VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

TRABAJO FIN DE GRADO

GRADO EN DERECHO

Departamento: Derecho Administrativo, Financiero y Procesal

Área de conocimiento: Derecho Procesal

Curso 2021/2022

DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICA: especial referencia a la biometría en delitos de terrorismo.

ALEX MORENO CARRASCO

Tutor: FEDERICO BUENO DE MATA

JUNIO 2022

TRABAJO FIN DE GRADO

GRADO EN DERECHO

Departamento: Derecho Administrativo, Financiero y Procesal

Área de conocimiento: Derecho Procesal

DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICA: especial referencia a la biometría en delitos de terrorismo.

TECHNOLOGICAL INVESTIGATION PROCEDURES: special emphasis on biometrics applied to terrorism.

Nombre del/la estudiante: ALEX MORENO CARRASCO
e-mail del/a estudiante: alexmcarrasco@usal.es

Tutor/a: FEDERICO BUENO DE MATA

RESUMEN

La era de la revolución industrial en que nos encontramos ha transformado diversos ámbitos de nuestras vidas, incluyendo el de la Administración de Justicia. Estas innovaciones tecnológicas han puesto de manifiesto la necesidad de actualizar nuestra vetusta Ley de Enjuiciamiento Criminal para adaptar el Derecho Procesal Penal español a las nuevas exigencias de la sociedad contemporánea, lo cual se materializó finalmente en la vigente 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. De la mano de esta reforma, se introdujeron un gran número de diligencias de investigación tecnológica, las cuales resultan ciertamente invasivas de algunos de los derechos fundamentales consagrados en nuestro texto constitucional. A la vanguardia de estas diligencias de investigación tecnológica, encontramos las técnicas biométricas, las cuales han sido empleadas para luchar contra la lacra del terrorismo.

PALABRAS CLAVE (entre 3 y 6): diligencias de investigación, biometría, terrorismo, reconocimiento facial, videovigilancia, proceso penal.

ABSTRACT

The Industrial Revolution Era in which we find ourselves has transformed multiple aspects of our lives, even including the Administration of Justice. The technological innovations have made clear the need to update our old-fashioned Criminal Procedure Law in order for the Spanish Criminal Procedure Law to adapt to the new demands of contemporary society, which has finally materialised in the current Organic Law 13/2015 of 5th October, modification of the Law of Criminal Procedure for the strengthening of procedural guarantees and the regulation of technological investigation measures. Hand in hand with this reform, many technological investigation procedures were introduced, which are certainly invasive of some of the fundamental rights enshrined in our constitutional text. At the forefront of these technological investigation procedures, we find biometric techniques being used as well to fight against the ongoing scourge of terrorism.

KEYWORDS: investigation procedures, biometrics, terrorism, facial recognition, video surveillance, criminal proceeding.

ÍNDICE

ABREVIATURAS

ADN: Ácido desoxirribonucleico

Art: Artículo

CE: Constitución española

CP: Código Penal

EE. UU.: Estados Unidos

ETA: Euskadi ta Askatasuna

FFCCSE: Fuerzas y Cuerpos de Seguridad del Estado

FBI: Federal Bureau of Investigations

FIRST: Facial, Imaging, Recognition, Searching, and Tracking

LECrim: Ley de Enjuiciamiento Criminal

LO: Ley Orgánica

RGPD: Reglamento General de Protección de Datos

S.A.: Sociedad Anónima

STC: Sentencia del Tribunal Constitucional

STJUE: Sentencia del Tribunal de Justicia de la Unión Europea

STS: Sentencia del Tribunal Supremo

TEDH: Tribunal Europeo de Derechos Humanos

TFG: Trabajo de Fin de Grado

1. Introducción.

La presencia de recursos tecnológicos en nuestra sociedad ha aumentado de manera exponencial en los últimos lustros, acentuándose especialmente en el escenario de crisis sanitaria propiciado por el virus SARS-CoV-19[1], donde hemos atisbado cómo los avances tecnológicos han supuesto una transformación radical de nuestras dinámicas sociales. El Derecho, como no podría ser de otro modo, no es ajeno a la realidad social que nos circunda, sino que avanza en la misma dirección que ésta, por lo que la mayor incidencia de la tecnología en nuestra vida cotidiana se ha trasladado, análogamente, al campo de la Administración de Justicia.

