aplicarán los artículos 588 sexies a) y siguientes, cuando se pretenda el registro de dispositivos GPS hallados en poder del investigado, o

324 V. Circular 4/2019, FGE.

325 Sobre la aplicación del plazo de 24 horas y su vinculación a la existencia de control judicial v. SSTS 475/2018, de 17 de octubre de 2018; 199/2023, de 21 de marzo; 549/2024, de 6 de junio,

326 Sobre la aplicación de los principios rectores en esta medida, es importante poner de relieve la STS 549/2024, de 6 de junio, en la que el Tribunal se pronuncia sobre la intensidad en su aplicación, diferenciando la medida de geolocalización de la intervención de las comunicaciones telefónicas y telemáticas.

el art. 588 ter j, cuando se trate de obtener datos asociados a comunicaciones telefónicas que obren en los archivos automatizados de los prestadores de servicios, o personas que faciliten comunicaciones, en cumplimiento de la legislación sobre retención de datos relativos a comunicaciones electrónicas³²⁷.

En este sentido, cabe apuntar que, en los supuestos de geolocalización y seguimiento derivados de datos electrónicos asociados a telefonía móvil, la injerencia en los derechos fundamentales es mayor, ya que la información proporcionada va a facilitar también otros datos como el itinerario, los horarios, las incidencias, etc., por lo que la aplicación del principio de necesidad y proporcionalidad de la medida ha de ser más riguroso³²⁸. En este sentido, también es importante que el juzgador tenga en cuenta el tiempo durante el cual se autoriza la medida, y desde luego, el hecho delictivo investigado. La estricta aplicación del principio de proporcionalidad, va a exigir que los elementos anteriores se ponderen, para decidir sobre la adopción de la medida.

En este contexto, ha de traerse a colación la importancia de precisar en la solicitud policial y en la autorización judicial, el dispositivo o el medio técnico que se va a utilizar, al influir también en la mayor o menor afectación de los derechos fundamentales. El juicio de la proporcionalidad va a depender en gran medida de su concreción, al vincularse con su alcance y con la limitación del derecho fundamental en juego. Así lo considera la Fiscalía General del Estado cuando afirma que *«...existen diferentes medios o dispositivos técnicos de seguimiento y localización y, cada uno de ellos, presenta unas características diferentes, al resultar también diferentes el número de datos que generan y su precisión»*³²⁹.

3.3.2. Geolocalización no vinculada al investigado

Hasta aquí, se han puesto de manifiesto los requisitos y garantías que han de observarse para la utilización de los dispositivos y medios técnicos de geolocalización y seguimiento vinculados al investigado. No obstante, la información útil para la investigación también puede obtenerse de terceros que, por su ubicación y relación con el investigado, o incluso, sin relación alguna, pueden proporcionar datos de los que se deduzcan la ubicación y los movimientos del sujeto investigado.

En estos casos, no se trata de la colocación de dispositivos o medios técnicos de transmisión por parte de la policía, sino del aprovechamiento de los

327 Circular FGE 4/2019, de 6 de marzo,

328 VELASCO NÚÑEZ, E., «Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica» en *Diario LA LEY*, número 8183, 4 de noviembre de 2013.

329 Circular FGE 4/2019, de 6 de marzo.

datos proporcionados por terminales, o instrumentos electrónicos de terceras personas, que son recabados por los agentes policiales para la investigación. El Tribunal Supremo analiza uno de los casos en los que se puede producir esta obtención de datos en poder de terceros. En su análisis pone de relieve la justificación dada por el Tribunal Superior de Justicia de Cataluña, al no considerar necesaria la autorización judicial para el acceso a los datos almacenados en el GPS de un vehículo de alquiler³³⁰. Se trata de un requerimiento hecho por la policía a una empresa de alquiler de vehículos para que le proporcione los datos del itinerario de uno de sus coches que ha sido utilizado por el investigado. El Tribunal Supremo describe los argumentos del tribunal de instancia, y si bien considera que la resolución judicial y el principio de proporcionalidad son aplicables cuando puede estar en juego el respeto al derecho a la intimidad, como es el caso de la instalación de dispositivos de geolocalización y seguimiento, y pone en duda que en el caso tratado por la sentencia de instancia pueda relativizarse la aplicación de los principios rectores, sin embargo justifica la resolución recurrida avalando la justificación del tribunal.

En la citada resolución, el tribunal de instancia considera que la policía no ha instalado ningún dispositivo en el vehículo, sino que se vale de los datos almacenados por el GPS, por lo que no se encuentra en el ámbito de aplicación de los instrumentos regulados en los artículos 588 quinquies y siguientes. La actuación policial no se realiza respecto de datos de dispositivos GPS que se encuentren en poder del investigado, por lo que no se puede acudir a las previsiones de los artículos 588 sexies a) y siguientes. Tampoco puede ubicarse en la regulación relativa a la obtención de datos asociados a comunicaciones telefónicas archivadas por prestadores de servicios, o personas que faciliten comunicaciones en cumplimiento de la legislación sobre retención de datos relativos a comunicaciones electrónicas. Finalmente, como la propia sentencia pone de relieve, los datos obtenidos por este requerimiento corroboran los proporcionados por el móvil del investigado, y, además no aportan tampoco ningún tipo de sonido o imagen. Teniendo en cuenta todo ello, el tribunal considera que en estos casos no es necesaria la autorización judicial previa³³¹.

Sin embargo, no es esta la postura más acorde con la protección del derecho fundamental a la intimidad. Una interpretación más garantista puede hacerse señalando que, en realidad, el legislador cuando hace referencia en el artículo 588 sexies a) 1, LECrim, a la exigencia de resolución judicial autorizante para la «...*aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática, o dispositivos de almacenamiento masivo de información digital, o el acceso a repositorios telemáticos de datos... el acceso de los agentes facultados a la información contenida en tales dispositivos*»,

330 STSJC 357/2021, de 2 de noviembre.

331 STS 835/2022, de 21 de octubre.

actuación que, como indica el precepto, se lleva a cabo con ocasión de un registro domiciliario, en ningún momento se especifica que dichos dispositivos sean propiedad del investigado.

En la misma línea, cuando en el artículo 588 sexies b) de la misma norma, se regula el acceso a la información de dispositivos electrónicos incautados fuera del domicilio del investigado, y se establece también que el procedimiento descrito anteriormente «...será también aplicable a aquellos casos en los que los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, o el acceso a repositorios telemáticos de datos, sean aprehendidos con independencia de un registro domiciliario», tampoco se exige que dichos instrumentos electrónicos se encuentren en poder del investigado. Sin embargo, lo que sí se requiere expresamente es que, si la policía considera indispensable el acceso a la información, lo ponga en conocimiento del juez para que otorgue la correspondiente autorización³³².

Parece evidente que el acceso a los datos almacenados en el GPS de un vehículo alquilado, puede reconducirse a la regulación prevista en el artículo 588 sexies b) LECrim, que recoge las disposiciones relativas a los dispositivos de almacenamiento masivo de datos, debiendo dictarse la correspondiente autorización judicial tal y como prevé el precepto³³³.

3.3.3. Geolocalización vinculada a datos proporcionados por terceros

Otra fuente de información sobre la localización de un sujeto puede proporcionarse por terceros con los que se relaciona ya sea directa o indirectamente. Diariamente accedemos e interactuamos con smartphones, ordenadores, iPads, etc., que facilitan la comunicación entre las personas a través del intercambio de información, pero que, al mismo tiempo, dejan un rastro fácilmente identificable de nuestra vida privada, de los datos intercambiados y del lugar en el que se produce la conexión. Los sistemas electrónicos de pago, las cámaras de videovigilancia instaladas no sólo por la policía en lugares públicos, sino también en establecimientos públicos y lugares de ocio, contribuyen a determinar el lugar concreto y el deambular de los ciudadanos³³⁴.

El Tribunal Constitucional se ha pronunciado sobre la vida personal que se refleja en los dispositivos electrónicos, y concretamente, en relación al

332 ZARAGOZA TEJADA, J.I., «La geolocalización del investigado en el proceso penal», en *Revista Aranzadi Doctrinal*, número 2, febrero 2025.

333 V. en este sentido la Circular 5/2019, de la FGE, que considera el GPS como un dispositivo de almacenamiento masivo de información; https://www.fiscal.es/memorias/memoria2020/FISCALIA_, pág. 1495.

334 ORTIZ PRADILLO, J.C., «Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos fundamentales en el proceso penal...», *op. cit.*, pág. 3.

contenido de los ordenadores personales, ha considerado que «...si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) —por lo que sus funciones podrían equipararse a los de una agenda electrónica—, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. 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 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. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática, así como de las nuevas tecnologías de la información»³³⁵.

De esta forma, el almacenamiento de datos personales por particulares y por entidades privadas, que los utilizan con fines comerciales, pueden proporcionar a los agentes policiales, no sólo la ubicación espacial del sujeto en cada momento determinado, sino incluso, un estilo de vida, hábitos y rutinas. La cesión por parte de entidades públicas y privadas de los datos relativos a operaciones bancarias, compra *online*, pago de peajes y alquiler de vehículos, cámaras de tráfico y datos proporcionados por la aerolíneas y hoteles, y un largo etcétera, no sólo proporcionan la ubicación temporal y espacial

335 STC 173/2011, de 7 de noviembre.

del individuo, sino que compromete seriamente sus derechos fundamentales vinculados al artículo 18 CE³³⁶.

Esta sociedad digital y tecnológica facilita y propugna nuevos cauces de investigación más acordes con el uso de los instrumentos de inteligencia artificial. Partiendo de lo apuntado, en estas nuevas formas de investigación policial, se favorece también la participación en la investigación de empresas externas a los poderes públicos, como cooperadores necesarios para la utilización de estos sistemas. Dicha entrada de operadores privados relacionados con las telecomunicaciones ya está prevista parcialmente por la Ley procesal penal que, en su artículo 588 ter e), los califica como colaboradores, si bien sus facultades, supervisión de actuaciones y responsabilidad no se regulan expresamente³³⁷.

Si se parte del deber de colaboración regulado en el artículo 7 de la LO 7/2021, puede defenderse que las entidades públicas y privadas deberán proporcionar a la policía judicial «...los datos, informes, antecedentes y justificantes que les soliciten y que sean necesarios para la investigación y enjuiciamiento de infracciones penales o para la ejecución de las penas». También precisa el precepto, que se dará cuenta a la autoridad fiscal o judicial, para recoger en su segundo apartado la obligación de facilitar «...los datos, informes, antecedentes y justificantes a las autoridades competentes que los soliciten, siempre que estos sean necesarios para el desarrollo específico de sus misiones para la prevención, detección e investigación de infracciones penales y para la prevención y protección frente a un peligro real y grave para la seguridad pública».

No obstante, el tercer apartado del este artículo 7, establece que lo dispuesto en los apartados anteriores no será de aplicación cuando «...legalmente sea exigible la autorización judicial para recabar los datos necesarios para el cumplimiento de los fines del artículo 1.» En este contexto, cabe deducir que las unidades policiales no podrán recabar los datos anteriormente indicados, cuando de su interacción o interrelación pueda afectarse gravemente en los derechos fundamentales previstos en el artículo 18 CE, puesto que para ello la regulación de los artículos 588 ter j) y 588 sexies b) de la Ley procesal penal, exige la autorización judicial³³⁸.

336 ORTIZ PRADILLO, J.C., «Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos fundamentales en el proceso penal» en *Diario La Ley*, número 9955, 18 de noviembre de 2021, Wolters Kluwer, pág. 4.

337 GASCÓN INCHAUSTI, F., «Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial», en *La justicia digital en España...*, op. cit., pág. 195.

338 V. en este sentido, DELGADO MARTÍN, J., «Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015» en *Diario LA LEY*, número 693, 2 de febrero de 2016.

De esta forma, el artículo 588 ter j) LECrim, al mismo tiempo que prevé la entrega de los datos electrónicos conservados por los prestadores de servicios en cumplimiento de la legislación sobre retención de datos, también la contempla respecto de otras personas que faciliten la comunicación por propia iniciativa cuando obedece a motivos comerciales o de otra índole³³⁹. En ambos casos se condiciona su entrega a la autorización judicial. Una vez más la intervención judicial se convierte en la garantía última de los derechos fundamentales. La misma autorización se exige en el segundo apartado del precepto, cuando la información almacenada en archivos automatizados de los prestadores de servicios resulte indispensable para la investigación, haciendo aquí una referencia expresa a la búsqueda entrecruzada o inteligente de datos³⁴⁰.

Esta posición se encuentra en estrecha relación con la protección del artículo 18.4 CE, respecto del derecho al entorno virtual, que protege los derechos fundamentales con entidad propia, como el derecho a la intimidad y a la propia imagen, el derecho al secreto de las comunicaciones y el derecho a la protección de datos, pero centrado en sus manifestaciones virtuales. Lo que resulta indudable hoy en día, es que el individuo no sólo desarrolla su personalidad y su vida privada en espacios físicos, sino que también lo hace, y cada vez en mayor medida, en espacios virtuales, que deben ser igualmente protegidos de injerencias tanto de particulares como de los poderes públicos.

3.4. Rastreo de redes

Otra de las modalidades de vigilancia policial que puede relacionarse con la investigación con fines de prevención, es la desarrollada en Internet, especialmente, en las redes sociales. A través de ella, los agentes de la policía, utilizando técnicas de rastreo, monitorizando redes y sitios web, almacenan una gran cantidad de datos que, relacionados por instrumentos de inteligencia artificial, proporcionan elementos relevantes para la prevención, o la investi-

339 En este sentido, la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, establece en su artículo 1, la obligación de los operadores de «...conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales»

340 Sobre la conservación de datos de telecomunicaciones v. más ampliamente V. RODRÍGUEZ LAINZ, J.L., «La nueva doctrina del Tribunal Supremo frente a la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de conservación preventiva de datos de telecomunicaciones» en *Uso de la información y de los datos personales...*, op. cit., págs. 375 y ss.

gación de hechos delictivos³⁴¹. Puede relacionarse este tipo de vigilancia con la realizada por los agentes policiales por las calles, las llamadas patrullas policiales. Tanto es así, que a esta vigilancia en redes se le denomina ciberpatrullaje. De todas formas, no es equiparable el patrullaje callejero con el que se desarrolla en la red. Este último afecta de una manera mucho más grave a los derechos relacionados con la vida privada, y además se lleva a cabo de forma más reservada.

La vigilancia de la red puede efectuarse, a través del rastreo de la red con cuentas propias relacionadas con sujetos concretos y determinados que pueden ser identificados, o a través de la creación de identidades falsas, que no permiten identificar al usuario. A través de la puesta en la red de una cuenta falsa se puede interactuar, sin dar a conocer la verdadera identidad, y al mismo tiempo recopilar información para que pueda ser analizada y relacionada con sistemas de inteligencia artificial. En la misma línea se incardina la interacción en red a través de programas informáticos que simulan a un usuario, y que se pone en relación con sujetos que creen estar comunicándose con una persona³⁴². En este último supuesto, la vigilancia se agrava al interactuar con identidades falsas, utilizando el engaño, y puede llegar a vincularse con la provocación delictiva, lo que incide de forma directa en las funciones propias de la policía, alejándola de la actuación preventiva a la que se está haciendo referencia³⁴³.

En este contexto, es preciso diferenciar entre la vigilancia de las denominadas fuentes abiertas (OSINT), de la que puede realizarse en las conocidas como fuentes cerradas³⁴⁴. Respecto de las primeras, se trata de fuentes disponibles, de fácil acceso, en las que se puede obtener información de los datos proporcionados por Administraciones públicas, empresas, redes sociales, etc. Si bien en la actualidad se vincula este sistema a las nuevas tecnologías, no quiere decir, que anteriormente no fuera utilizado. Las fuentes como periódicos, revistas, radio y televisión, fueron, en otros años, las vías en las que se obtenía material que podía resultar útil en la investigación delic-

341 Referencia obligada en este punto es la relativa a la base de datos SIGO (Sistema Integrado de Gestión Operativa, Análisis y Seguridad Ciudadana), en la que se archiva información relacionada con sujetos que pueden considerarse sospechosos, y que proviene de grabaciones realizadas con videocámaras instaladas en lugares públicos por la policía, o por cámaras de tráfico, imágenes captadas por esas cámaras o drones, e información obtenida de la red. La Agencia Española de Protección de Datos resolvió se pronunció favorablemente a la existencia de sistema y su finalidad.

342 Sobre esta forma de vigilancia en redes v. GONZÁLEZ LÓPEZ, J.J., «La interacción automatizada por medio de simuladores como medida de investigación penal» en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, número 41, 2016.

343 BUENO DE MATA, F., *Investigación y prueba de delitos de odio en Redes Sociales: Técnicas OSINT e inteligencia policial*, Tirant lo Blanch, Valencia, 2023, págs. 174 y ss.

344 V. más ampliamente, BUENO DE MATA, F., *Investigación y prueba de delitos de odio en Redes Sociales*, op. cit., pág. 68.

tiva. A estas fuentes clásicas se unen, en la actualidad, otras más avanzadas, que muestran un perfil muy preciso de los sujetos que lo facilitan a través de sus datos. En estos casos los contenidos que se muestran en la red se encuentran indexados en motores de búsqueda.

No obstante, en este punto es conveniente precisar que los datos sobre los que trabajan los sistemas inteligentes son proporcionados por los sujetos que acceden a la red, por lo que, en muchas ocasiones no son datos reales, sino manipulados o falseados, con el fin de enmascarar su verdadera identidad. Dentro de esta técnica de investigación en fuentes abiertas, se puede integrar la denominada SOCMINT, que se centra en la obtención de datos que se encuentran expuestos al público en redes sociales, como Facebook, Twitter, Instagram, YouTube...