El desarrollo de las nuevas tecnologías a las que acabo de hacer referencia ha portado consigo nuevas formas de ataque a los bienes jurídicos, así como una mayor comisión de hechos delictivos a través de dichas tecnologías. Ello, irremediablemente, ha evidenciado la necesidad de adaptar nuestras diligencias de investigación a las nuevas exigencias criminales, pues si los sujetos cuentan con medios técnicos innovadores de gran eficacia para conseguir una afección de los bienes jurídicos, paralelamente, las Fuerzas y Cuerpos de Seguridad del Estado (en lo sucesivo, FFCCSE) necesitan contar con medios igualmente innovadores y eficaces para poder dar respuesta a estas nuevas modalidades de ataque. Sólo en este sentido resulta posible cumplir con la doble finalidad que caracteriza la fase de instrucción de nuestro proceso penal: el esclarecimiento de los hechos punibles y la determinación de la culpabilidad de los presuntos autores.

En efecto, la exigencia de una actualización digital de la justicia española se ha hecho patente en las últimas décadas materializándose, finalmente, en la introducción de la LO 13/2015, que vino a modificar nuestra obsoleta LECrim y a regular el fortalecimiento de las garantías procesales y de las medidas de investigación tecnológica. Así, a través de esta nueva ley –vigente desde finales de 2015– se actualizaron las denominadas *diligencias de investigación tecnológica*, situadas en el Título VIII del Libro II de la actual LECrim.

Al haber sido incorporadas estas diligencias de investigación tecnológica, ahora ya es posible hablar de la presencia de técnicas como la biometría empleada como una diligencia en los procesos penales. Es por esta razón por la que realizaré un estudio de las

[1] Del inglés *severe acute respiratory syndrome Coronavirus 2019*.

diferentes diligencias de investigación tecnológica que conforman nuestro ordenamiento jurídico, así como de la biometría como diligencia de investigación tecnológica, detallando en ambos casos el funcionamiento de cada una de ellas para lograr un profundo entendimiento de esta materia.

En relación con la regulación positiva de estas diligencias, ésta vino marcada por su carácter ineludible, pues resultan ciertamente restrictivas de derechos tildados de "fundamentales" en nuestro texto constitucional[2], como son el derecho al honor, al secreto de las comunicaciones, a la intimidad personal y familiar, a la inviolabilidad del domicilio y a la propia imagen, consagrados en el artículo 18 CE, así como el derecho a la tutela judicial efectiva recogido en el tenor literal del art. 24.1 del mismo texto legal. Esto ha hecho necesario una regulación detallada de estas diligencias para garantizar el escrupuloso respeto de los derechos fundamentales.

En este sentido, tanto las diligencias de investigación tecnológica en general, como las técnicas biométricas como diligencias de investigación en particular pueden causar graves afecciones de derechos fundamentales, ya que acceden a datos tan sensibles como los pertenecientes a la privacidad de las comunicaciones telefónicas, por ejemplo, lo que hace preceptiva la autorización judicial en la mayor parte de los casos. Como consecuencia, expondré a lo largo de este trabajo la gran controversia que han suscitado este tipo de diligencias, pues resultan tan intrusivas que es necesario ponderar el interés público en contraposición con el perjuicio individual causado. Ello ha generado abundante jurisprudencia en nuestros tribunales, los cuales han perfilado la licitud o ilicitud de la injerencia que estas medidas tienen en los derechos fundamentales (en adelante, DDFF) del investigado.

Por último, centraré mi atención en el empleo de la biometría como medio de identificación de presuntos terroristas gracias a la existencia de bases de datos biométricos que permiten cotejar los datos biométricos incorporados a la propia base de datos con los obtenidos de un individuo, por ejemplo, en un control aduanero.

No obstante, resulta necesario subrayar que la biometría no sólo se aplica de forma fructífera en casos de los delitos de terrorismo, sino que es de aplicación para identificar

[2] BUENO DE MATA, F. DEL, "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 [BOE n. o 239, 6-X-2015]", *Ars Iuris Salmanticensis*, 2016, p. 1.

presuntos criminales en gran parte de los ilícitos tipificados en nuestro Código Penal. Ello, no obstante, he decidido acotar mi campo de estudio a los delitos de terrorismo, pues considero que la aplicación de la biometría en esta materia resulta particularmente provechosa e innovadora, máxime teniendo en cuenta las peculiaridades que presenta el tratamiento procesal de los autores de un delito de terrorismo: estamos, en mi opinión, aplicando un Derecho Procesal Penal a aquellos sujetos que -paradójicamente- se declaran enemigos de un Estado de Derecho, pues su fin no es atentar contra la vida e integridad física de cientos de personas por el mero hecho de acabar con ellas, sino subvertir el orden constitucional. Ello constituye una explicación a que, en el estudio pormenorizado de estos delitos, hallemos la concurrencia de "reglas especiales" en la investigación o incluso en la prisión preventiva de los presuntos autores de un delito de terrorismo como puede ser, por ejemplo, la aplicación forzosa de la técnica de frotis bucal para la obtención de muestras de ADN y la posibilidad de acceder a un domicilio o incluso de llevar a cabo intervenciones telefónicas sin autorización judicial.

Para el estudio de todas estas cuestiones, la metodología jurídica aplicada ha consistido en la lectura de abundante literatura jurídica como se recoge en la bibliografía, contrastada con información de diversos recursos web y complementada con pronunciamientos jurisprudenciales de nuestros tribunales, pues al ser un tema relativamente reciente y en continua innovación ha sido crucial la consulta de jurisprudencia para una comprensión íntegra de la materia.

Teniendo en cuenta lo expuesto, el objeto de estudio del presente Trabajo de Fin de Grado no sólo me resulta atractivo, sino que estamos ante una cuestión contemporánea cuyo conocimiento -a pesar de no ser abordado en profundidad en las aulas- resulta indispensable, pues la justicia debe posicionarse en la vanguardia, evitando quedarse obsoleta y contemplando todos estos medios de investigación desde una óptica garantista y respetuosa con los DDFF del investigado.

En definitiva, este Trabajo de Fin de Grado tiene por objeto el estudio circunstanciado de las diferentes diligencias de investigación, con especial atención a la biometría como diligencia de investigación empleada para satisfacer los fines de la fase instructora de nuestro proceso penal español, especialmente en lo que respecta a la prevención de delitos de terrorismo.

2. Marco teórico de las diligencias de investigación en el proceso penal español.

La investigación penal se fundamenta en una amalgama de diligencias de investigación cuyo fin es esclarecer los hechos delictivos y las circunstancias en las que estos acaecieron, al mismo tiempo que queda probado que el sujeto investigado es efectivamente el autor de los hechos delictivos[3].

No obstante, la era tecnológica en la que vivimos actualmente ha supuesto la implantación de la tecnología en el proceso penal, lo cual ha significado un cambio cuantitativo y cualitativo en la investigación procesal penal, ya que contamos con más medios de investigación y dotados de una mayor eficiencia. A este respecto, interesa realizar un estudio pormenorizado de las diferentes diligencias de investigación tecnológica recogidas en nuestra moderna LECrim.

2.1. Rasgos comunes de las diligencias de investigación tecnológica: régimen común.

Por lo que respecta a la regulación de las diligencias de investigación tecnológica, nuestra vigente LECrim presenta un régimen común general contenido en los artículos 588 bis a) a 588 bis k), el cual tiene un carácter subsidiario con respecto de las regulaciones específicas que analizaré detenidamente en el siguiente apartado.