Por el contrario, las fuentes cerradas no son de acceso público, su acceso es limitado a través de una contraseña de la que se vale el usuario. Su contenido no está indexado, por lo que su acceso es restringido. No quiere decirse que no se pueda acceder a esta clase de fuentes, sino que para su acceso es preciso disponer de una contraseña o clave que se facilita al usuario. Esta distinción entre dos tipos de canales o fuentes, es importante desde la perspectiva de la investigación policial, porque en la primera, el canal abierto, no es necesaria la autorización judicial para su monitorización, mientras que, en la segunda, canal cerrado, sí que ha de partirse de la autorización judicial en el marco de un proceso penal. Finalmente, ha de hacerse alusión a la denominada red oscura, en la que se persigue el anonimato, poniendo barreras a la investigación policial. Se trata de una red utilizada por los cibercriminales en los delitos que se comenten principalmente en la red.

Internet es una «*red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación*»³⁴⁵. Esta red utiliza un lenguaje en común para la comunicación entre los dispositivos. Se vale de protocolos y servicios, y opera a través de diferentes tipos de conexiones (línea telefónica, un cable o 4G y 5G, fibra óptica o ADSL). A través de ella se intercambia información, que se transmite a través de protocolos que permiten crear una red única capaz de transmitir entre los dispositivos. De igual forma, se ofrecen servicios (correo electrónico, chats, redes sociales y web,) que permiten a los usuarios crear, enviar, recibir y acceder a la información. Es indudable que el acceso a Internet ha cambiado no sólo la forma de comunicarse, sino también de relacionarse, de acceder al comercio, a la educación, al trabajo, a las relaciones económicas y empresariales, al ocio, y en general a todas las actividades que los ciudadanos pueden desarrollar.

Se trata de un fenómeno global que se ha convertido en una herramienta esencial de la sociedad. Por tanto, el acceso a esta red global resulta de tanta

345 Diccionario de la Lengua Española

importancia al extender su aplicación a todos los ámbitos de la vida de los ciudadanos. Esta capacidad de interactuar a todos los niveles que proporciona Internet, ha propiciado que el acceso a la red se convierta en un derecho de los ciudadanos. De esta forma, se regula en el artículo 81 de la LO 3/2018, de 5 de diciembre, el derecho de acceso universal a Internet³⁴⁶.

A través del acceso a la red se pueden desplegar otros derechos que tienen entidad propia y que pueden ejercerse tanto fuera de la red, como en ella. Pero al mismo tiempo, que permite el desarrollo de la personalidad de los ciudadanos y de sus relaciones y derechos, también puede convertirse en un vehículo adecuado para el desarrollo de nuevas formas de criminalidad.

En este fin constante de lucha contra la criminalidad, los Fuerzas y Cuerpos de la Seguridad del Estado, utilizan también el rastreo y la monitorización de las redes con la finalidad de detectar conductas delictivas. Una vez más, y ante la falta de una regulación legal precisa sobre este tipo de actuaciones relacionadas con la prevención delictiva³⁴⁷, es preciso buscar el equilibrio entre las funciones policiales y el respeto a los derechos y libertades de los ciudadanos.

Se ha defendido jurisprudencialmente, sobre todo en resoluciones anteriores a la regulación de la Ley 13/2015, de modificación de la Ley de Enjuiciamiento Criminal respecto de las medidas de investigación tecnológica, que, el que ponía a disposición del público sus datos personales, hacía decaer, por propia iniciativa, la protección de ese espacio reservado que constituye la vida privada. En este sentido se ha pronunciado el Tribunal Supremo al considerar que «...los rastreos que realiza el equipo de delitos telemáticos de la Guardia Civil en Internet tienen por objeto desenmascarar la identidad críptica de los IPS (Internet protocols) que habían accedido a los "hash" que contenían pornografía infantil. El acceso a dicha información, calificada de ilegítima o irregular, puede efectuarla cualquier usuario. No se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma. La huella de la entrada —como puntualiza con razón el M.^o Fiscal— queda registrada siempre y ello lo sabe el usuario»³⁴⁸. De esta forma, cada usuario de la red va a configurar el alcance de ese espacio reservado de protección, que constituye el derecho al entorno virtual.

No obstante, este espacio reservado también se ha vinculado por el Tribunal Constitucional, con el contenido del derecho a la intimidad, afirmando

346 Sobre los antecedentes de esta regulación v. BUENO DE MATA, F., *Investigación y prueba de delitos de odio...*, op. cit., págs. 74 y ss.

347 MARTÍN RIOS, P., «Empleo de big data y de inteligencia artificial en el ciberpatrullaje: de la tiranía del algoritmo y otras zonas oscuras» en *Revista de los Estudios de Derecho y Ciencia Política*, número 36, octubre 2022, <https://idus.us.es/>, pág. 4.

348 SSTs 236/2008, de 9 de mayo; 292/2008, de 28 de mayo, entre otras.

que la protección del artículo 18.1 CE se proyecta sobre la esfera personal del individuo y excluye que los terceros, tanto particulares como públicos, puedan delimitar el alcance de la vida privada de los ciudadanos³⁴⁹. Así, la «*esfera de la intimidad personal está en relación con la acotación que de la misma realice su titular, habiendo reiterado este Tribunal que cada persona puede reservarse un espacio resguardado de la curiosidad ajena*»; en consecuencia «*corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno*»³⁵⁰.

En este aspecto, es necesario matizar, que es habitual que el usuario de Internet deje rastro de sus intercomunicaciones y acceso, y además proporcione información sobre su vida privada, y no tan privada, de forma involuntaria. Es decir, sin ser consciente que realmente está dejando un rastro accesible a terceros. Así se pone de relieve por el propio Tribunal Supremo en una sentencia posterior a la reforma introducida por la Ley 13/2015. Reconoce el Tribunal el derecho al entorno virtual, integrándose en su contenido los derechos fundamentales recogidos en el artículo 18 CE, y que tendría como base la «*...información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital*»³⁵¹.

Lo cierto es que la información proporcionada, voluntaria o involuntariamente, facilita un nutrido número de datos que configuran un perfil del sujeto³⁵². Datos que provienen en primer lugar de su identificación y localización, de sus opiniones, de su imagen y, a través de su visionado, de los lugares que frecuenta, de las cuentas que visita y con cuales se muestra conforme, del nivel cultural y de sus aficiones, de los gustos que comparte³⁵³.

Por todo ello, y partiendo de la grave injerencia que el rastreo de la red causa en los derechos fundamentales relacionados con la vida privada de las personas, no puede mantenerse una posición ambigua o confusa, o incluso permisiva o flexible con este tipo de actuaciones. Lo más conveniente sería

349 SSTC 159/2009, de 29 de junio; 185/2002, de 14 de octubre; 93/2013, de 23 de abril.

350 STC 241/2012, de 17 de diciembre, entre otras.

351 STS 342/2013, de 17 de abril). V. también la STS 786/2015, de 4 de diciembre.

352 Sobre la elaboración de perfiles v. el considerando 31 REIA, su artículo 6 que remite al anexo III en cuyas letras d) y e) se hace referencia a la utilización de sistemas de IA destinados a la elaboración de perfiles; el artículo 3.4 y el artículo 11 de la Directiva (UE) 2016/680; artículo 14 LO 7/2021.

353 V. más ampliamente, BUENO DE MATA, F., Investigación y prueba de delitos de odio..., *op. cit.*, págs. 97 y ss.

desarrollar una regulación específica sobre los supuestos en los que la policía podría llevar a cabo funciones de monitorización, y los requisitos a observar. Téngase en cuenta que las actuaciones a prevención, objeto de estas consideraciones, pueden llevarse a cabo sin que realmente se haya cometido ningún hecho delictivo, actuando como consecuencia de hechos pasados, o conductas consideradas como peligrosas.

En relación con el acceso a Internet, y la propia configuración de un espacio de privacidad por los usuarios, es preciso diferenciar entre los datos accesibles y los datos abiertos. Respecto de los primeros, datos accesibles, se podrá acceder a través de una autorización específica derivada del pago de una cuota, o de la pertenencia a una institución o sociedad que permite el acceso a sus afiliados previo cumplimiento de determinadas condiciones. En el caso de los datos abiertos, como su propia denominación indica, se puede acceder libremente a ellos, sin restricciones ni técnicas ni legales. Relacionada con la distinción anterior, se encuentra la diferencia entre canal virtual abierto, disponible públicamente sin autorización especial (blogs, páginas web públicas, foros de debate...), y canal virtual cerrado, sólo disponible para usuarios autorizados expresamente (chats privados, grupos conectados en red privados...).

La posición jurisprudencial del Tribunal Constitucional, respecto de la protección de las comunicaciones a través de la red, se centra en considerar que el artículo 18.3 CE «...*protege únicamente ciertas comunicaciones: las que se realizan a través de determinados medios o canales cerrados*»³⁵⁴. Así se ha pronunciado en resoluciones anteriores, afirmando que no se encuentran protegidas constitucionalmente aquellas comunicaciones que los propios usuarios no consideran secretas, al formalizarlas por canales abiertos, de los que no se puede predicar la confidencialidad³⁵⁵.

En el mismo sentido, haciéndose eco de la STC 170/2013, de 7 de octubre, se ha posicionado la Fiscalía General del Estado, al afirmar que «...*no toda comunicación resulta acreedora de la protección constitucional, que solo alcanzará a aquellas que se transmitan a través de canales cerrados, esto es, las comunicaciones que puedan considerarse secretas* (STC n.º 170/2013, de 7 de noviembre) y, en el caso de las generadas por medio de dispositivos técnicos de seguimiento y localización, la comunicación se transmite a través de canales abiertos»³⁵⁶. En este supuesto, por tanto, no sería necesaria la autorización judicial previa para acceder a las comunicaciones y opiniones que el sujeto comparte en ese canal abierto. Sin embargo, cuando el ciudadano quiere proteger su espacio reservado de la vida privada, acotando los derechos desplegados en la red, y que se desarrollan en el espacio virtual, la

354 V. por todas la STC 170/2013 de 7 de octubre.

355 SSTC 281/2006, de 9 de octubre, o 241/2012, de 17 de diciembre.

356 CFGE 4/2019, de 19 de mayo.

necesidad de una autorización judicial previa para el acceso a los contenidos se convierte en indiscutible. Se trataría de una limitación por parte de la policía del derecho al entorno virtual, que como derecho fundamental en el que se desarrollan otros derechos con entidad propia como el derecho a la intimidad o el derecho al secreto de las comunicaciones, requiere una autorización judicial, adoptada en el seno de un proceso penal y con observancia del principio de proporcionalidad entendido en sentido amplio³⁵⁷.

El análisis por la policía de las comunicaciones desarrolladas en las redes sociales y canales abiertos, que se agrupa bajo la denominación de ciberpatrullaje, puede tener lugar con carácter previo a la incoación del proceso penal, e incluso a la comisión de hechos delictivos, al integrarse en las funciones de prevención de las actuaciones criminales, utilizándose también con fines predictivos.

Con la finalidad de detectar actuaciones delictivas los agentes policiales utilizan técnicas relacionadas con la inteligencia artificial. Para ello, ese rastreo y monitorización de la red, pretende la obtención de información y su análisis con dos finalidades principales: detectar la comisión de ilícitos penales, y evaluar los riesgos de actuaciones criminales. Se desarrollan al margen del proceso penal y, como ya se ha apuntado, no necesitan autorización judicial³⁵⁸. A estas dos finalidades propias del ciberpatrullaje, ha de añadirse una más, consecuencia de su puesta en funcionamiento, como es el descubrimiento de delitos flagrantes cometidos en la red, que obviamente puede derivarse directamente del análisis de los contenidos rastreados.

Esta técnica de vigilancia policial no tiene cabida en un precepto específico de la Ley procesal penal, aunque se puede integrar en las funciones policiales generales reguladas su artículo 282. Sin embargo, tampoco resulta imprescindible su incorporación a la norma procesal porque, en su función preventiva, se desarrolla con carácter previo a la incoación del proceso. Cuestión diferente es el análisis de los datos obtenidos como consecuencia del Registro de dispositivos de almacenamiento masivo de información, que se regula en los artículos 588 sexies y siguientes, o el registro remoto de dispositivos informáticos de los artículos 588 septies y ss. LECrim.

Esta actividad de vigilancia policial con fines de prevención puede encuadrarse en el artículo 11 LO 2/1986, de 13 de marzo, reguladora de las Fuerzas y Cuerpos de Seguridad, en el que les encomienda la protección del libre ejercicio de derechos y libertades, garantizando la seguridad ciudadana. Dicha misión se concreta en una serie de funciones (mantener el orden y la seguridad ciudadana, prevenir la comisión de actos delictivos), en las que se

357 V. más ampliamente BUENO DE MATA, F., *Investigación y prueba de delitos de odio...*, op. cit., págs. 144 y ss.

358 MARTÍN RÍOS, P., «Empleo de big data y de inteligencia artificial en el ciberpatrullaje...», op. cit., pág. 3

podían integrar el ciberpatrullaje, y las técnicas relacionadas con la inteligencia artificial al servicio de la prevención de actuaciones criminales. Además de estas funciones generales, el precepto incluye la de «*Investigar los delitos para descubrir y detener a los presuntos culpables, asegurar los instrumentos, efectos y pruebas del delito, poniéndolos a disposición del Juez o Tribunal competente y elaborar los informes técnicos y periciales procedentes*», que obviamente podría incluir este tipo de técnicas con las que se pretende la elaboración de informes que puedan llevar a poner en marcha estrategias de prevención delictiva. Y una más concreta recogida en la letra h), «*Captar, recibir y analizar cuantos datos tengan interés para el orden y la seguridad pública, y estudiar, planificar y ejecutar los métodos y técnicas de prevención de la delincuencia*», en la que claramente se podrían incluir estas técnicas de análisis de datos obtenidos del rastreo en la red³⁵⁹.

359 BUENO DE MATA, F., *Investigación y prueba de delitos de odio...*, op. cit., pág. 172.

CAPÍTULO IV

LA EFICACIA DE LA INVESTIGACIÓN POLICIAL CON INTELIGENCIA ARTIFICIAL EN EL PROCESO PENAL. PROPORCIONALIDAD Y CONTROL JUDICIAL

1. Introducción

En el capítulo anterior ya se ha indicado que el estudio de las garantías que han de presidir las diligencias de investigación relacionadas con la inteligencia artificial, se centraría, fundamentalmente, en aquellas que se desarrollan por las Fuerzas y Cuerpos de la Seguridad del Estado con anterioridad a la incoación del proceso penal, si bien, en algunos puntos, se ha considerado conveniente acudir a la regulación que la Ley de Enjuiciamiento Criminal desarrolla respecto de las diligencias de investigación tecnológicas, acordadas en la fase de instrucción, al considerarlas como normas de referencia en la investigación penal. Y ello obedece a que los presupuestos y requisitos que se exigen para la adopción de las medidas instructoras que restringen derechos fundamentales, deberían aplicarse también en las diligencias preprocesales, principalmente cuando puedan afectar a sujetos determinados que desarrollan su actividad en localizaciones físicas o virtuales vigiladas por la policía.

De esta forma, resulta obligado hacer referencia al principio de proporcionalidad y al control judicial como presupuestos determinantes de la posible eficacia que este tipo de diligencias puedan desarrollar en un futuro proceso. El legislador de 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, ha optado por

la incorporación a este cuerpo de legal de unos principios cuyo contenido ya había sido desarrollado por la jurisprudencia constitucional y por el Tribunal Supremo. Las aportaciones jurisprudenciales y doctrinales³⁶⁰, en las que se han sentado las bases sobre los principios generales y el régimen jurídico de las medidas de investigación tecnológica, han proporcionado al legislador los mimbres necesarios para abordar la regulación que se ha llevado a cabo³⁶¹.

Es precisamente esta doctrina jurisprudencial la que ha venido reclamando desde años atrás³⁶², la necesaria previsión legislativa que resulte «asequible» para el ciudadano y proporcione la información necesaria sobre las normas aplicables al caso concreto³⁶³. En este sentido, resulta importante reclamar ahora, que los requisitos a observar en las medidas de investigación preprocesales realizadas por la policía con sistemas de inteligencia artificial en el curso de una investigación a prevención, estén definidos y previstos con claridad en una norma legal. Para ello, no es suficiente con una previsión

360 En este sentido se han pronunciado autores como ASENCIO MELLADO, J.M^a, *Prueba prohibida y prueba preconstituida*, Editorial Trivium, Madrid, 1989, pág. 105; GONZÁLEZ-CUELLAR SERRANO, N., *Proporcionalidad y derechos fundamentales en el proceso penal*, Colex, Madrid, 1990, pág. 92; JIMENEZ CAMPO, J., «La garantía constitucional del secreto de las comunicaciones», en *REDC*, número 20, 1987, pág. 37; LÓPEZ-BARJA DE QUIROGA, J., *Escuchas telefónicas y prueba ilegalmente obtenida*, Akal, Madrid, 1989, pág. 163 a 165; LÓPEZ-FRAGOSO ÁLVAREZ, T., *Las intervenciones telefónicas en el proceso penal*, Madrid, Colex, 1991, pág. 32; MARTÍN MORALES, R., *El régimen constitucional del secreto de las comunicaciones*, Civitas, Madrid, 1995, pág. 102; MONTERO AROCA, J., *La intervención de las comunicaciones en el proceso penal. Estudio jurisprudencial*, Tirant lo Blanch, Valencia, 1999, pág. 75; MONTÓN REDONDO, A., «Las intervenciones telefónicas constitucionalmente correctas», en *Revista Jurídica La Ley*, número 3915, 1995, pág. 1. MORENO CATENA, V., «Garantía de los derechos fundamentales en la investigación penal», *Poder Judicial*, número especial II, 1987, pág. 157; RODRÍGUEZ RAMOS, L., «Intervenciones telefónicas», en *La prueba en el proceso penal. Cuadernos de Derecho Judicial*, CGPJ, Madrid, 1992, pág. 453, entre otros muchos.

361 MARCHENA GÓMEZ, M./GONZÁLEZ-CUELLAR SERRANO, N., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Castillo de Luna, ediciones jurídicas, Madrid, 2015, pág. 213.

362 V. SSTC 62/1982, de 15 de octubre; 37/1989, de 15 de febrero; Auto del Tribunal Supremo de 18 de junio de 1992, sobre el caso Naseiro. V también las SSTEDH de 26 de abril de 1979, Caso Sunday Times; 25 de marzo de 1983, Caso Silver; 30 de julio de 1998, Caso Valenzuela Contreras, entre otros.

363 Así, hay que hacer referencia al art. 8.2 CEDH que exige el cumplimiento de determinados requisitos para la adopción de cualquier medida que implique la restricción de los derechos relacionados con la vida privada. Concretamente, dispone que no podrá haber injerencia alguna en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté, prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.
V. SSTEDH de 6 de septiembre de 1978, caso Klass y otros; de 25 de marzo de 1983; caso Silver y otros; de 27 de octubre de 1983, caso Malone; de 18 febrero de 2003, Caso Prado Bugallo; de 31 mayo 2005, Caso Vetter; de 1 julio 2008, caso Liberty y otros.

general sobre su posible ejecución³⁶⁴, sino que la ley deberá regular el ámbito de actuación policial, los casos en los que es posible su puesta en marcha, y los requisitos que se han de cumplir para garantizar el respeto a los derechos fundamentales afectados. Todo ello teniendo en cuenta que de dichas diligencias pueden derivarse datos importantes para una investigación delictiva, cuya utilidad resultaría relevante en una futura instrucción.

A título de ejemplo, cabe señalar la insuficiente regulación de la LO 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. En su artículo 13, recoge el tratamiento de datos personales especialmente sensibles³⁶⁵, pero no concreta en absoluto en qué situaciones se puede proceder al tratamiento de esos datos. Sólo condiciona su autorización a que «...sea estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado...» y siempre que se cumplan alguna de las circunstancias recogidas en el propio precepto. Teniendo en cuenta el objeto de la ley, y que se trata de una ley de desarrollo de una Directiva³⁶⁶, debería precisar qué tipo de situaciones pueden justificar las actuaciones policiales de tratamiento de datos y las garantías a observar.

A estas precisiones se refiere el Tribunal Europeo de Derechos Humanos cuando exige la calidad de la ley que desarrolle medidas limitativas de derechos fundamentales. En este sentido considera que *«...con las palabras «prevista por la ley» se pretende, en primer lugar, que la medida impugnada tenga una base en el Derecho interno. Ahora bien, esta expresión no se limita a remitir al Derecho interno, sino que también hace referencia a la calidad de la «ley», exigiendo que la medida sea compatible con la preeminencia del derecho, implicando, por tanto, que el Derecho interno debe ofrecer una cierta protección contra los atentados arbitrarios de los poderes públicos a los derechos garantizados en el párrafo 1 (Sentencia Malone antes citada, pág. 32, §67). De esta exigencia deriva la necesidad de la accesibilidad de la*

364 Esta era también la deficiente regulación que el viejo artículo 579 LECrim, abordaba respecto de la medida de intervención telefónica, y que, hasta la reforma de 2015, fue objeto de tantas críticas por parte del TEDH, del Tribunal Constitucional y del Tribunal Supremo.

365 Datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, los datos relativos a la salud o a la vida sexual o a la orientación sexual de una persona física,

366 Directiva (Ue) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

ley para la persona afectada, quien, además, debe poder prever las consecuencias para ella de dicha ley (Sentencias Kruslin antes citada, pág. 20, §27, y Kopp antes citada, pág. 540, §55)»³⁶⁷.

Como resulta obvio, cuando las actuaciones policiales de las que deriva el tratamiento de los datos personales, se vinculan a su utilización con fines de prevención o de investigación en el proceso penal, las precauciones y caute- las han de ser más estrictas, para dar protección no sólo a los derechos rela- cionados con la vida privada de los ciudadanos, sino también a todo el con- junto de derechos de naturaleza procesal que se constituyen en los pilares del proceso de un Estado de Derecho. Su tratamiento ha de ser ampliamente regulado, estableciendo un protocolo donde la transparencia y la accesibili- dad se respeten a lo largo de todo el procedimiento.

Lo que parece indudable, es que, aún en aquellos casos en los que se puede admitir la práctica por los agentes policiales de diligencias de investigación desarrolladas al margen del proceso penal, y, por tanto, realizadas sin control judicial, lo que ha de defenderse es que, en tales ocasiones, la policía tenga en cuenta si existe una previsión que ampare, aunque sea de forma general, su actuación, y que su ejecución se lleve a cabo bajo el paraguas del princi- pio de proporcionalidad³⁶⁸. Uno y otro requisito van a resultar determinantes cuando se pretenda la eficacia de estas diligencias en el futuro proceso penal y se intente validar el resultado bajo el control judicial.

Sobre esta cuestión ya se había pronunciado el Tribunal Constitucional, con anterioridad a la reforma de la Ley de Enjuiciamiento Criminal en 2015, considerando como requisitos a tener en cuenta para la válida actuación policial al margen del control judicial que concurren las condiciones: «a) la existencia de un fin constitucionalmente legítimo, considerando como tal el interés público propio de la prevención e investigación del delito, y, más en concreto, la determinación de hechos relevantes para el proceso penal; b) que la medida limitativa del derecho a la intimidad esté prevista en la ley (principio de legalidad); c) que, en caso de no contar con autorización judicial (o consentimiento del afectado), la actuación policial se atenga a la habilitación legal, teniendo en cuenta que la ley puede autorizar a la policía la prác- tica de inspecciones, reconocimientos e incluso intervenciones corporales leves, siempre y cuando se respete el principio de proporcionalidad, concre- tado en tres exigencias o condiciones: idoneidad de la medida, necesidad de la misma y juicio de proporcionalidad en sentido estricto»³⁶⁹. Y, en relación

367 STEDH 30 de julio de 1998, Caso Valenzuela Contreras. V.también, SSTEDH de 2 de agosto de 1984, Caso Malone contra el Reino Unido; 24 de abril de 1990, Caso Kruslin c. Francia, o en la misma fecha Caso Huvig contra Francia; 25 de marzo de 1998, caso Kopp contra Suiza, entre otras.

368 GARCÍA MARCOS, J., «Hacia una exclusiva reserva jurisdiccional en la protección del derecho a la intimidad» (1), en *Actualidad Civil*, Número 4, abril 2024.

369 STC 115/2013, de 9 de mayo.

con la exigencia de previsión legal, el alto Tribunal, en la misma resolución, admite la legitimidad constitucional de la injerencia de carácter leve en el derecho a la intimidad, sin autorización judicial ni consentimiento del afectado «...con la suficiente y precisa habilitación legal»³⁷⁰.

En el mismo sentido, se pronuncia el Consejo de Estado, en su informe al proyecto de LO 7/2021, cuando señala que «...debe aclararse la determinación del conjunto normativo aplicable a la utilización por las Fuerzas y Cuerpos de Seguridad, así como por los demás órganos competentes, de cámaras y videocámaras para la grabación de imágenes y sonidos en lugares públicos en función de los usos y fines específicos»³⁷¹.

Así pues, es clara la postura sobre la necesidad de una Ley en la que se recojan las garantías de las actuaciones policiales de investigación a prevención, y el procedimiento a observar cuando sus resultados hayan de introducirse en un proceso penal. Es evidente que hasta ese momento pueden aplicarse los presupuestos y requisitos previstos en la LO 13/2015, de modificación de la Ley procesal penal, en cuanto que recoge los principios rectores y el control judicial aplicable a las medidas de investigación tecnológica, que, en otra fase de la investigación policial, en la que se desarrolla bajo el paraguas del proceso penal, es exigible para dichas actuaciones. De esta forma, cabe precisar que la citada Ley 13/2015, ha supuesto un gran avance en la regulación de estas medidas que están estrechamente relacionadas con los sistemas e instrumentos de inteligencia artificial, al abordarse un régimen jurídico completo en el que se determinan principios, garantías, procedimiento... Además, el desarrollo de la Ley por el legislador se hace de tal forma, que puede afrontar futuras incorporaciones de nuevos instrumentos, al ser una norma flexible dentro de la precisión³⁷².

Al hacer referencia a las garantías que han de reunir las diligencias de investigación policial en la que se utilicen técnicas de inteligencia artificial, lo primero que cabe apuntar es que la Ley 13/2015, de modificación de la Ley procesal penal, ya regula un régimen jurídico perfectamente diseñado, aunque siempre caben mejoras, en el que se establecen los requisitos y garantías para la utilización de los instrumentos relacionados con las nuevas tecnologías. No obstante, este régimen jurídico está pensado, como es obvio, para aquellas diligencias que se ejecutan en el seno del proceso penal, esto es, una vez iniciada la instrucción.

370 V. SSTC 70/2002, de 3 de abril; 123/2002, de 20 de mayo; 56/2003, de 24 de marzo; 281/2006, de 9 de octubre; 142/2012, de 2 de julio, entre otras.

371 Dictamen del Consejo de Estado 675/2020, de 28 de enero de 2021, relativo al Anteproyecto de Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación o enjuiciamiento de infracciones penales y de ejecución de sanciones penales. <https://www.boe.es/buscar/doc.php?id=CE-D-2021-213>

372 BUENO DE MATA, F., *Investigación y prueba de delitos de odio...*, op. cit., pág. 130.

Lo importante, ahora, es determinar el procedimiento a seguir cuando estas nuevas técnicas de investigación se llevan a cabo al margen del proceso penal, pero su resultado pretende introducirse posteriormente en un proceso penal ya iniciado.

Lo más conveniente, será tomar como referencia los principios rectores de las medidas de investigación tecnológica para que, en la medida de lo posible, puedan ser respetados por los agentes policiales en sus diligencias a prevención. No es posible, por razones evidentes, aplicar la necesaria resolución judicial autorizante de estas medidas, dado que estamos tratando diligencias policiales preprocesales, pero sí se ha de analizar la aplicación del principio de proporcionalidad, y el control judicial posterior cuando se pretenda hacer uso del resultado en el proceso penal.

2. El principio de proporcionalidad

2.1. Consideraciones previas

Aunque la Constitución española no regula expresamente el principio de proporcionalidad, su rango constitucional se deduce de varios de sus preceptos. El sistema de valores recogidos constitucionalmente, consagra la libertad y seguridad como pilares fundamentales del Estado de Derecho, y como fundamento del orden político y de la paz social. En este sentido, la libertad dota de contenido al principio de proporcionalidad, favoreciendo la efectividad de los derechos fundamentales³⁷³. También el artículo 9 CE, fundamenta su engarce constitucional, al prohibir la arbitrariedad de los poderes públicos en sus actuaciones. Finalmente, el artículo 10 CE proporciona dos referencias importantes, de un lado, al regular constitucionalmente la dignidad humana, y de otro, al residenciar en los tratados y convenios internacionales la interpretación de las normas relativas a los derechos fundamentales.

El principio de proporcionalidad ha sido objeto de desarrollo doctrinal, llegando a establecerse su contenido que cabe desdoblar en tres subprincipios, recogidos en la Ley 13/2015, como principios rectores. La idoneidad, la necesidad y la proporcionalidad en sentido estricto forman parte de su contenido esencial, y por tanto su observancia es de estricto cumplimiento en la adopción de medidas limitativas de derechos fundamentales³⁷⁴.

373 V. en este sentido GONZÁLEZ-CUELLAR SERRANO, N., *Proporcionalidad y derechos fundamentales...*, op. cit., pág. 54; PECES BARBA MARTÍNEZ, G., *Los valores superiores*, Tecnos, Madrid, 1986, pág. 13. V. también STC 65/1986, de 22 de mayo.

374 V. por todos, GONZÁLEZ-CUELLAR SERRANO, N., *Proporcionalidad y derechos fundamentales...*, op. cit., pág. 69 Y 153; LÓPEZ-FRAGOSO ÁLVAREZ, T., *Las intervenciones telefónicas...*, op. cit., pág. 40; PEDRAZ PENALVA, E., «El principio de proporcionalidad y su configuración en la jurisprudencia del Tribunal Constitucional y literatura especializada alemana», *Poder Judicial*, número 17, 1990, pág. 343.

2.1.1. Principio de idoneidad

La idoneidad supone que el examen previo de la investigación y de los hechos que la integran, determina que la medida elegida es la más adecuada para conseguir el fin perseguido. Así, la medida debe ser por su naturaleza la más apta para la consecución del fin previsto, y además, la fijación de su duración ha de estar en estrecha relación con su finalidad. Cuando las medidas previstas por la policía se adoptan en el curso de un proceso penal, la idoneidad de la medida ha de estar vinculada a la investigación de un sujeto concreto y respecto de los hechos delictivos objeto de la instrucción. Sin embargo, estos criterios no pueden aplicarse en la investigación a prevención. En estos casos, las actuaciones policiales no se proyectan sobre sujetos determinados, sino que se llevan a cabo con carácter general con la finalidad de detectar la posible comisión de actuaciones criminales. Lo que tendrá que valorar la policía es si la aplicación de los instrumentos y medidas elegidas, va a resultar la más adecuada para el fin que se persigue. Para ello, tendrá en cuenta la naturaleza de los posibles hechos delictivos a los que van dirigidos las medidas, las características físicas, ambientales y sociales de su posible localización y todas las circunstancias que ayuden a determinar que la medida elegida es la más idónea respecto del resultado pretendido.

2.1.2. Principio de necesidad

La necesidad conlleva, que, de todas la medidas idóneas o aptas para la finalidad perseguida, se debe elegir aquella que cause una menor lesión en los posibles sujetos que puedan verse afectados. Si el resultado puede obtenerse a través de otra medida que implique una restricción menor de los derechos fundamentales, no estaría constitucionalmente justificada la adopción de medidas más invasivas. Obviamente, y a título de ejemplo, no es lo mismo colocar cámaras fijas de videovigilancia en lugares públicos muy concurridos por hallarse situados cerca de centros comerciales, o en lugares de ocio, que aquellas que se pueden instalar también en lugares públicos, pero de barrios pequeños, en los que los vecinos son los usuarios más habituales. En estos casos puede llegar a determinarse qué sujetos suelen acudir a esas localizaciones, por lo que ha de extremarse el juicio de proporcionalidad de la medida. También el uso de cámaras móviles puede llegar a convertirse en una vigilancia específica de sujetos determinados. Debe valorarse que la intromisión sea esencial para conseguir el fin perseguido, frustrándose dicha finalidad de no adoptarse la medida.

La jurisprudencia se ha pronunciado sobre la aplicación del principio de proporcionalidad en relación a la necesidad de las medidas limitativas de derechos fundamentales en el marco del proceso penal, llegando a crearse, como se ha apuntado al inicio de este capítulo, una doctrina jurisprudencial que ha servido de base a la regulación legal. El Tribunal Supremo ha afirmado

en este sentido que «*la resolución autorizando la escucha de las conversaciones telefónicas de una persona tiene que concederse con carácter excepcional y siempre que no exista otro medio de investigación menor incisivo que permita el desenvolvimiento de la actividad judicial sin interferir y dañar derechos y libertades fundamentales...*»³⁷⁵.

2.1.3. Proporcionalidad en sentido estricto

Finalmente, conforme a la proporcionalidad en sentido estricto, el órgano jurisdiccional, o en su caso, la policía, ha de valorar la idoneidad y la necesidad, ponderando los intereses en conflicto, esto es, si la seguridad y la investigación delictiva que se pretende, justifican el sacrificio de derechos fundamentales. En este aspecto juega un importante papel la gravedad de los hechos que se pretenden evitar, al igual que el número de personas o su especial condición, que pueden ser víctimas de los mismos. En el caso de la investigación preprocesal, este examen previo por parte de los agentes policiales, será después supervisado por el juzgador, en su función de control judicial de las actuaciones. De esta forma, habrá que resolver si el interés estatal en la prevención delictiva justifica la posible vulneración de los derechos fundamentales, o si, por el contrario, el sacrificio resulta excesivo, por lo que no puede validarse la ejecución de la diligencia. Por tanto, el peso, o la ponderación de los intereses enfrentados resulta decisivo para su ratificación. En dicha ponderación es importante valorar también la incidencia de la medida en los derechos fundamentales de todos los sujetos que se pueden ver afectados³⁷⁶.

La importancia de esta operación, adquiere mayor relevancia en estos casos de investigación a prevención, en los que, como ocurría en el ordenamiento jurídico anterior a la reforma de la Ley 13/2015, los presupuestos y requisitos de la limitación no estaban establecidos en una norma legal, resultando por tanto imprescindible realizar la citada ponderación en cada supuesto concreto con un análisis claro y preciso de los intereses en juego. Así, podrían establecerse ciertos criterios de referencia para la defensa del interés estatal, como son las consecuencias jurídicas del hecho delictivo y el número posible de víctimas, la importancia del bien jurídico que se intenta proteger³⁷⁷, los indicios policiales sobre actuaciones criminales ligadas a una

375 STS de 25 de junio de 1993. V. también SSTC 62/1982, de 15 de octubre. SSTs de 18 de junio de 1993, 25 de junio de 1993, 18 de abril de 1994, 27 de septiembre de 1994, 4 de noviembre de 1994, 12 de enero de 1995, 20 de enero de 1995, 22 de enero de 1996, 11 de marzo de 1996, 15 de marzo de 1996, 12 de abril de 1996, 24 de junio de 1996, 18 de julio de 1996, 29 de julio de 1996, 8 de julio de 1997, 14 de febrero de 1998 y 23 de febrero de 1998.

376 V. STC 37/1989, de 15 de febrero.

377 GONZÁLEZ-CUELLAR SERRANO, N., *Proporcionalidad y derechos fundamentales...*, op. cit., pág. 252 y ss.

ubicación, o a la utilización de redes determinadas para hechos delictivos vinculados a la ciberdelincuencia³⁷⁸.