Esta regulación general contenida en el citado articulado posibilita el acuerdo de las medidas de investigación tecnológica previstas en nuestra LECrim de oficio o bien a instancia de la Policía Judicial o Ministerio Fiscal[4] previa autorización judicial sujeta a los principios rectores de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad[5]. Realizada la petición, en un plazo máximo de veinticuatro horas, el Juez de Instrucción dicta auto motivado -oído el Ministerio Fiscal- autorizando o denegando la medida de investigación solicitada[6] y, en caso de autorizarla, será el Juez Instructor quien controle el desarrollo y los resultados de tal medida[7].

[3] MORENO CATENA, V., "Garantías de los derechos fundamentales en la investigación penal", *Revista del Poder Judicial*, número 2, 1988, p. 131

[4] Vid. Art. 588 bis b) 1 LECrim.

[5] Vid. Art. 588 bis a) 1 LECrim.

[6] Vid. Art. 588 bis c) 1 LECrim.

[7] Vid. Art. 588 bis g) LECrim.

Por lo que se refiere a la duración de la medida de investigación tecnológica, la propia ley prevé que tendrán la duración que se especifique para cada una de ellas, sin exceder el tiempo imprescindible para el esclarecimiento de los hechos[8], pudiendo prorrogarse mediante auto motivado, de oficio por la autoridad judicial o bien a petición del Ministerio Fiscal o de la Policía Judicial[9], empezando a computar la prórroga en la fecha de expiración del plazo que inicialmente se acordó.[10]

Por último, cabe mencionar que este régimen general prevé la destrucción de los registros originales que consten en los sistemas electrónicos e informáticos que se hubieran utilizado para ejecutar la medida[11], conservándose una copia custodiada por el Letrado de la Administración de Justicia, la cual será destruida una vez transcurridos cinco años desde la ejecución de la pena, cuando la pena o delito hayan prescrito, se haya dictado sentencia absolutoria firme o bien se haya decretado sobreseimiento libre.

Sin embargo, debemos criticar que la actual LECrim no garantiza la destrucción de las copias que hubieran sido entregadas a las partes[12], lo que implica una destrucción meramente parcial o defectuosa de los registros.

2.2. Regulaciones específicas: la tipología de las diligencias de investigación tecnológica.

2.2.1. Interceptación de comunicaciones.

Aunque esta diligencia de investigación escapa, en cierto modo, de las innovadoras técnicas biométricas que analizaré posteriormente en profundidad, ya que la interceptación de comunicaciones utiliza tecnologías que resultan mucho más naturales, considero preciso mencionarla y realizar un estudio de la misma ya que es una diligencia muy utilizada para el esclarecimiento y persecución de diversos ilícitos como, por ejemplo, los delitos de tráfico de drogas tipificados en los artículos 368 a 377 del Código Penal.

[8] Vid. Art. 588 bis e) 1 LECrim.
[9] Vid. Art. 588 bis e) 2 LECrim
[10] Vid. Art. 588 bis f) 3 LECrim
[11] Vid. Art. 588 bis k) 1 LECrim.
[12] VEGAS TORRES, J., "Las medidas de investigación tecnológica", *Nuevas tecnologías y derechos fundamentales en el proceso*, 2017, p. 47.