Es importante destacar la jurisprudencia del Tribunal Constitucional relativa a los datos a tener en cuenta para realizar la ponderación que exige la proporcionalidad. Si bien el Tribunal se pronuncia sobre la medida de intervención telefónica, y el análisis de la proporcionalidad por el juez de instrucción, su doctrina puede aplicarse también al juicio que han de realizar las autoridades policiales. Afirma el Tribunal, que para la correcta aplicación del principio de proporcionalidad el juez, y también la policía en este caso, ha de tener en cuenta todos los datos que concurren en el supuesto de que se trate, tanto los intereses estatales como los individuales, considerando a este respecto que *«la apreciación de la necesidad de limitación de un derecho fundamental y el cálculo consiguiente de la proporcionalidad de la medida adoptada no pudieron ser enunciados en la mente del juez a falta de un examen, ni siquiera mínimo, del objeto sobre el que recayó su prohibición, que constituye así una ablación del derecho a comunicar y a recibir información del artículo 20.1.d) de la Constitución, así como un acto contrario al principio general de interdicción de la arbitrariedad (art. 9.3)»*³⁷⁹.

2.2. El principio de proporcionalidad en la LO 13/2015, de modificación de la Ley de Enjuiciamiento Criminal

La importancia del principio de proporcionalidad, como garante de la adopción de las medidas de investigación tecnológicas, en las que se pueden integrar los sistemas de inteligencia artificial, se reconoce por el legislador de la Ley 13/2015, al regularlo en las disposiciones comunes a las medidas de interceptación de comunicaciones, considerándolo además como principio rector de su régimen jurídico. Así, en el artículo 588 bis a) LECrim, condiciona su adopción a la existencia de una previa instrucción de la causa, a la autorización judicial y a la sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.

En este contexto, es importante destacar, por servir como uno de los parámetros a tener en cuenta en el juicio de la proporcionalidad, el ámbito objetivo de aplicación de las medidas de investigación tecnológica que se recoge

378 Cuando se trata de la ponderación aplicada en el curso de la instrucción penal, los criterios a tener en cuenta se recogen en el artículo 588 bis a), apartado 5, al establecer que «Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho».

379 STC 13/1985, de 31 de enero.

en el artículo 579.1 LECrim, respecto de la intervención de la correspondencia escrita y telegráfica, y cuya aplicación se extiende a todas las intervenciones telefónicas, telemáticas y ambientales, por mandato expreso de los arts. 588 ter a) 588 quater b), y que es objeto de previsión específica en otras intervenciones³⁸⁰. Así, se permite la intervención respecto de los siguientes hechos delictivos:

1. Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.
2. Delitos cometidos en el seno de un grupo u organización criminal.
3. Delitos de terrorismo.

A estos tres supuestos se añade en el art. 588 ter a) los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o comunicación.

Más restrictivo es el ámbito de aplicación de las medidas sobre el registro remoto de equipos informáticos, que el artículo 588 septies a) LECrim, limita a:

1. Delitos cometidos en el seno de organizaciones criminales.
2. Delitos de terrorismo.
3. Delitos cometidos contra menores o personas con capacidad modificada judicialmente.
4. Delitos contra la Constitución, de traición y relativos a la defensa nacional.
5. Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

Obviamente, si la investigación delictiva con instrumentos tecnológicos, vinculada a un proceso penal en curso, sólo podrá realizarse sobre determinados delitos comprendidos en algunas de estas categorías, es lógico que la investigación policial a prevención se lleve a cabo también teniendo en cuenta estas limitaciones. No obstante, también es preciso destacar que, en relación a las otras medidas de investigación tecnológica no se establece límite alguno, por lo que la actuación policial podría ser también más flexible a la hora de realizar el juicio de la proporcionalidad. Lo que va a resultar determinante en el juicio de proporcionalidad es la gravedad de los hechos que se pretenden evitar, el número de personas que pueden verse afectadas

380 Sobre esta cuestión ya se había pronunciado el Tribunal Constitucional en las SSTC 49/1999, de 5 abril y 167/2002, de 18 septiembre, y el Tribunal Supremo en el Auto de 18 de junio de 1992 y en algunas de sus resoluciones como el Auto 609/2013, de 14 marzo; y las sentencias 299/2006, de 17 marzo; 271/2011 de 13 abril y 184/2003 de 23 octubre.

por la realización de diligencias preventivas, y, fundamentalmente, si se las actuaciones policiales pueden derivar en una vigilancia de personas o grupos de personas determinadas.

El contenido de la solicitud policial por la que se instan la adopción de las medidas de investigación tecnológica en el curso de un proceso penal, también puede tomarse como parámetro de referencia en la adopción de diligencias policiales a prevención. En este sentido, el art. 588 bis b) LECrim, regula el contenido mínimo de la solicitud que la fiscalía o la policía han de dirigir al juez de instrucción. Resulta de suma importancia la identificación de los datos o hechos objetivos que puedan considerarse indicios de la existencia del delito, y la conexión de la persona o personas investigadas con el mismo³⁸¹, señalándose que «los indicios son *algo más que simples sospechas pero también algo menos que los indicios racionales que se exigen para el procesamiento*» o «*sospechas fundadas en alguna clase de dato objetivo*»³⁸².

Si aplicamos esta exigencia legislativa a la ejecución de medidas a prevención, la existencia de indicios racionales de comisión de determinados hechos delictivos en lugares específicos, o en espacios virtuales, y el encaje de esos hechos delictivos con los tipos previstos en el artículo 579.1 o en el artículo 588 septies a) LECrim, pueden servir de referencia a la policía para utilizar las diligencias policiales relacionadas con sistemas de inteligencia artificial.

El Tribunal Supremo se pronuncia sobre los indicios que resultan determinantes para la adopción de una medida de intervención telefónica, doctrina que puede aplicarse perfectamente a la valoración policial de los indicios que justifican medidas policiales. Así afirma que los indicios no deben entenderse como sospechas, sino como datos objetivos que por su naturaleza pueden ser susceptibles de valoración posterior. Esta exigencia relativa a la objetividad del indicio, es de suma importancia para el posterior control judicial de la diligencia y para el ejercicio del derecho de defensa³⁸³.

2.3. La aplicación del principio de proporcionalidad y la protección de datos personales

De todas formas, en el caso de la instalación de cámaras de videovigilancia habrá que tener en cuenta lo dispuesto en el artículo 15.2 LO 7/2021, sobre la instalación de cámaras de videovigilancia fijas, que ya hace alusión al princi-

381 SSTC 167/2002 de 18 de septiembre; 184/2003, de 23 de octubre; 26/2010, de 27 de abril; 70/2010, de 18 de octubre y 25/2011, de 14 de marzo.

382 Sobre esta cuestión pueden consultarse las SSTC 49/1999 de 5 de abril; 166/1999 de 27 de septiembre; 299/2000 de 11 de diciembre; 14/2001, de 29 de enero; 202/2001, de 15 de octubre; 167/2002 de 18 de septiembre; 184/2003 de 23 de octubre; 261/2005, de 24 de octubre y 220/2006 de 3 de julio.

383 SSTS 635/2012, de 17 de julio; 616/2022, de 22 de junio.

pio de proporcionalidad, vinculando su valoración en función de las siguientes finalidades: «...asegurar la protección de los edificios e instalaciones propias; asegurar la protección de edificios e instalaciones públicas y de sus accesos que estén bajo custodia; salvaguardar y proteger las instalaciones útiles para la seguridad nacional y prevenir, detectar o investigar la comisión de infracciones penales y la protección y prevención frente a las amenazas contra la seguridad pública». A este respecto, el artículo 16.1 de la citada norma, obliga al responsable del tratamiento de los datos obtenidos con la instalación de las cámaras fijas a una valoración del principio de proporcionalidad, que habrá de residenciar en la idoneidad de su tratamiento y en la intervención mínima. Igualmente, el legislador requiere que el responsable mencionado lleve a cabo un análisis de los riesgos y del impacto del tratamiento en la protección de datos, que deberá realizar ponderando, de un lado, los perjuicios que puedan derivar en la ciudadanía, y de otro la finalidad perseguida.

En este contexto, conviene retomar lo dispuesto en la Directiva 2016/680, de protección de datos personales y la definición que recoge sobre los datos y su tratamiento. Así, en el artículo 3.1 establece el concepto de datos personales, como «...*toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.* Para en su segundo apartado recoger lo que ha de entenderse por tratamiento, considerando como tal «...*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*».

La importancia de estas dos definiciones se pone de manifiesto en el análisis del principio de proporcionalidad aplicado a las medidas de prevención, al regular también la citada Directiva, en su artículo 4, las condiciones o requisitos que legitiman el tratamiento de los datos personales, al igual que la forma en que ha de realizarse dicho tratamiento. Así, tal y como establece el precepto, los datos personales ... han de ser «...*a) tratados de manera lícita y leal; b) recogidos con fines determinados, explícitos y legítimos, y no ser tratados de forma incompatible con esos fines; c) adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados; d) exactos y, si fuera necesario, actualizados; se habrán de adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean*

inexactos con respecto a los fines para los que son tratados; e) conservados de forma que permita identificar al interesado durante un período no superior al necesario para los fines para los que son tratados; f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas». Todos estos requisitos servirán para realizar el juicio de proporcionalidad, al marcar las pautas a seguir, no sólo para la obtención de los datos personales, sino incluso para su tratamiento y conservación. Estos parámetros servirán de referencia al juzgador en el momento de realizar el control judicial sobre la licitud de las diligencias realizadas por la policía cuyo resultado quiere incorporarse al proceso. De igual forma, LO 7/2021, proporciona un concepto de dato personal y de tratamiento en su artículo 5 a) y b), y también regula los parámetros para el tratamiento de los datos en el artículo 6, recogiendo literalmente lo dispuesto en la Directiva³⁸⁴.

En este orden de consideraciones, se ha prestar también atención a lo dispuesto en el artículo 11.1 de la Ley Orgánica de Fuerzas y Cuerpos de la Seguridad del Estado, que entre las funciones propias de la policía recoge la de «...Captar, recibir y analizar cuantos datos tengan interés para el orden y la seguridad pública, y estudiar, planificar y ejecutar los métodos y técnicas de prevención de la delincuencia», si bien dicha función se encuentra condicionada al respeto al derecho fundamental a la protección de datos previsto constitucionalmente en el artículo 18.4³⁸⁵.

Una vez adoptadas las diligencias de investigación policial, obtenidos los datos y realizadas, en su caso, las operaciones de tratamiento, la autoridad responsable deberá poner el resultado en conocimiento de la autoridad judicial, cuando se derive la vinculación de sujetos concretos con actuaciones delictivas, para que se inicie el correspondiente proceso penal. A este respecto el artículo 18, de la LO 7/2021, establece que el resultado de las grabaciones derivadas de la instalación de cámaras de vigilancia, se pondrán en conocimiento de la autoridad judicial en el menor plazo posible y, en todo caso, en el plazo de setenta y dos horas desde su grabación.

Junto con esta puesta a disposición judicial de las grabaciones de las que puedan derivar hechos delictivos, sería conveniente que las autoridades responsables del tratamiento de los datos, realizaran un informe detallado en el que se recogieran todos aquellos datos, que pudieran ayudar al juez en el

384 V. LARO GONZÁLEZ, M.E. «Principio de proporcionalidad y tratamiento de datos personales en el proceso penal», en *La Administración de Justicia en España y en América: José Martín Ostos, Liber Amicorum* (Martín Ríos, dir.), 2021, Astigi editores, págs. 1075 y ss.

385 NACARINO LORENTE, J.M. «La prevención del delito por las Fuerzas y Cuerpos de Seguridad y su relación con el adelanto de las barreras penales. ¿Dichas actuaciones permiten prevenir el delito y asimismo contribuir a tipificar conductas preparatorias?», en *Diario La Ley*, número 9740, 20 de noviembre de 2020.

control judicial del juicio de proporcionalidad de la medida ejecutada³⁸⁶: De esta forma, deberán constar en el informe:

1. Una exposición detallada de los indicios que han servido de apoyo para la adopción de las diligencias policiales realizadas, tanto en relación con los hechos investigados, como la localización de las actividades.
2. La justificación de la idoneidad y necesidad de la medida
3. El tiempo durante el cual se ha ejecutado.
4. La forma de su ejecución.
5. Las unidades o agentes encargados de su realización y de su supervisión.
6. Los sujetos que han resultado afectados.

La importancia de los datos que se trasladen al juzgador, y que éste ha de tomar como referencia en el juicio de proporcionalidad, en este caso *post* diligencias, se ha puesto de relieve en la modificación de la Ley procesal penal, por la Ley 13/2015, al precisar ahora en su art. 588 bis b) el contenido de la solicitud policial o del Ministerio fiscal. Si bien en los casos de diligencias preprocesales no es posible la concreción de los elementos que detallan el precepto, sí se puede tomar como referencia para que los agentes policiales tomen en consideración la necesidad de realizar un juicio de la proporcionalidad previo a la adopción de determinadas diligencias de investigación policial que pueden afectar a derechos fundamentales de los ciudadanos.

Cabe destacar que el artículo 588 bis b) LECrim, utiliza en el segundo punto la expresión «*investigación previa*»³⁸⁷. En una primera aproximación puede deducirse que el legislador exige la existencia anterior de un proceso penal en curso para la adopción de la medida a la que hace referencia³⁸⁸. Sin embargo, esta interpretación resulta demasiado restrictiva, por lo que puede

386 V. relacionado con esta cuestión la jurisprudencia del Tribunal Supremo relativa a la valoración de la proporcionalidad en las medidas de intervención telefónica STS 635/2012, de 17 de julio. V. también la STS 505/2016, de 9 de junio.

387 Al regular el contenido de la solicitud del Ministerio Fiscal o de la policía para la adopción por el juez de instrucción de una medida de investigación tecnológica, este apartado dispone que la citada solicitud deberá recoger una «exposición detallada de las razones que justifiquen la necesidad de la medida de acuerdo con los principios rectores establecidos en el artículo 588 bis a, así como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia».

388 Se recogen en estos artículos de la Ley procesal penal, las disposiciones comunes a las medidas de interceptación de las comunicaciones telefónicas, telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.

defenderse también que estaría comprendida la investigación realizada por la policía con anterioridad al inicio del proceso. En este caso, al tratarse de la medida de intervención telefónica, la solicitud de la medida supondría la inmediata incoación del proceso y, ya en este marco, se produciría su adopción. No obstante, lo que se desprende de la citada regulación y de la exigencia del legislador, es que con carácter previo al inicio del proceso, ya tiene lugar una investigación en la que se pone de manifiesto una serie de indicios y datos que pueden llevar a la realización de diligencias policiales de investigación, que después permitirán el inicio de la fase de instrucción del proceso penal³⁸⁹.

Lo que resulta evidente es que el análisis de los datos extraídos de los instrumentos relacionados con la inteligencia artificial facilita la investigación policial y la prevención de hechos delictivos, fundamentalmente de aquellos relacionados con la ciberdelincuencia y con ubicaciones de riesgo (terrorismo vinculado a creencias religiosas que ponen el foco de atención en determinados lugares de culto, tráfico de drogas o de armas con localizaciones utilizadas habitualmente, etc.). No obstante, en esta tarea policial ha de garantizarse la protección de los derechos fundamentales de las personas que utilizan las redes sociales, o que transitan por los lugares vigilados, y que en su gran mayoría no están relacionados con hechos delictivos, garantía que, como resulta obvio, ha de extenderse también a aquellos que puedan estar vinculados con actuaciones criminales. Estas garantías y protección han de extremarse en la captación de los datos en las diligencias de investigación policiales de carácter preprocesal, por lo que la aplicación del principio de proporcionalidad resulta imprescindible, dado que los resultados obtenidos pueden ser posibles fuentes a introducir en un futuro proceso penal³⁹⁰.

Postura contraria mantiene la Fiscalía General del Estado, cuando apunta una diferencia de tratamiento entre la captación de imágenes en lugares públicos y el resto de las medidas de investigación tecnológica. Respecto de estas medidas se requiere la aplicación de los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad, examinados para conceder la autorización judicial. Sin embargo, este examen no se establece en relación con la videovigilancia en lugares públicos, dado que la supervisión judicial se ha de realizar posteriormente³⁹¹. Difícil es mantener esta postura, dado que no se entiende como el juez puede validar posteriormente la diligencia aportada, por entender que se han cumplido con los principios rectores, cuando éstos no han sido objeto de valoración por las autoridades policiales. Además, es preciso tener en cuenta que la aplicación de los principios

389 MARCHENA GÓMEZ, M./GONZÁLEZ-CUELLAR SERRANO, N., *La reforma de la Ley...*, op. cit. pág. 240.

390 VELASCO NÚÑEZ, E., «Investigación penal y protección de datos, tecnología y proceso», en *Problemas procesales en un mundo digital* (Fuentes Soriano, coord.), Aranzadi, Cizur Menor, 2022, págs.81 y ss.

391 V. Circular FGE 4/2019

rectores a las medidas de investigación tecnológica se prevé con respecto a todas ellas, salvo exclusión expresa, en las disposiciones comunes recogidas en el artículo 588 bis a) LECrim. Dicha aplicación ha de observarse por todas las autoridades públicas, incluidas las autoridades policiales, dado que la vigencia del principio de proporcionalidad, de naturaleza constitucional, se exige a todos ellos para la limitación de los derechos fundamentales³⁹².

Corroborar esta postura la doctrina jurisprudencial del Tribunal Constitucional, que se ha pronunciado con ocasión de decidir sobre la validez del acceso policial a lista de contactos de un teléfono móvil sin autorización judicial, acceso basado en razones de urgencia y de investigación de los hechos. En este sentido, ha señalado que la justificación constitucional a la injerencia policial en el derecho a la intimidad, derecho afectado por la diligencia acordada, viene avalada por la existencia de un fin constitucionalmente legítimo, como lo es la investigación delictiva, por la previsión legislativa de la medida y, en el caso de no contar con la autorización judicial o el consentimiento del titular, las autoridades policiales han de llevar a cabo sus actuaciones con respeto a la legalidad³⁹³. Atendiendo a ello, cabe apuntar que la policía está autorizadas para *«la práctica de inspecciones, reconocimientos e incluso intervenciones corporales leves, siempre y cuando se respete el principio de proporcionalidad, concretado en tres exigencias o condiciones: idoneidad de la medida, necesidad de la misma y juicio de proporcionalidad en sentido estricto»*³⁹⁴.

3. El control judicial de las medidas policiales a prevención

3.1. Control judicial relativo a la adquisición del material obtenido

3.1.1. La importancia del control judicial

Si el control judicial de las medidas de investigación adoptadas en la fase de instrucción constituye un requisito imprescindible para su eficacia en el proceso, con mayor razón ha de predicarse respecto de las diligencias policiales realizadas para prevenir hechos delictivos. En estos casos el juzgador

392 RODRÍGUEZ LAINZ, J.L., «La investigación judicial de fraudes cometidos mediante empleo de tecnologías de las comunicaciones», en *Era digital, sociedad y Derecho* (Fuentes Soriano, dir.), Tirant lo Blanco, Valencia, 2020, pág. 411.

393 V. artículo 282 LECrim, y el artículo 11.1 LOFCSE.

394 STC 115/2013, de 9 de mayo. V. también, SSTC 206/2007, de 24 de septiembre; 173/2011, de 7 de noviembre, entre otras. V. también la STS 786/2015, de 4 de diciembre.

no actúa como garante de los derechos fundamentales y del respeto al proceso debido durante la investigación penal. Su actuación no tiene lugar en el momento de la solicitud de la medida, valorando su necesidad y proporcionalidad, y examinando todos los indicios que aporta la policía en su petición. Tampoco se produce un control durante la ejecución de la medida, supervisando la actuación policial y decidiendo el tiempo durante el cual cabe mantenerla, esto es, si ya se han obtenido resultados útiles para la causa y no es preciso extender más la limitación de derechos, o si, por el contrario, debe prolongarse la duración. En el caso de las diligencias policiales a prevención, su labor de control se desarrolla una vez que la diligencia se ha llevado a cabo, y su resultado, en el que se han apreciado indicios delictivos y posibles sujetos implicados, se traslada al juzgador con la finalidad de inicio del proceso, o incluso, de incorporar los datos obtenidos como fuentes de prueba. Es en este momento cuando el juzgador, a través del control judicial, ha de valorar si las autoridades policiales han utilizado las medidas en atención a la base legal que las regula, y han aplicado el juicio de proporcionalidad en todas sus manifestaciones.

La importancia del control judicial de las medidas de investigación tecnológica practicadas en la instrucción penal, se ha puesto de relieve antes de su regulación por la LO 13/2015, y se ha incorporado a dicha regulación. Precisamente, por su extraordinaria relevancia se ha considerado necesario realizar ahora algunas precisiones al respecto.

En primer lugar, conviene apuntar que la jurisprudencia ha hecho referencia a dos tipos de control judicial en el desarrollo de las medidas de investigación tecnológica acordadas en el proceso penal. Uno, que se relaciona con el control de constitucionalidad, y otro, con el control de legalidad ordinaria. Así lo destaca el Tribunal Supremo cuando afirma que *«el control judicial de la ejecución de la medida se integra en el contenido esencial del derecho cuando es preciso para garantizar su corrección y proporcionalidad. Pero no existe lesión del derecho fundamental cuando las irregularidades denunciadas, por ausencia o insuficiencia del control judicial, no se realizan en la ejecución del acto limitativo sino al incorporar a las actuaciones sumariales su resultado —entrega y selección de cintas, custodia de originales o transcripción de su contenido— pues en tales casos la restricción del derecho fundamental al secreto de las comunicaciones llevada a cabo por los funcionarios policiales en los que se delegó su práctica se ha mantenido dentro de los límites de la autorización... Cuestión distinta es que la defectuosa incorporación a las actuaciones de su resultado no reúna las garantías de control judicial y contradicción suficientes como para convertir la grabación de las escuchas en una prueba válida para desvirtuar la presunción de inocencia. Mas al ser tales irregularidades procesales posteriores a la adquisición del conocimiento cuya prueba funda la condena, lo conocido gracias a las escuchas puede ser introducido en el juicio oral como elemento de convicción a través de otros medios de prueba que acrediten su contenido, por ejem-*

plo, mediante las declaraciones testificales de los funcionarios policiales que escucharon las conversaciones intervenidas... Todo lo que respecta a la entrega y selección de las cintas grabadas, a las custodia de las originales y a la transcripción de su contenido no forma parte de las garantías derivadas del art. 18.3 CE»³⁹⁵.

De esta forma, el control judicial de la medida durante la fase de ejecución, forma parte del contenido esencial del derecho, y así lo ha señalado doctrina y jurisprudencia³⁹⁶. Sólo a través de dicho control puede supervisarse su desarrollo garantizando el juicio de proporcionalidad. Así lo continúa afirmando en sentencias recientes el Tribunal Supremo, cuando señala que *«forma parte del contenido esencial del artículo 18.3 CE la exigencia de motivación de las resoluciones judiciales que autorizan la intervención o su prórroga, y que en el momento de la adopción de la medida las resoluciones deben explicitar todos los elementos indispensables para realizar el juicio de proporcionalidad y para hacer posible su control posterior, pues por la propia naturaleza del mecanismo de investigación, la defensa no puede tener lugar en el momento de su adopción»*³⁹⁷.

Para el Tribunal Constitucional *«...el control judicial efectivo, en el desarrollo y cese de la medida, es indispensable para el mantenimiento de la restricción del derecho fundamental, dentro de los límites constitucionales. El Juez que la autorice debe, en primer término, conocer los resultados obtenidos con la intervención, y en el supuesto de que se produzca una divergencia entre el delito objeto de investigación y el que de hecho se investiga, debe adoptar la resolución que proceda, puesto que en otro caso (Sentencia T.E.D.H., caso Klass, de 6 de septiembre de 1978, caso Malone, de 2 de agosto de 1984, y caso Kruslin de 24 de abril de 1990), las intervenciones constituirían una injerencia de la autoridad pública en el ejercicio del derecho del afectado al respeto de su correspondencia y de su vida privada»*³⁹⁸.

395 STC 121/1998, de 15 de junio. V. también las SSTC 49/1999, de 5 de abril; 166/1999, de 27 de septiembre; 236/1999, de 20 de diciembre; 237/1999, de 20 de diciembre; 75/2000, de 27 de marzo; 92/2000, de 10 de abril; 126/2000, de 16 de mayo; 202/2001, de 15 de octubre; 82/2002, de 22 de abril; 167/2002, de 18 de septiembre; 184/2003, de 23 de octubre; 165/2005, de 20 de junio; 150/2006 de 22 de mayo; 9/2011, de 28 de febrero entre otras.

396 SSTs. 56/2009 de 3 de febrero; 924/2009 de 7 de abril. V. MARCHENA GÓMEZ, M./GONZÁLEZ-CUELLAR SERRANO, N., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Castillo de Luna. Ediciones jurídicas, Madrid, 2016, pág—268 y ss.

397 STS 491/2019, de 16 de octubre. V. también las SSTC 197/2009, de 28 de septiembre. Y las SSTs 116/2013, de 21 de febrero; 821/2012, de 31 de octubre, 629/2011, de 23 de junio, 628/2010, de 1 de julio.

398 STC 49/1996, de 26 de marzo. V. también las SSTC166/1999, de 27 de septiembre; 299/2000, de 11 de diciembre; 138/2001, de 18 de junio; 202/2001, de 15 de octubre; 167/2002, de 18 de septiembre.

Obviamente, estas consideraciones no pueden aplicarse estrictamente al control judicial que ha de supervisar las actuaciones policiales a prevención, y ello porque dicho control se produce siempre con posterioridad al desarrollo de las medidas³⁹⁹. En estos casos, el control por el juzgador se convierte siempre en un control de constitucionalidad, al requerirse que la actuación judicial supervise si las diligencias policiales se han desarrollado conforme a las previsiones legales, y si las autoridades policiales han aplicado principio de proporcionalidad (idoneidad, necesidad y proporcionalidad en sentido estricto). Además, el juez también ha de comprobar si en la incorporación de los materiales obtenidos en el proceso, se cumplen las garantías exigidas por la Ley procesal penal y la jurisprudencia para ese tipo de diligencias (soportes originales, autenticidad, contenido preciso y descriptivo del atestado en el sentido antes descrito).

El cumplimiento de todos estos requisitos, así como la información que pueda trasladarse al juez sobre la ejecución de las diligencias y el tratamiento de los datos obtenidos, no sólo van a facilitar el examen del juicio de proporcionalidad, sino que también favorecerá la contradicción y el derecho de defensa. En este sentido, ha de ponerse de relieve que el traslado al juzgador de las circunstancias de adopción y ejecución de las medidas va a permitir a la defensa contradecir los resultados aportados, o bien solicitar diligencias de investigación complementarias que ratifique o contradigan el resultado. Por tal motivo, es importante trasladarle los datos relacionados con los criterios de búsqueda en redes, en su caso, o los utilizados para la localización de las cámaras de videovigilancia, o los que se han ejecutado para el análisis y tratamiento de datos, la identificación de las autoridades responsables del tratamiento, el tiempo durante el cual se ha ejecutado la diligencia, etc.⁴⁰⁰.

Una expresa referencia al contenido del control judicial en relación con la videovigilancia en lugares públicos, la realiza el Tribunal Supremo, recogiendo las garantías que han de tenerse en cuenta: «1.º) *Control judicial de la legitimidad de la filmación, que implica el que el juez instructor supervise que la captación de las imágenes se efectuó con el debido respeto a la intimidad personal y a la inviolabilidad domiciliaria, pues si la filmación merece un juicio desfavorable notoriamente a la luz de los citados derechos fundamentales debería negarse la incorporación a los autos de la filmación* «ex» artículo 11 de la Ley Orgánica del Poder Judicial. 2.º) *Comunicación y puesta a disposición judicial del material videográfico, en términos rela-*

399 V. en esta cuestión la Circular 4/2019, FGE, en la que se señala esta diferencia temporal del control judicial. Mientras que en las otras medidas de investigación tecnológica el control se produce con anterioridad a la resolución judicial, por tanto, la autorización del juez de instrucción se otorga previo análisis de los principios de proporcionalidad, idoneidad y necesidad de la medida. En el caso de la captación de imágenes en lugares públicos, el control judicial tiene lugar a posteriori, una vez realizada la grabación.

400 VELASCO NÚÑEZ, E., «Investigación penal y protección de datos, tecnología y proceso», en *Problemas procesales...*, op. cit., pág. 111.

tivamente breves, por cuanto que la aportación mientras más rápida sea, constituye una garantía en favor de su autenticidad, por cuanto que ella, va en detrimento de su posible manipulación. 3.º) Aportación de los soportes originales a los que se incorporan a las imágenes captadas. 4.º) Aportación íntegra de lo filmado, a fin de posibilitar la selección judicial de las imágenes relevantes para la causa»⁴⁰¹.

Respecto de la inmediata puesta a disposición judicial del resultado de la medida, se ha pronunciado el Tribunal Supremo en numerosas ocasiones, considerando que esta cuestión evita sospechas sobre una posible manipulación, y, además, cumple con lo exigido de poner a disposición judicial en el plazo de 72 horas, cuando de las grabaciones se pueda deducir la comisión de hechos delictivos. Así lo expresa el Tribunal afirmando que «...efectivamente es preferible que las grabaciones videográficas sean puestas cuanto antes a disposición de la autoridad judicial, el transcurso del tiempo no es un elemento que prive de valor de forma absoluta a tales grabaciones. La razón de la celeridad en la aportación se explica, cuando el autor de las grabaciones es la Policía, por la obligación que le cumple de informar al Juez, en los términos marcados por la Ley, de la integridad de los resultados de su investigación preliminar. Y tal aportación se encamina a disminuir las posibilidades de manipulación del material, de manera que el retraso en la entrega pudiera conducir a hacer recomendable una mayor verificación de su autenticidad mediante su confrontación con otras pruebas y, en su caso, de ser así solicitado o de oficio en caso de que existan dudas razonables por parte del Juez instructor, mediante los exámenes técnicos que permitan garantizar la ausencia de alteraciones significativas»⁴⁰².

3.1.2. Elementos de referencia en el control judicial

Hechas estas consideraciones, conviene precisar que la puesta a disposición judicial del resultado de diligencias policiales realizadas con carácter previo a la incoación del proceso penal, y de las que se derivan datos importantes para la instrucción y fuentes de prueba que pueden ser útiles para el enjuiciamiento⁴⁰³, requiere la valoración del juzgador de varios aspectos, cuya combinación va a permitir determinar la legalidad de la diligencia desde la perspectiva del juicio de la proporcionalidad, ejecutándose así el control judicial exigido constitucionalmente para la limitación de derechos fundamentales.

401 STS 968/1998, de 17 julio.

402 V. por todas, SSTs. 1154/2010 de 12 enero 2011 y 200/2017, de 27 de marzo.

403 V. VELASCO NUÑEZ, E., «La captación de la imagen de lugares y personas como medio de investigación penal» en *El Derecho.com. Noticias jurídicas y actualidad*, 25 enero 2011. <https://elderecho.com/la-captacion-de-la-imagen-de-lugares-y-personas-como-medio-de-investigacion-penal>

En este sentido, lo primero que cabe examinar es la adecuada adopción de la diligencia acordada, teniendo en cuenta las condiciones de su previsión legal. Además, el juez comprobará si se ha realizado el conveniente juicio de proporcionalidad por las autoridades policiales con carácter previo a la ejecución de estas diligencias. Para ello tendrá en cuenta la gravedad de los hechos, o de los indicios que han servido de base para que la policía decidiera que esta medida era necesaria; los posibles sujetos afectados por las actuaciones que se quieren prevenir; los derechos fundamentales que se pueden poner en juego; la previsión temporal de la medida, y, en el caso de ser una medida continuada, la justificación de esta continuidad. Además, resulta de gran importancia, que se justifique el tiempo que se ha tardado en poner a disposición del juzgador el material resultante, y las diligencias que se han acordado durante ese tiempo. No cabe obviar que, una vez descubiertos hechos delictivos concretos y sus posibles autores, la puesta a disposición judicial ha de ser inmediata, ya que la investigación debe continuar con la incoación del proceso penal, rodeando al investigado de todas las garantías del proceso debido.

Llegados a este punto el juez validará o no la medida adoptada por la policía, recogiendo en el auto correspondiente su conformidad sobre la necesidad de la medida y con la válida actuación policial⁴⁰⁴.

En este contexto, y en relación con las fuentes de prueba que pueden derivar de las medidas policiales adoptadas a prevención, podría tomarse en consideración lo dispuesto en el artículo 282 LECrim que autoriza a la policía a la práctica de las «...*diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la autoridad judicial*». Sin embargo, es necesario precisar que este precepto se encuentra integrado dentro del Título III, De la policía, en el Libro II Del Sumario, de la Ley procesal penal, por lo que su contenido ha de encuadrarse dentro de la investigación policial desarrollada en la fase de instrucción del proceso penal.

La investigación policial preprocesal se enmarca, como se ha apuntado, en el ámbito de actuación de las Fuerzas y Cuerpos de la Seguridad del Estado. Así, el artículo 11 de la LO 2/1986, de 13 marzo, de Fuerzas y Cuerpos de Seguridad, recoge, en su primer apartado, las funciones principales relacionadas con la comisión de actuaciones criminales: Prevenir la comisión de actos delictivos; Investigar los delitos para descubrir y detener a los presuntos culpables, asegurar los instrumentos, efectos y pruebas del delito, poniéndolos a disposición del Juez o Tribunal competente, y elaborar los informes técnicos y periciales procedentes; Captar, recibir y analizar cuantos datos tengan

404 RODRÍGUEZ LAINZ, J.L., «La investigación judicial de fraudes cometidos mediante empleo de tecnologías de las comunicaciones», en *Era digital y Derecho...*, op. cit., pág. 420.

interés para el orden y la seguridad pública, y estudiar, planificar y ejecutar los métodos y técnicas de prevención de la delincuencia. Es este campo en el que se centra las actuaciones a prevención, que se complementa con lo específicamente previsto en la LO 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos, y en la LO 7/2021, de protección de datos personales.

En relación con la legalidad de las medidas policiales a prevención, es preciso puntualizar que su eficacia procesal se condiciona a la legitimidad en su obtención. La previsión legal se convierte así en la primera garantía. Conforme a la jurisprudencia del TEDH⁴⁰⁵, que ha sido convenientemente destacada por el Tribunal Constitucional⁴⁰⁶ y el Tribunal Supremo⁴⁰⁷, las intromisiones en la esfera de protección de la vida privada han de estar previstas en una ley y ser necesarias en una sociedad democrática. La necesaria previsión legal ha de concretarse en una norma legal accesible para los ciudadanos, con la finalidad de que puedan conocer y asumir las posibles restricciones de sus derechos fundamentales.

3.2. Control judicial relativo a la incorporación del resultado al proceso

3.2.1. Incorporación del resultado de las medidas policiales a prevención al proceso

Lo que resulta evidente es que el resultado obtenido con las diligencias policiales preventivas, ha de incorporarse al proceso, y que, en el control judicial preceptivo, ha de examinarse, además de lo señalado anteriormente, si la forma de incorporación de los instrumentos utilizados y de su resultado cumple con las garantías del proceso penal, desde la perspectiva no sólo de la

405 El artículo 8.2 CEDH dispone que no podrá haber injerencia alguna en el ejercicio de los derechos fundamentales, en tanto en cuanto esta injerencia esté, prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás. V. V. SSTEDH de 6 de septiembre de 1978, caso Klass y otros; de 25 de marzo de 1983; caso Silver y otros; de 27 de octubre de 1983, caso Malone; de 18 febrero de 2003, Caso Prado Bugallo; de 31 mayo 2005, Caso Vetter; de 1 julio 2008, caso Liberty y otros.