Estamos, en este caso, ante un acto investigatorio que conlleva una gran injerencia en el derecho fundamental del secreto de las comunicaciones. En este sentido, ante un hecho punible que revista especial gravedad, el Juez de Instrucción puede acordar mediante auto motivado que la Policía Judicial proceda al registro y/o grabación de las comunicaciones del sujeto investigado durante el tiempo que resulte imprescindible para preconstituir la prueba que desvirtúe la presunción de inocencia del investigado y pueda demostrar su participación en los hechos delictivos.[13]

El Juez, sin embargo, sólo autorizará la interceptación de las comunicaciones telefónicas y telemáticas cuando la investigación tenga por objeto delitos dolosos castigados con una pena con límite máximo de al menos tres años de prisión, delitos cometidos en el seno de un grupo u organización criminal, delitos de terrorismo, delitos cometidos a través de instrumentos informáticos o a través de tecnologías de la información o la comunicación o servicio de comunicación.[14]

Junto a esto, hay que tener en cuenta la observancia de los principios rectores, concretamente el de proporcionalidad, que se podrá justificar en atención a la gravedad de los hechos, 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, y todo ello siempre que el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros.[15] De este modo, el legislador confecciona un marco legal mínimo dentro del cual el Juez tendrá que valorar la concurrencia de los principios rectores consagrados en el art. 588 bis a LECrim y, de respetarse tales principios, la injerencia a los derechos contemplados en el art. 18 CE estará permitida.[16]

Así, con carácter general, podemos concluir que no va a ser posible adoptar esta medida de investigación tecnológica cuando nos encontremos ante un delito leve cometido a través de instrumentos informáticos o tecnologías de la información o

[13] GIMENO SENDRA, V., "Las intervenciones telefónicas en la jurisprudencia del Tribunal Constitucional y del Tribunal Supremo", *Diario la Ley,* 1996, p.1

[14] Vid. Art. 588 ter a LECrim

[15] Vid. Art. 588 bis a 5 LECrim

[16] Así, la STC 25/2011 14 de marzo, establece que la práctica de intervenciones telefónicas -aun cuando se desconozca cómo la Policía obtuvo número de teléfono del investigado- no conlleva una lesión del derecho al secreto de las comunicaciones (art. 18.3. CE) ni del derecho a la intimidad (art. 18.1 CE), sino que nos hallamos ante una injerencia en la intimidad de carácter leve que responde a un fin legítimo, por lo que puede considerarse como una diligencia de investigación proporcionada al constituir un medio idóneo para un fin legítimo.

comunicación, ni tampoco en caso de que hubieran sido cometidos en el seno de una organización o grupo criminal.[17] Ello resulta, en mi opinión, una configuración razonable, en tanto que la comisión de un delito menos leve difícilmente presenta una entidad suficiente como para satisfacer las exigencias del principio de proporcionalidad.

No obstante, cabe señalar que sí tendrán cabida injerencias menores como, por ejemplo, acceder a determinados datos de tráfico vinculados al investigado, lo cual también supondrá -paralelamente- una menor exigencia de los hechos delictivos que justifican la adopción de la medida, pero exigiéndose siempre una decisión judicial con una fundamentación reforzada.[18]

Por otra parte, y atendiendo a las directrices de la Circular 2/2019 anteriormente citada, los delitos conexos no van a suponer una autorización de esta diligencia en todo caso, sino que sólo estaría justificada la injerencia cuando el delito conexo se fundamente en el ilícito principal, sin perjuicio de que se valore el delito conexo que se haya hallado casualmente, pero, en todo caso, sin que quepa posibilidad de acordar esta diligencia de investigación ni prorrogarla con fundamento en el delito conexo si llegara a desaparecer el delito que justificaba la adopción de la medida.

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

Esta diligencia de investigación tecnológica es lo que, coloquialmente, se conoce como "escucha ambiental". En este caso, estamos ante una medida consistente en colocar y utilizar dispositivos electrónicos con el fin de captar y grabar comunicaciones orales directas que el investigado haya mantenido, bien sea en la vía pública o incluso en un lugar cerrado como puede ser, por ejemplo, su domicilio[19].

[17] Circular 2/2019, de 6 de marzo, de la Fiscal General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas.