406 STC 37/1989, de 15 de febrero; 150/1989, de 25 de septiembre; 85/1994, de 14 de marzo; 34/1996, de 17 de abril; 49/1996, de 26 de marzo; 54/1996, de 27 de abril; 123/1997, de 1 de julio; 49/1999, de 5 de abril; 206/2007, de 24 de septiembre, entre muchas otras.

407 Auto de 18 de junio de 1992, STS 579/88, de 22 de abril; STS 533/1999, de 29 de marzo. 1335/2001, de 19 de julio; 269/2013, de 27 de marzo; 155/2007 de 28 de febrero; 297/2006 de 6 de marzo, entre muchas otras.

legalidad del procedimiento, sino con mayor relevancia incluso, del principio de contradicción y del derecho de defensa. Garantizar el ejercicio de contradicción y facilitar la defensa se plantean como exigencias inexcusables en la introducción de este material.

La LO 3/2015, de modificación de la Ley de Enjuiciamiento Criminal, no ha establecido un procedimiento específico de incorporación de las actuaciones policiales a prevención en el proceso penal, pero ello no quiere decir, que esta incorporación no se produzca. La ausencia de regulación expresa exige recurrir a los cauces ya existentes, y que habían sido utilizados ya con anterioridad a la reforma. De esta forma la prueba documental, o el reconocimiento judicial, se convierten en los medios probatorios de referencia. Sorprendentemente, a pesar de la completa regulación de la LO 13/2015, no se ha introducido en la Ley procesal penal un cauce adecuado y específico para la introducción de estos materiales en el proceso. De esta forma, no se contempla una regulación *ad hoc*, en la que se establezcan el procedimiento y garantías de introducción de las fuentes derivadas de diligencias de investigación tecnológica⁴⁰⁸.

Si bien no se ha producido esta necesaria reforma en la norma procesal penal es ya habitual la referencia a la regulación de un procedimiento autónomo para la introducción de estas fuentes de prueba tecnológicas, haciéndose además alusión a que los soportes magnéticos que las incorporan pueden calificarse de documentos electrónicos de los que deriva un contenido similar o equiparable al que se desprende de un documento escrito.

Así pues, es preciso traer a colación el concepto de documento electrónico que proporciona el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, y por la que se deroga la Directiva 1999/93/CE, norma a la que se remite el artículo 326 LEC después de su modificación por la Ley 6/2020, de 11 noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. El artículo 3, en su apartado 35, define el documento electrónico como «*todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual*». A esta definición se puede sumar la prevista anteriormente por la ahora derogada Ley 59/2003, de 19 de diciembre, de firma electrónica, que lo entendía como aquel que recoge aquella «*...información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado*»⁴⁰⁹. Además, la inclu-

408 DURAN SILVA, C., «Aspectos procesales de la videovigilancia practicada por las Fuerzas y Cuerpos de Seguridad del Estado» en *La ley Penal*, número 126, mayo 2017, <https://observatorio-cientifico.ua.es>

409 Artículo 3.5 y 8 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, ahora derogada por la Ley 6/2020, de 11 noviembre, reguladora de determinados aspectos de los ser-

sión del contenido de un dispositivo electrónico en el concepto de documento viene también avalada por el artículo 26 C, cuando establece que «...a los efectos de este Código se considera documento todo soporte material que exprese e incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica»⁴¹⁰.

Otra cuestión a tener en cuenta, ante la falta de una regulación específica de estos instrumentos como medios de prueba en el proceso penal, será la relativa a determinar qué tipo de instrumentos, de los reconocidos como documentos electrónicos, pueden incorporarse al proceso. Parece evidente que al no existir limitación legal alguna, y teniendo en cuenta lo dispuesto en el artículo 24.2 CE, relativo al derecho a utilizar todos los medios de prueba pertinentes para la defensa y la prohibición de indefensión del artículo 24.1 CE, procederá la entrada de todos los instrumentos, siempre que se cumplan estas dos condiciones. La primera, que puedan ser examinados por el tribunal con respecto a las garantías del proceso debido, y la segunda, que el juzgado disponga o pueda disponer de los medios técnicos necesarios para la práctica de dicha prueba⁴¹¹.

Si se parte del concepto de prueba electrónica, como aquella que hace referencia a la información contenida en un medio electrónico, o transmitida por dicho medio, que proporciona el conocimiento de un hecho controvertido, mediante el convencimiento del juzgador o por imperativo legal⁴¹², será

vicios electrónicos de confianza. Precisaba también la citada norma que El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio».

410 DELGADO MARTÍN, J. «La prueba digital. Concepto, clases, aportación al proceso y valoración», en *Diario La Ley*, número 6, 11 de abril de 2017, <https://diariolaley.laleynext.es/Content/Documento.aspx>, pág. 7. V. también BUENO DE MATA, F., *Investigación y prueba de delitos de odio...*, op. cit., pág. 32 y siguientes; DELGADO MARTÍN, J., «La prueba digital. Concepto, clases...», op. cit., pág. 1; DURÁN SILVA, C., «Aspectos procesales de la videovigilancia practicada por las Fuerzas y Cuerpos de Seguridad del Estado» en *La ley penal: Revista de Derecho penal, procesal y penitenciario*, número 126, 2017, <https://legalteca-aranzadi-laley-es.ezbusc.usc.gal>, pág. 7.

411 DELGADO MARTÍN, J. «La prueba digital. Concepto...», op. cit., pág. 7.

412 V. SANCHÍS CRESPO, C., «La prueba en soporte electrónico» en *Las Tecnologías de la información y de la comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio*, (Valero Torrijos, coord.), Thomson Reuters Aranzadi, Navarra, 2012, pág. 713; DELGADO MARTÍN, J., «La prueba digital. Concepto...», op. cit., pág. 1. V. también sobre esta cuestión el Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023 (LA LEY 22209/2023), sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales, y la Directiva (UE) 2023/1544 del Parlamento Europeo y del Consejo, de 12 de julio de 2023 (LA LEY 22208/2023), por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales.

necesario admitir que este tipo de pruebas se compone de dos elementos: uno técnico que se concreta en el dispositivo de almacenamiento (hardware) y otro lógico (software) que se refiere a su contenido⁴¹³. Así, esta clase de prueba se caracteriza porque puede abarcar cualquier tipo de información, que se almacena y transmite por medios electrónicos, con la finalidad de acreditar hechos en un proceso. En este concepto se integrarían tanto aquellos dispositivos que permiten el almacenamiento de datos, como los que permiten su transmisión por redes de comunicación como Internet, telefonía u otras. En este segundo grupo, no sólo se incluyen la transmisión de datos persona a persona, como es el caso de la telefonía, o la utilización de Internet con carácter restringido entre sujetos determinados, sino también la transmisión, vía red, sin destinatario concreto⁴¹⁴.

Partiendo de la ausencia de previsión legislativa sobre el acceso de estas fuentes de prueba al proceso penal, podrá acudir a las disposiciones de la Ley de Enjuiciamiento Civil, en cuanto norma supletoria con carácter general⁴¹⁵. De esta forma, el acceso al proceso podría realizarse a través del artículo 299.2 LEC, sin embargo, en el precepto citado tampoco se describe o diseña el procedimiento de práctica de este medio de prueba, si bien los artículos 382 y 383 LEC, sí hacen referencia a su aportación en el proceso civil. Por ello, respecto del proceso penal, sería necesario acudir, al igual que otros instrumentos tecnológicos, a la prueba documental, o incluso al reconocimiento judicial cuando el juzgador pueda examinar por sí mismo el dispositivo aportado⁴¹⁶. Por tanto, la prueba documental y, en algunos casos, la inspección ocular o el reconocimiento judicial, se consideran los medios probatorios más adecuados para la introducción en el proceso de estas fuentes de prueba⁴¹⁷.

413 V. BUENO DE MATA, F., «La utilización de drones como diligencia de investigación...», *op. cit.*, pág. 4.

414 DELGADO MARTÍN, J., «La prueba digital. Concepto, clases...», *op. cit.*, pág. 1.

415 V. ARRABAL PLATERO, P., «El binomio Derecho procesal y nuevas tecnologías: de las pruebas tecnológicas al uso de la inteligencia artificial en la Administración de Justicia» en *El Derecho de la encrucijada tecnológica...*, *op. cit.*, pág. 4; BUENO DE MATA, F., «La utilización de drones como diligencia de investigación...», *op. cit.*, pág. 5; DELGADO MARTÍN, J., «La prueba digital. Concepto...», *op. cit.*, pág. 2; DURÁN SILVA, C., «Aspectos procesales de la videovigilancia...», *op. cit.*, pág. 10.

416 A título de ejemplo podrá practicarse a través del reconocimiento judicial cuando se pretenda el examen de un documento videográfico, del examen directo de los correos electrónicos o de los mensajes de telefonía móvil. V. ARRABAL PLATERO, P., «El binomio Derecho procesal y nuevas tecnologías...», *op. cit.*, pág. 5; DURÁN SILVA, C., «Aspectos procesales de la videovigilancia...», *op. cit.*, pág. 12.

417 Es obligado acudir a la distinción entre fuentes y medios de prueba. La fuente de prueba designa una realidad extrajurídica que existe con anterioridad al proceso, y seguirá existiendo, aunque éste no llegue a iniciarse. Por el contrario, cuando se habla de medio de prueba, se hace referencia a la actividad que es preciso desarrollar para que esa realidad extraprocesal pueda ser introducida en el proceso. Por tanto, cuando se alude a los

La prueba documental es objeto de una insuficiente regulación en la Ley procesal penal, que se limita a recogerla en su artículo 726, cuando se refiere al examen por el tribunal de «...libros, documentos, papeles y demás piezas de convicción que puedan contribuir al esclarecimiento de los hechos o a la más segura investigación de la verdad». Por tal motivo, de nuevo habrá de acudir a la Ley de Enjuiciamiento Civil, dada su consideración de norma supletoria respecto del proceso penal⁴¹⁸.

En la incorporación de las fuentes de prueba tecnológicas, ha de diferenciarse entre aquellas que se pueden transcribir, y son los documentos escritos los que se introducen en el proceso, y aquellas otras en las que se incorporan al proceso los soportes electrónicos. De todas formas, en el primer caso, los documentos escritos derivados de la transcripción del contenido de los soportes electrónicos, es necesario apuntar que siempre puede requerirse la aportación de los citados soportes a efectos de practicar pruebas complementarias relativas a su autenticidad e integridad.

Respecto de la transcripción del contenido de los soportes electrónicos por fedatarios públicos⁴¹⁹, no se puede sostener que la transcripción por el notario convierta el documento en un documento público en cuanto a su autenticidad. En estos casos, lo que se refuerza es que el contenido aportado a través del acta notarial es el mismo que el que se «guarda» en el documento transcrito, pero ello no quiere decir que ese contenido se convierta automáticamente en auténtico⁴²⁰.

Cuando la incorporación al proceso se lleve a cabo a través de la aportación de los soportes electrónicos, resulta imprescindible disponer de un medio técnico que permita la lectura de su contenido. En este aspecto, el examen por el tribunal y las partes no se limita únicamente al contenido del documento electrónico, sino que también podrá examinarse el soporte aportado, dado a determinar su autenticidad y la ausencia de manipulación. En un

medios de prueba siempre se hace en consideración a un proceso ya iniciado. V. CARNELUTTI, F., *La prova civile*, Roma, 1947, págs. 83 y ss. En las pruebas relacionadas con las nuevas tecnologías y la inteligencia artificial, la denominada prueba electrónica, la fuente de la prueba sería la información obtenida por medios electrónicos que se pretende introducir en el proceso, mientras que el medio de prueba será el procedimiento a través del cual esa información entra en el proceso. V. BANACLOCHE PALAO, «La prueba en el proceso penal», en *Aspectos fundamentales del Derecho Procesal Penal*, Editorial La Ley, 2.ª edición, Madrid, 2011, pág. 273. DELGADO MARTÍN, J., «La prueba digital. Concepto, clases...» *op. cit.*, pág. 1.

418 Artículo 4 LEC «En defecto de disposiciones en las leyes que regulan los procesos penales, contencioso-administrativos, laborales y militares, serán de aplicación, a todos ellos, los preceptos de la presente Ley».

419 Sobre los tipos de documentos públicos electrónicos v. DELGADO MARTÍN, J., «La prueba digital. Concepto, clases...» *op. cit.*, págs. 9-10.

420 MARTÍNEZ GALINDO, G., «Problemática jurídica de la prueba digital y sus implicaciones en los principios penales» en *Revista Electrónica de Ciencia Penal y Criminología*, <http://criminet.ugr.es/recpc>, pág. 17.

determinado número de contenidos de soportes electrónicos (correos electrónicos, pantallazos, comentarios en redes sociales o en chats, etc.) la incorporación por medios escritos, o en imágenes, no garantiza su fiabilidad, y por tanto no se puede derivar automáticamente su eficacia probatoria. La integridad de los medios aportados en los que se contiene la información resulta de especial relevancia a efectos de posteriores comprobaciones⁴²¹.

En este aspecto, también la prueba pericial juega un papel muy importante, ya que es habitual que la introducción en el proceso de estos dispositivos tecnológicos vaya acompañada de dudas sobre su autenticidad⁴²². Por tanto, la práctica de una pericial complementaria podrá despejar las posibles dudas que rodean a este tipo de pruebas, pericial que ha de pronunciarse tanto sobre la autenticidad del dispositivo aportado, como sobre la ausencia de manipulación de su contenido. El peritaje informático se integra por aquellas operaciones periciales derivadas de conocimientos técnicos relacionados con la informática y el funcionamiento de las nuevas tecnologías y los instrumentos de inteligencia artificial⁴²³. Requiere conocimientos específicos sobre la materia y se caracterizan por su especial complejidad, lo que exige al perito en el proceso judicial una explicación clara y precisa sobre el funcionamiento de los sistemas y sobre las posibles manipulaciones que pueden sufrir.

La aportación de estas fuentes al proceso también podrá completarse con la práctica de la testifical por parte de las unidades policiales que han supervisado la ejecución de la medida y de los responsables del tratamiento de datos, en su caso.

3.2.2. Algunas reflexiones sobre la cadena de custodia

Otra de las cuestiones relevantes, respecto de la introducción del material obtenido en diligencias policiales a prevención, es la garantía de la cadena de custodia desde su obtención hasta su puesta a disposición judicial. Cuando estas diligencias se practican en la fase de instrucción, la presencia del Letrado de la Administración de Justicia en el volcado de datos es determinante, pero en diligencias preprocesales no se cuenta con esta garantía. La cadena de custodia permite, a través de la documentación aportada por la policía, constatar la integridad y autenticidad del material obtenido⁴²⁴. Para ello se procederá a su sellado para ponerlo a disposición del tribunal cuando sea necesario. Si es preciso continuar con las diligencias y trabajar con el

421 MARTÍNEZ GALINDO, G., «Problemática jurídica de la prueba digital...», *op. cit.*, pág. 18. V. también la STS 300/2015, de 19 mayo

422 V. STS 300/2015, de 19 mayo

423 DELGADO MARTÍN, J., «La prueba digital. Concepto, clases...», *op. cit.*, pág. 13.

424 V. artículos 326 y 338 LECrim.

material, o incluso realizar una pericial, se puede realizar un clonado o volcado de datos, a efectos de preservar el original de posibles daños⁴²⁵.

La observancia de la cadena de custodia requiere que en la fase de investigación policial se adopten las medidas necesarias para que el material obtenido se incorpore al proceso penal en el mismo estado en el que se produjo su captación o adquisición, garantizándose la ausencia de alteraciones. De esta forma, se puede comprobar que se trata de la misma fuente de prueba (autenticidad), y que no se ha producido ninguna manipulación (integridad)⁴²⁶.

De todas formas, la garantía de la cadena de custodia en las evidencias tecnológicas tiene una especial consideración, precisamente por las dudas y sospechas sobre su autenticidad y manipulación, que las convierten en piezas de convicción sujetas habitualmente a prácticas periciales. En este sentido, ya se ha pronunciado el Tribunal Supremo al considerar que las dudas sobre su autenticidad no se pueden plantear por las partes, con carácter genérico, sino que se han de aportar datos e indicios que planteen una duda razonable sobre la custodia de los dispositivos⁴²⁷. El propio Tribunal ya dejaba claro en 2015, que determinadas aportaciones del contenido de los dispositivos electrónicos habían de rodearse de periciales para garantizar su autenticidad, que en muchas ocasiones deben practicarse por quien aportaba el dispositivo. Así lo afirmaba respecto a las capturas de pantalla, considerando imprescindible que una pericial informática acreditase el contenido, la identidad de los interlocutores y la integridad de la conversación⁴²⁸. Sin embargo, en resoluciones posteriores, se matizaba esta exigencia en el sentido de que la prueba pericial era necesaria en aquellos casos en los que se impugnaba la autenticidad de lo aportado⁴²⁹.

La constante impugnación de los documentos electrónicos aportados en el proceso penal ha llevado al Tribunal Supremo a relajar su doctrina jurisprudencial de una forma un tanto preocupante⁴³⁰. En recientes resoluciones, parece partir el tribunal de la validez inicial de este tipo de documento, y hace recaer en la parte perjudicada la carga de demostrar su falsedad. Cuando estos documentos son aportados por la acusación, es la defensa, a través

425 VELASCO NUÑEZ, E., «Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica» en *Diario LA LEY*, número 8183, noviembre de 2013, <https://soluciones-aranzadilaley-es.ezbusc.usc.gal>, pág. 12.

426 V. más ampliamente BUJOSA VADEL, L.M./BUSTAMANTE RÚA, M.M.³/TORO GARZÓN, L.O., La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia, en *Revista Brasileira de Direito Processual Penal*, <https://revista.ibraspp.com.br/RBDPP/article/view/482/424>.

427 STS 990/2016, de 12 de enero.

428 STS 300/2015, de 19 de mayo.

429 SSTS 375/2018, de 19 de julio; 332/2019 de 27 de junio.

430 SSTS 116/2025, de 13 de febrero; 603/2025 de 1 de julio; 629/2025 de 7 de julio.

de su impugnación y la práctica de la prueba pericial, la que ha de demostrar la autenticidad e integridad del documento. De esta forma, la acusación se libera de justificar la veracidad del contenido de las pruebas aportadas⁴³¹.

Es indudable que la correcta incorporación al proceso del material derivado de las diligencias policiales a prevención favorece y facilita el derecho de defensa y la observancia del principio de contradicción. Por tal motivo, es importante y, además, en el caso de diligencias policiales, también es de obligado cumplimiento, que dicho material se incorpore en la fase de instrucción, dando lugar incluso, en algunos casos, a la incoación del proceso penal. La aportación de los soportes originales contribuye a despejar las dudas sobre su autenticidad al facilitar las posibles prácticas periciales. De igual forma, las partes podrán comprobar el contenido completo del material, preservándose así la igualdad de armas⁴³².

Dada la complejidad de las diligencias de investigación tecnológica y relacionadas con la inteligencia artificial, y teniendo en cuenta, en nuestro caso, la ausencia de una autorización judicial previa y de un control judicial en su ejecución, las sospechas sobre la manipulación y las dudas relativas a la integridad y autenticidad de los dispositivos electrónicos, o de su contenido, deben derivar en una exclusión probatoria, o en una valoración negativa de su resultado. No cabe que este tipo de diligencias puedan desvirtuar la presunción de inocencia cuando existen dudas sobre su autenticidad e integridad, aunque no se haya podido comprobar la existencia de manipulaciones o alteraciones⁴³³.

431 V. AVILA MARTÍNEZ, V., «A la deriva con la prueba informática: el Supremo relaja el estándar probatorio de las capturas de 'WhatsApp'», en *Economist & Jurist*, 27 de agosto de 2025.

432 ETXEBERRÍA GURIDI, J.F., «Videovigilancia y su eficacia en el proceso penal español», en *Cuadernos de Derecho Penal*, febrero de 2014, págs. 98-99.

433 MARTÍNEZ GALINDO, G., «Problemática jurídica de la prueba digital...», *op. cit.*, pág. 22.

BIBLIOGRAFÍA

ALONSO SALGADO, C., «El problema de la falta de transparencia en la interacción de la inteligencia artificial y la justicia», en *Inteligencia artificial legal y Administración de justicia* (Calaza López/Llorente Sánchez-Arjona, dirs.), Aranzadi, Cizur Menor (Navarra), 2022.

ARIZA COLMENAREJO, M.^a J., Garantías procesales en el uso de drones en la investigación penal, en *Era digital, sociedad y Derecho* (Fuentes Soriano, dir.), Tirant lo Blanch, Valencia, 2020.

— «Fuentes de datos al servicio de sistemas de inteligencia artificial dirigidos a la toma de decisiones judiciales» en *Inteligencia artificial y proceso penal: un reto para la Justicia*, (Castillejo Manzanares/Noya Ferreiro, dirs.), Aranzadi, Cizur Menor (Navarra), 2023.

ARMENTA DEU, T. *Derivas de la justicia. Tutela de los derechos y solución de controversias en tiempos de cambio*, Editorial Marcial Pons, Madrid 2021.

— «El proceso en la Europa digital: entre recuperar liderazgos y proteger derechos» (Colomer Hernández, Dir.), *Uso de la información y de los datos personales en los procesos: los cambios en la era digital*, Cizur Menor, 2022.

ARRABAL PLATERO, P., «El derecho fundamental al propio entorno virtual y su incidencia en el proceso», en *Era digital, sociedad y Derecho* (Fuentes Soriano, dir.), Editorial Tirant lo Blanch, Valencia, 2020.

— «El binomio Derecho procesal y nuevas tecnologías: de las pruebas tecnológicas al uso de la inteligencia artificial en la Administración de Justicia» en *El Derecho de la encrucijada tecnológica. Estudios sobre derechos fundamentales, nuevas tecnologías e inteligencia artificial*, (Martín Ríos/Villegas Delgado, coords.), Tirant lo Blanch, Valencia, 2022.

ASENCIO MELLADO, J.M.^a., *Prueba prohibida y prueba preconstituida*, Editorial Trivium, Madrid, 1989.

AVILA MARTÍNEZ, V., «A la deriva con la prueba informática: el Supremo relaja el estándar probatorio de las capturas de 'WhatsApp'» en *Economist&Jurist*, 27 de agosto de 2025.

BANACLOCHE PALAO, «La prueba en el proceso penal» en *Aspectos fundamentales del Derecho Procesal Penal*, Editorial La Ley, 2.ª edición, Madrid, 2011.

BARONA VILAR, S., *Solución extrajurisdiccional de conflictos. Alternative Dispute Resolution (ADR) y Derecho Procesal*, Tirant lo Blanch, Valencia, 1999.

— «Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia» en *Revista Jurídica Digital UANDES*, número 3, 2019.

— *Algoritmización del derecho y de la justicia. De la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, Valencia, 2021.

— «Una justicia «digital» y «algorítmica» para una sociedad en estado de mudanza» en *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar* (Barona Vilar, editora), Tirant lo Blanch, Valencia, 2021.

BARRIO ANDRÉS, M., (dir.) *El Reglamento Europeo de Inteligencia Artificial*, Tirant lo Blanch, Valencia, 2024.

— *Comentarios al Reglamento europeo de Inteligencia artificial*, Editorial La Ley, Madrid, 2024.

BORGES BLAZQUEZ, R., «El sesgo de la máquina en la toma de decisiones en el proceso penal» en *Ius Et Scientia*, volumen 6, número 2, 2020.

— «La inteligencia artificial en el proceso penal y el ¿regreso? de Lombroso», en *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar* (Barona Vilar, editora), Tirant lo Blanch, Valencia, 2021.

BUENO DE MATA, F., —«La utilización de drones como diligencia de investigación tecnológica: consecuencias probatorias» en *Diario La Ley*, número 16, 20 de Marzo de 2018, <https://laleydigital.laleynext.es/>

— «Macrodatos, inteligencia artificial y proceso: luces y sombras», *Revista General de Derecho Procesal*, número 51, 2020,

— «Protección de datos, investigación de infracciones penales e inteligencia artificial: novedades y desafíos a nivel nacional y europeo en la era postcovid» en *La Ley Penal*, número 150, Mayo-Junio 2021, La Ley Digital, de 25 de enero de 2022.

— *Investigación y prueba de delitos de odio en Redes Sociales: Técnicas OSINT e inteligencia policial*, Tirant lo Blanch, Valencia, 2023.

- BUJOSA VADEL, L.M./BUSTAMANTE RÚA, M.M./TORO GARZÓN, L.O.**, «La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia» en *Revista Brasileira de Direito Processual Penal*.
- CALAMANDREI, P.**, *Proceso y democracia*, Editoriales jurídicas Europa-América, Buenos Aires, 1960.
- CALAZA LÓPEZ, S.**, «Protección judicial del derecho a la intimidad informática en su doble dimensión de derecho a la Autodeterminación informativa y derecho al entorno virtual» en *Nuevos postulados de la cooperación judicial en la Unión Europea "Libro homenaje a la profesora M.^a Isabel González Cano*, (Moreno Catena/Romero Prada, dirs.), Tirant lo Blanch, Valencia, 2021.
- CAMPOS ACUÑA, C.**, «El Reglamento de Inteligencia Artificial ya está funcionando: a quién afecta, plazos y sanciones» en *Noticias Jurídicas. Actualidad noticias*, 3 de febrero de 2025, <https://noticias.juridicas.com/actualidad/noticias/19904-el-reglamento-de-inteligencia-artificial-ya-esta-funcionando>.
- CARNELUTTI**, *Derecho y proceso* (traducido por Sentis Melendo), Buenos Aires, 1971.
- CARRASCO DURÁN, M.**, «La definición constitucional del derecho a la tutela judicial efectiva» en *UNED. Revista de Derecho político*, número 107, 2020.
- COLOMER HERNÁNDEZ, I.**, «Control y límites en el uso de la información y los datos personales por parte de la Inteligencia artificial en los procesos penales», en *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar* (Barona Vilar, editora), Tirant lo Blanch, Valencia, 2021.
- COLOMER HERNÁNDEZ, I./OUBIÑA BARBOLLA, S.**, *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*. Aranzadi, Cizur Menor, Navarra, 2015.
- COTINO HUESO, L./SIMÓN CASTELLANO, P.**, *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Aranzadi, Madrid, 2024.
- CUATRECASAS MONFORTE, C.**, «IA: herramienta de investigación criminal» en *La Ley digital*, 24 enero 2024.
- DE HOYOS SANCHO, M.**, «Premisas y finalidades del Libro Blanco sobre Inteligencia Artificial de la Comisión Europea: perspectiva procesal del nuevo marco regulador» en *Justicia algorítmica y Neuroderecho. Una mirada interdisciplinar* (dirigido por Barona Vilar), Tirant lo Blanch, Valencia, 2021.
- «El uso jurisdiccional de los sistemas de inteligencia artificial y la necesidad de su armonización en el contexto de la Unión Europea» en *Revista General de Derecho Procesal*, número 55, 2021.

– «El proyecto de Reglamento de la Unión Europea sobre inteligencia artificial, los sistemas de alto riesgo y la creación de un ecosistema de confianza» en *Justicia poliédrica en periodo de mudanza: Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad* (Barona Vilar (edit.), 2022).

DE LEMUS VARA, F.J., «Límites para el tratamiento de los datos de los no investigados en el proceso penal», en *Uso de la información y de los datos personales en los procesos: los cambios de la era digital*, (Colomer Hernández, dir.), Aranzadi, Cizur Menor, 2022.

DELGADO MARTÍN, J., «Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015» en *Diario LA LEY*, número 693, 2 de febrero de 2016.

– «La prueba digital. Concepto, clases, aportación al proceso y valoración», en *Diario La Ley*, número 6, 11 de abril de 2017, <https://diariolaley.laleynext.es/Content/Documento.aspx>

– «Protección de datos personales y prueba en el proceso» en *Diario La Ley*, número 9383, 2019.

– «Dispositivos de localización y seguimiento en la investigación penal», en «Logos». *Revista Científica del Centro Universitario de la Guardia Civil*, número especial, febrero, 2023.

DE LUIS GARCÍA, E., «Justicia, inteligencia artificial y derecho de defensa», en *Revista de internet, Derecho y política, Monográfico: «Digitalización y algoritmización de la justicia»* (Miró Llinares, dir.), <https://idp.uoc.edu/>

DE URBANO CASTRILLO, E., «El principio de contradicción en el proceso penal», en *Diario La Ley*, número 5474, 4 Feb. 2002.

DURAN SILVA, C., «Aspectos procesales de la videovigilancia practicada por las Fuerzas y Cuerpos de Seguridad del Estado» en *La ley Penal*, número 126, mayo 2017, <https://observatorio-cientifico.ua.es>

ESPARZA LEIBA, I., «La Inteligencia Artificial y el derecho fundamental a la protección de datos de carácter personal», en *Justicia algorítmica y Neuroderecho. Una mirada interdisciplinar* (Barona Vilar, dir.), Tirant lo Blanch, Valencia, 2021, pág. 277 y siguientes.

– «Derecho fundamental a la protección de datos de carácter personal en el ámbito jurisdiccional e inteligencia artificial. En especial la LO 7/2021, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales», en *Inteligencia artificial legal y Administración de justicia* (Calaza López/Llorente Sánchez-Arjona, dir.), Aranzadi, Cizur Menor (Navarra), 2022.

- ESTÉVEZ MENDONZA, L.M.^a**, «Luces y sombras en la protección de datos personales en las investigaciones penales: perspectiva española» en *Investigación y proceso penal en el siglo XXI. Nuevas tecnologías y protección de datos* (Pereira Puigvert y Ordoñez Ponz, dirs.), Editorial Aranzadi, Cizur Menor (Navarra).2021.
- ETXEBERRÍA GURIDI, J.F.** «Videovigilancia y su eficacia en el proceso penal español», en *Cuadernos de Derecho Penal*, febrero de 2014.
- «El uso de sistemas de inteligencia artificial (IA) de identificación biométrica remota en espacios públicos en la ley europea de IA» en *Actualidad Jurídica Iberoamericana*, número 21, agosto 2024.
- FERNÁNDEZ LÓPEZ, M.**, *Prueba y presunción de inocencia*, Editorial Iustel, Madrid, 2005-
- FAGGIANI, V.**, «El derecho a un proceso con todas las garantías ante los cambios de paradigma de la inteligencia artificial», en *UNED. Teoría y Realidad Constitucional*, número 50, 2022.
- FIDOROVA, A.**, «Directiva 2016/680: hacia mayor coherencia de protección de datos personales en la cooperación policial y judicial penal», en *Nuevos postulados de la cooperación judicial en la Unión Europea. Libro homenaje a la profesora M.^a Isabel González Cano* (Moreno Catena/Romero Pradas, dirs.), Tirant lo Blanch, Valencia, 2021.
- FRIAS MARTÍNEZ, E.**, «Ficheros jurisdiccionales. Autoridad de control» en *Diario La Ley*, número 9986, 11 de Enero de 2022, <https://laleydigital-laley-next-es.ezbusc.usc.gal/Content/Documento.aspx>.
- GALLEGO RODRÍGUEZ, P.**, «Los registros biométricos y su aplicación al proceso penal desde una perspectiva constitucional», en *Inteligencia artificial legal y Administración de justicia* (Calaza López/Llorente Sánchez-Arjona, dirs.), Aranzadi, Cizur Menor (Navarra), 2022.
- GAMERO CASADO, E.**, «El enfoque europeo de inteligencia artificial», en *Revista de Derecho Administrativo*, 2021, págs. 268 a 269.
- GARCÍA MARCOS, J.** «Geolocalización y derechos fundamentales» en *El Derecho.com. Noticias jurídicas y de actualidad*, 29 noviembre 2011, <https://elderecho.com/geolocalizacion-y-derechos-fundamentales>
- Hacia una exclusiva reserva jurisdiccional en la protección de derechos a la intimidad», en *Actualidad Civil*, número 4, abril de 2024.
- GASCÓN INCHAUSTI, F.**, «Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial», en *La justicia digital en España y la Unión Europea* (Conde Fuentes/Serrano Hoyo, dirs.), Atelier y Fundación Serra Domínguez, Barcelona, 2019.

GUERRERO PALOMARES, S., «La denominada «prueba de inteligencia policial» o «pericial de inteligencia» en *Revista Aranzadi de Derecho y Proceso Penal*, número 25, 2011.

GIMENO SENDRA, V., «El derecho de defensa» en *Constitución y proceso*, Editorial Tecnos, Madrid, 1988.

– «Libertad de expresión, honor e intimidad personal», *Economist & Jurist*, volumen 17, número 136, 2010.

GÓMEZ COLOMER, J.L., «El aumento de intervencionismo público en la investigación del delito. Una reflexión al hilo del acto de investigación criminal de registro remoto de equipos informáticos (coloquialmente llamado «del gusano informático»)», en *Derecho Probatorio y otros estudios procesales. Liber amicorum Vicente Gimeno Sendra* (Asencio Mellado, dir.), editorial Castillo de Luna Ediciones Jurídicas, Madrid, 2020

– «Unas reflexiones sobre el llamado «juez-robot», al hilo del principio de la independencia judicial» en *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar* (Barona Vilar, editora). Tirant lo Blanch, Valencia, 2021.

– «Derechos fundamentales, proceso e Inteligencia Artificial: una reflexión» en *Inteligencia artificial legal y Administración de justicia*, (Catala López/Llorente Sánchez-Arjona, dirs.), Aranzadi, Cizur Menor (Navarra), 2022.

– *El juez robot. La independencia judicial en peligro*, Tirant lo Blanch, Valencia, 2023.

GONZALEZ CANO, I., «Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680» en *Revista Brasileña de Derecho Procesal Penal*, volumen 5, número 3, 2019.

GONZÁLEZ-CUELLAR SERRANO, N., *Proporcionalidad y derechos fundamentales en el proceso penal*, Colex, Madrid, 1990.

– «Garantías constitucionales en la persecución penal en el entorno digital» en *Derecho y Justicia Penal en el Siglo XXI. Liber amicorum en homenaje al profesor Antonio González-Cuellar García*, Colex, Madrid, 2006.

– «El derecho de defensa y la marca de Caín» en *Nuevos debates en torno a la justicia española* (Castillejo Manzanares, dir.), Editorial Tirant lo Blanch, Valencia, 2017.

GONZÁLEZ LÓPEZ, J.J., «La interacción automatizada por medio de simuladores como medida de investigación penal» en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, número 41, 2016.