[18] En este sentido, la STJUE de 2 de octubre 2018 (asunto C-207/16) ha mantenido que la injerencia en el derecho fundamental de un sujeto al acceder a estos danos no revista una gravedad suficiente como para limitar dicho acceso exclusivamente a la delincuencia grave ECLI:EU:C:2018:788, accesible en: https://curia.europa.eu/juris/document/document.jsf?text=&docid=206332&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=5522740

[19] Vid. Art. 588 quater a) 1. LECrim

Ello supone, y así se deduce del propio artículo, que esta diligencia de investigación tecnológica no se refiere al hecho de captar y grabar comunicaciones orales espontáneamente, sino que lleva aparejada toda una actuación previa consistente en colocación de dispositivos electrónicos destinados a tal fin, lo cual se traduce en una importante injerencia no sólo en el derecho al secreto de las comunicaciones y a la intimidad de la persona investigada, sino incluso en el derecho a la inviolabilidad del domicilio, lo cual hace preceptiva la autorización judicial[20] en caso de que el dispositivo electrónico se coloque en el interior del domicilio.

Con respecto al derecho a la intimidad, es indiferente que la captación o grabación de comunicaciones orales se produzca en vía pública o en el domicilio, pues nuestro derecho a la intimidad no se condiciona a que nos encontremos en un espacio público o privado, de manera que nuestra intimidad también puede verse vulnerada en la vía pública, por ejemplo, mediante una utilización inadecuada de micrófonos direccionales o el uso de cualquier otra tecnología que resulte invasiva de las conversaciones orales que puedan mantener los transeúntes.[21] No obstante, nuestra jurisprudencia matiza que la captación y grabación de comunicaciones espontáneas en un espacio público por un funcionario que se encuentre próximo a quienes conversan excluye cualquier tipo de consideración de atentado al derecho a la intimidad del comunicante[22].

Por lo que se refiere al derecho al secreto de las comunicaciones, es ilustrativo de la gran afección que esta diligencia de investigación tecnológica comporta en este derecho fundamental el hecho de que, con anterioridad a la reforma de 2015, la colocación de micrófonos en una celda policial fuera declarada nula a pesar de contar con autorización judicial para ello.[23] Esto fue así porque existía una carencia de habilitación legal, ya que esta medida de investigación no contaba con una regulación específica en nuestra anterior LECrim. Por ello, el Tribunal Constitucional consideró que la injerencia de esta medida en el derecho al secreto de las comunicaciones necesitaba no sólo una autorización judicial sino también una habilitación legal, puesto que la reserva de ley "constituye el

[20] SANTOS MARTÍNEZ, A. M., *Medidas de investigación tecnológica en la instrucción* penal, Bosh-Wolters Kluwer, Barcelona 2017, p. 191.

[21] MARTÍN MORALES, R., *El régimen constitucional del seguimiento directo de personas*, Comares, Granada, 2015, p. 15

[22] STS de 5 de marzo de 2007

[23] STC 145/2014 de 22 de diciembre de 2014

único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas."

Por último, es preciso destacar la injerencia de esta diligencia en el derecho fundamental a la inviolabilidad del domicilio. Con respecto a esto, es una diligencia que supone una injerencia mucho más intensa que la interceptación de comunicaciones, ya que cabe la posibilidad de situar los dispositivos electrónicos en el domicilio del investigado, es decir, en un espacio concebido y configurado para el desarrollo de su intimidad. A este respecto, el apartado segundo del art. 588 quater a) LECrim exige que, en caso de que sea necesario acceder al domicilio del investigado o en algún otro espacio destinado al ejercicio de la privacidad para colocar un dispositivo electrónico, será necesario que la autorización judicial extienda su motivación a la procedencia del acceso a dichos lugares.