- GUTIERREZ ALVIZ CONRRADI, F.**, *El derecho de defensa y la profesión de abogado*, Atelier, 2012.
- GUZMÁN FLUJA, V.**, «Arbitraje y soluciones técnicas inteligentes: elementos para un debate», en *Justicia algorítmica y Neuroderecho. Una mirada interdisciplinar* (Barona Vilar, dir.), Tirant lo Blanch, Valencia, 2021.
- «Proceso penal y justicia automatizada» en *Revista General del Derecho*, número 53, 2021.
 - «Automated justice. La preocupante tendencia hacia la justicia penal automatizada» en *Derecho procesal. Retos y transformaciones* (Bujosa Vadell, dir.), Editorial Atelier, Barcelona, 2021
 - «Consideraciones sobre el alcance objetivo y subjetivo de la Directiva 2016/680» en *Nuevos postulados de la cooperación judicial en la Unión Europea: libro homenaje a la Profesora Isabel González Cano*, (Moreno Catena/Romero Pradas, dirs.), Tirant lo Blanch, Valencia, 2021.
 - «Ideas para un debate sobre la predicción del crimen» en *Inteligencia artificial legal y Administración de Justicia* (Calaza López/Llorente Sánchez-Arjona, Dirs.), Aranzadi, 2022.
- IGLESIAS CANLE, I.**, «Registros biométricos y su aplicación al proceso penal en España e Italia» en *Inteligencia artificial legal y Administración de justicia* (Calaza López/Llorente Sánchez-Arjona, dirs.), Aranzadi, Cizur Menor (Navarra), 2022.
- JIMENEZ CAMPO, J.**, «La garantía constitucional del secreto de las comunicaciones» en *REDC*, número 20, 1987.
- LAFONT NICUESA, L.**, «La policía predictiva más allá de Minority Report», en *Diario LA LEY*, número 10687, 9 de Marzo de 2025.
- LARO GONZÁLEZ, M.E.**, «Principio de proporcionalidad y tratamiento de datos personales en el proceso penal», en *La administración de justicia en España y en América: José Martín Ostos, Liber Amicorum* (Martín Ríos, dir.), Astigi editores, 2021.
- LÓPEZ-BARAJAS PEREA, I.**, «El derecho a la protección del entorno virtual y sus límites: el registro de los sistemas informáticos» en *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas* (Díaz Martínez/López-Barajas Perea, dirs), Tirant lo Blanch, Valencia 2018.
- LÓPEZ-BARJA DE QUIROGA, J.**, *Escuchas telefónicas y prueba ilegalmente obtenida*, Akal, Madrid, 1989.
- LÓPEZ-FRAGOSO ÁLVAREZ, T.**, *Las intervenciones telefónicas en el proceso penal*, Madrid, Colex, 1991.

- LÓPEZ JIMÉNEZ, R.**, «La videovigilancia por las Fuerzas y Cuerpos de Seguridad del Estado: tratamiento de los datos personales» en *Uso de la información y de los datos personales en los procesos: los cambios de la era digital*, (Colomer Hernández, dir.), Aranzadi, Cizur Menor, 2022.
- LÓPEZ YAGÜE, V.**, «La condición de imputado en el proceso penal español. Formas de adquisición y status jurídico que conlleva. Ideas para su reforma» en *La reforma del proceso penal*, Editorial LA LEY, Madrid, 2011.
- MARCOS AYJÓN, M.**, «Captación de imágenes por la policía en el garaje de una comunidad de vecinos. Análisis de la STC 92/2023» en *LA LEY Penal*, número 164, 2023, <https://legalteca-aranzadilaley-es.ezbusc.usc.gal>.
- MARCHENA GÓMEZ, M.**, «Inteligencia artificial y jurisdicción penal», Discurso leído por el Excmo. Sr. Dr. D. Manuel Marchena Gómez en el acto de su recepción como Académico de número de la Real Academia de Doctores de España, <https://confilegal.com/wp-content/uploads/2023/03/INTELIGENCIA-ARTIFICIAL-INGRESO-MARCHENA-REAL-ACADEMIA-DE-DOCTORES-.pdf>
- MARCHENA GÓMEZ, M./GONZÁLEZ-CUELLAR SERRANO, N.**, *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Editorial Castillo de Luna, Madrid, 2015.
- MARTÍN DÍZ, F.**, «Del derecho a la tutela judicial efectiva hacia el derecho a una tutela efectiva de la justicia» en *Revista Europea de Derechos Fundamentales*, número 23, primer semestre 2014.
- «Presunción de inocencia en procesos penales por violencia de género», *Ius et Praxis*, vol. 24, núm. 3, 2018.
 - «Inteligencia artificial y proceso: garantías frente a eficiencia en el entorno de los derechos procesales fundamentales» en *Justicia: ¿Garantías versus Eficiencia?* (Llopis Nadal/Bellido Penadés/Jiménez Conde/De Luis García, coords.) <http://www.tirantonline.com>, 21 de enero 2020.
 - «Herramientas de inteligencia artificial y adecuación en el ámbito del proceso judicial» en *Derecho Procesal. Retos y transformaciones*, Atelier y Fundación Serra Domínguez, Barcelona, 2021.
 - «Modelos de aplicación de Inteligencia Artificial en justicia: asistencial o predictiva versus decisoria» en *Justicia algorítmica y Neuroderecho. Una mirada interdisciplinar* (Barona Vilar, dir.), Tirant lo Blanch, Valencia, 2021.
- MARTÍN MORALES, R.**, *El régimen constitucional del secreto de las comunicaciones*, Civitas, Madrid, 1995.

- MARTÍN RÍOS, P.**, «Empleo de big data y de inteligencia artificial en el ciberpatrullaje: de la tiranía del algoritmo y otras zonas oscuras» en *Revista de los Estudios de Derecho y Ciencia Política*, número 36, octubre 2022, <https://idus.us.es/>
- MARTÍNEZ GALINDO, G.**, «Problemática jurídica de la prueba digital y sus implicaciones en los principios penales» en *Revista Electrónica de Ciencia Penal y Criminología*, <http://criminnet.ugr.es/recpc>
- MARTÍNEZ GARCÍA, J.I.**, «Inteligencia y derechos humanos en la sociedad digital» en *Cuadernos electrónicos de Filosofía del Derecho*, número 40, 2019.
- MÍGUEZ MACHO, L./MARCOS TORRES, C.**, «Sistemas de IA prohibidos y sistemas de IA de alto riesgo» en *El Reglamento Europeo de Inteligencia Artificial* (Barrio Andrés, dir.), Tirant lo Blanch, Valencia, 2024.
- MIRÓ LLINARES, F.**, «Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots», *Revista de Derecho Penal y Criminología*, 3.^a Época, número 20, julio de 2018.
- MORENO CATENA, V.**, *La defensa penal*, Editorial Civitas, Madrid, 1982.
- «Garantía de los derechos fundamentales en la investigación penal» en *Poder Judicial*, número especial II, 1987.
 - «Algunos problemas del derecho de defensa» en *Justicia*, número 3, 1990
 - «La garantía de los derechos fundamentales durante la investigación penal» en *Cuadernos penales José María Lidón*, número 7, 2010.
 - *Fiscalía europea y derechos fundamentales*, Tirant lo Blanch, Valencia, 2014.
 - «Los datos en el sistema de justicia y la propuesta de reglamento UE sobre Inteligencia artificial» en *Uso de la información y de los datos personales en los procesos: los cambios de la era digital*, (Colomer Hernández, dir.), Aranzadi, Cizur Menor, 2022.
- MONTERO AROCA, J.**, *Principios del proceso penal. Una explicación basada en la razón*, Tirant lo Blanch, Valencia, 1997.
- *La intervención de las comunicaciones en el proceso penal. Estudio jurisprudencial*, Tirant lo Blanch, Valencia, 1999.
- MONTESINOS GARCÍA, A.**, «Los algoritmos que valoran el riesgo de reincidencia. En especial, el sistema Viogen» en *Revista Aranzadi de Derecho y Proceso Penal*, número 64, 2021.

MONTÓN REDONDO, A., «Las intervenciones telefónicas constitucionalmente correctas» en *Revista Jurídica La Ley*, número 3915, 1995.

MONTORO SÁNCHEZ, J.A., La obtención y tratamiento de datos de carácter personal con fines penales por la policía judicial» en *Uso de la información y de los datos personales. Uso de la información y de los datos personales en los procesos: los cambios de la era digital*, (Colomer Hernández, dir.), Aranzadi, Cizur Menor, 2022.

NACARINO LORENTE, J.M., «La prevención del delito por las Fuerzas y Cuerpos de Seguridad y su relación con el adelanto de las barreras penales. ¿Dichas actuaciones permiten prevenir el delito y asimismo contribuir a tipificar conductas preparatorias? (1), *Diario La Ley*, número 9740, 20 de Noviembre de 2020, <https://laleydigital-laleynext-es.ezbusc.usc.gal/>

NISA ÁVILA, J.A., «Teoría del Mosaico y Data Mining: análisis jurídico del estado actual en comparativa con la Theory Modular Data Privacy» en *El Derecho.Com Noticias Jurídicas y Actualidad*.

ORTIZ PRADILLO, J.C., «Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos fundamentales en el proceso penal», *La Ley digital*, 25 de enero de 2022.

PECES BARBA MARTÍNEZ, G., *Los valores superiores*, Tecnos, Madrid, 1986.

PEDRAZ PENALVA, E., «El principio de proporcionalidad y su configuración en la jurisprudencia del Tribunal Constitucional y literatura especializada alemana», *Poder Judicial*, número 17, 1990.

PÉREZ GIL, J., «Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal», en *Justicia: ¿garantías versus eficiencia?*, Tirant lo Blanch, Valencia, 2019.

PÉREZ GIL, J./GONZÁLEZ PÉREZ, J.J., La videovigilancia como diligencia de recogida de datos de carácter personal: una reflexión sobre sus repercusiones procesales» en *Videovigilancia. Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de datos personales* (Etxeberría Guridi/Ordeñana Gezuraga, coords.), Tirant lo Blanch, Valencia, 2011

PÉREZ ESTRADA, M.J., *Fundamentos jurídicos para el uso de la inteligencia artificial en los órganos judiciales*, Tirant lo Blanch, Valencia, 2022.

PILLADO GONZÁLEZ, M.E., «Principios generales de protección de datos en la cesión de información en la persecución criminal a la vista de la Directiva 2016/680 del Parlamento europeo y del Consejo, de 27 de abril de 2016, por la que se deroga la Decisión Marco 2008/977», en *Nuevos postulados de la cooperación judicial en la Unión Europea: libro homenaje a la Profesora Isabel González Cano*, (Moreno Catena/Romero Pradas, dirs.), Tirant lo Blanch, Valencia, 2021.

PLANCHADELL GARGALLO, A., *El derecho fundamental a ser informado de la acusación*, Tirant lo Blanch, Valencia, 1999.

RICHARD GONZÁLEZ, M., «Investigación policial en lugares públicos y privados atendiendo al derecho a la intimidad de los ciudadanos investigados. Comentario de la STC 92/2023 de 11 de septiembre, sobre la categoría de los garajes comunitarios respecto del derecho a la intimidad» en *LA LEY Probática*, número 14, 2023.

RODRÍGUEZ FERNÁNDEZ, R., «Protección de datos personales: normativa europea y nacional (especial referencia a la normativa de protección de datos en la prevención, detección, investigación y enjuiciamiento de infracciones penales)» en *La Ley Penal*, número 157, Julio-Agosto 2022, <https://laleydigital-laleynext-es>

RODRÍGUEZ LAINZ, J.L., «La investigación judicial de fraudes cometidos mediante empleo de tecnologías de las comunicaciones», en *Era digital, sociedad y Derecho* (Fuentes Soriano, dir.), Tirant lo Blanch, Valencia, 2020.

— «La nueva doctrina del Tribunal Supremo frente a la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de conservación preventiva de datos de telecomunicaciones» en *Uso de la información y de los datos personales en los procesos: los cambios de la era digital*, (Colomer Hernández, dir.), Aranzadi, Cizur Menor, 2022.

— «La nueva jurisprudencia sobre dispositivos de seguimiento y localización. (Comentario a la STS, Sala 2.ª, 141/2020, de 13 de mayo)» en *La Ley*, número 9650, 2020, *La Ley Digital*, 22/02/2023.

— «Últimos pronunciamientos del Tribunal de Justicia de la Unión Europea sobre cesión de datos de telecomunicaciones para fines de investigación criminal» en *La inteligencia artificial y su aplicación en el sistema de justicia penal* (Noya Ferreiro, dir.), Tirant lo Blanch, Valencia, 2025.

RODRÍGUEZ RAMOS, L., «Intervenciones telefónicas», en *La prueba en el proceso penal*, Cuadernos de Derecho Judicial, CGPJ, Madrid, 1992.

RUÍZ VADILLO, E., «Algunas breves consideraciones sobre el sistema acusatorio y la interdicción constitucional de toda indefensión en el proceso penal» en *Diario La Ley*, tomo 4, 1987.

SAN MIGUEL DEL CASO, C., «Inteligencia artificial y algoritmos: la controvertida evolución de la tutela judicial efectiva en el proceso penal» en *Estudios Penales y Criminológicos*, 44, 2023, <https://doi.org/10.15304/epc.44.8859>,

SANTOS SÁNCHEZ, D.J., «Los tratamientos de datos personales para la prevención, investigación, detección o enjuiciamiento de infracciones penales: consideraciones de la AEPD» en *Investigación y proceso penal en el siglo XXI. Nuevas tecnologías y protección de datos* (Pereira Puigvert/Ordoñez Ponz, dirs), Editorial Aranzadi, Cizur Menor, 2021.

SCHUMANN BARRAGÁN, G., «La inteligencia artificial aplicada al proceso penal» en *Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos* (Pereira Puigvert/Ordóñez Ponz, dir.), Aranzadi, Cizur Menor, 2021.

SERRANO ACITORES, A., Consideraciones éticas y legales en el uso de la inteligencia artificial: el enfoque de la unión europea, en *Revista de Fiscalidad Internacional y Negocios Transnacionales*, número 24, 2023, <https://soluciones-aranzadilaley-es.ezbusc.usc.gal/Content/Documento.aspx>.

SERRANO RUIZ-CALDERÓN, J.M., «El derecho de defensa según la sentencia 79/2012 de la Sala de lo Penal del Tribunal Supremo» en *Diario La Ley*, número 7850, 3 mayo, 2012

SOLAR CAYÓN, J.I., «Inteligencia artificial en la justicia penal: los sistemas algorítmicos» en *Dimensiones éticas y jurídicas de la Inteligencia artificial en el marco del Estado de Derecho*, Cuadernos de la Cátedra de Democracia y Derechos Humanos, 16, Universidad de Alcalá, Defensor del Pueblo, 2020.

— «Reflexiones sobre la aplicación de la Inteligencia artificial en la Administración de justicia» en *Teoría jurídica contemporánea*, volumen 6, 2021.

SUAREZ XAVIER, P.R., «Policía predictiva: entre seguridad y garantías fundamentales» en *Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos* (Pereira Puigvert/Ordóñez Ponz, dir.), Aranzadi, Cizur Menor, 2021.

VELASCO NÚÑEZ, E., «La captación de la imagen de lugares y personas como medio de investigación penal» en *El Derecho.com. Noticias jurídicas y actualidad*, 25 enero 2011. <https://elderecho.com/la-captacion-de-la-imagen-de-lugares-y-personas-como-medio-de-investigacion-penal>

— «Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica» en *Diario LA LEY*, número 8183, 4 de noviembre de 2013.

— «Investigación penal y protección de datos» en *El Cronista del estado Social y Democrático de Derecho*, número 88-89, 2020.

– «Investigación penal y protección de datos, tecnología y proceso, en *Problemas procesales en un mundo digital* (Fuentes Soriano, coord.), Aranzadi, Cizur Menor, 2022.

ZARAGOZA TEJADA, J.I., «La geolocalización del investigado en el proceso penal», en *Revista Aranzadi Doctrinal*, número 2, febrero 2025.



LA EDITORIAL JURÍDICA DE REFERENCIA PARA
LOS PROFESIONALES DEL DERECHO **DESDE 1981**



Paso a paso

Códigos
comentados

Vademecum



Formularios



Flashes
formativos



Colecciones
científicas

DESCUBRA NUESTRAS OBRAS EN:

www.colex.es

Editorial Colex SL Tel.: 910 600 164 info@colex.es

INTELIGENCIA ARTIFICIAL E INVESTIGACIÓN PENAL

El recurso a los instrumentos tecnológicos relacionados con los sistemas de IA es habitual en el campo científico, empresarial, social y en el ámbito jurídico. El sistema de justicia penal no es ajeno a estas nuevas técnicas, que se incorporan en la investigación incluso antes del inicio de la instrucción, a través de actuaciones policiales, que, en muchas ocasiones, van a proyectar su eficacia en el proceso. Su aplicación en el proceso penal ha llevado a profesores universitarios y profesionales jurídicos a colaborar en un Proyecto de investigación I+D «Inteligencia artificial, Justicia y Derecho: ¿irrupción o disrupción tecnológica en el proceso penal?». Del trabajo realizado deriva esta monografía, centrada en las garantías que deben rodear la investigación policial preprocesal, como paraguas para la protección de derechos fundamentales, y en los requisitos que han de presidir la incorporación de los resultados al proceso. Para ello se ha partido de un primer análisis del marco legislativo aplicable, y del examen de la protección de los derechos fundamentales relacionados con la vida privada y aquellos de naturaleza procesal. A continuación, se lleva a cabo una aproximación al estudio de la investigación policial y sus límites, para finalizar planteando algunas cuestiones sobre la eficacia de estas medidas policiales en el proceso, centrando la atención en la aplicación del principio de proporcionalidad y del control judicial como presupuestos de su válida incorporación.



MARÍA LOURDES NOYA FERREIRO

Doctora en Derecho por la Universidad de Santiago de Compostela, miembro del Consejo del Centro Integral de Análisis y Resolución de Conflictos (CIARCUS), del Consejo del Instituto Alonso Martínez de Justicia y Litigación, Universidad Carlos III de Madrid.

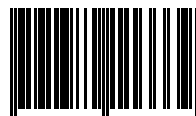
Centra su investigación en el estudio de diligencias de investigación tecnológica, trata de seres humanos, violencia de género, prueba en el proceso civil y administrativo, el pleito testigo, y la aplicación de la Inteligencia Artificial. Ha publicado varias obras como «La intervención de comunicaciones orales directas en el proceso penal», «Las diligencias finales en el proceso civil», «El derecho de defensa y la intervención de las comunicaciones de los abogados», «La protección de las mujeres víctimas de tráfico ilegal con fines de explotación», o «El pleito

testigo en el proceso civil y en el proceso administrativo». Ha participado como investigador principal y miembro en proyectos de investigación del Ministerio de Ciencia, Innovación y Universidades y de la Xunta de Galicia.

Ha sido Secretaria General de la USC y Juez de Primera Instancia e Instrucción en provisión temporal en los Juzgados de Caldas de Reyes (Pontevedra) y Noya (A Coruña) desde 1986 a 1990.



ISBN: 979-13-7011-333-9



9 791370 113339