De esta manera, resulta palmario que nuestras expectativas de intimidad cuando nos encontramos en el domicilio propio son mayores que cuando mantenemos una conversación a través de un teléfono o cualquier otro dispositivo tecnológico.[24] Es en este mismo sentido en el que se han pronunciado nuestros tribunales al establecer que, si el dispositivo electrónico se coloca en el domicilio del investigado, la injerencia es mucho mayor puesto que no sólo afecta al investigado, sino a toda la unidad familiar.[25]

2.2.3. Videovigilancia en el proceso penal.

La videovigilancia en el proceso penal se regula, concretamente, en el art. 588 quinquies a) LECrim, que permite la captación de la imagen en lugares y espacios públicos mediante la utilización de dispositivos técnicos.

Esta captación de la imagen, sin embargo, está dispensada de autorización judicial alguna siempre que se realice en lugares o espacios públicos, pues nuestra jurisprudencia entiende que es un acto legítimo y no vulnerador de los derechos fundamentales del investigado[26]. No va a ser así cuando el investigado objeto de grabación se encuentre en

[24] GONZÁLEZ-CUÉLLAR SERRANO, N., MARCHENA GÓMEZ, M., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Castillo de Luna, Madrid, 2015, p. 337.
[25] Sentencia de 10 de abril del Juzgado de lo Penal nº 1 de Huesca
[26] STS de 13 de marzo de 2003

un lugar o espacio privado[27], en cuyo caso sí que va a ser preceptiva la autorización judicial, como consecuencia de la afectación de derechos fundamentales del art. 18 CE.

Nuestros tribunales, además, han examinado la instalación de cámaras desde el punto de vista de la injerencia en el derecho fundamental a la intimidad del investigado. Así, el Tribunal Supremo cuenta con jurisprudencia consolidada sobre el uso de cámaras de videovigilancia y estima que la mera colocación de un distintivo informático genérico con la frase "zona videovigilada" sin especificar la finalidad de éste resulta suficiente para justificar la limitación del derecho fundamental del sujeto, por lo que, si es una medida necesaria, justificada, idónea y equilibrada, se descartará que se haya lesionado el derecho a la intimidad personal recogido en el art. 18.1 de nuestro texto constitucional.

En este sentido, el Tribunal Constitucional ha considerado legítima la colocación de una cámara por parte del empresario puesto que la cámara simplemente grababa el espacio comprendido en la caja registradora tras haber percibido grandes desajustes de contabilidad. Según el criterio de nuestro Tribunal Constitucional, una medida como ésta no debe concebirse como arbitraria, pues en estos casos no se pretende vigilar la conducta del trabajador con carácter general, sino que se pretende observar su conducta laboral tras haberse detectado ciertas irregularidades con el único fin de verificar fundadas sospechas de que se estuviera llevando a cabo un hecho ilícito.[28] Este mismo criterio jurisprudencial ha sido ampliamente aplicado en lo sucesivo.[29]

Por último, es preciso destacar que la ley no prevé nada con respecto a la duración de esta medida de investigación tecnológica, por lo que resulta de aplicación el régimen general de la LECrim expuesto anteriormente, a excepción de los supuestos en que los integrantes de las FFCCSE sean quienes practican la videovigilancia, en cuyo caso se necesitará una autorización judicial previa que posibilite la captación indiscriminada de imágenes en sitios públicos, sin ser preceptiva en casos en que la videovigilancia se dirija

[27] Así lo afirma la Circular 4/2019, de 6 de marzo, donde se dispone que el concepto de lugar privado debe ser considerado atendiendo a "la perspectiva de la privacidad y del ejercicio del derecho a la intimidad", de manera que este lugar protegido por la inviolabilidad domiciliaria o por generar una razonable expectativa de privacidad (por ejemplo, el aseo de un establecimiento público) determinará la naturaleza y el alcance de la medida.

[28] STC 39/2016 de 3 de marzo de 2016

[29] Ejemplos de ello son la STS de 31 de enero de 2017 donde se afirma que cuando el trabajador conoce que se ha instalado un sistema de control por videovigilancia no es preceptivo especificar "la finalidad exacta que se le ha asignado a ese control", al igual que las SSTS de 1 de febrero de 2017, y 2 de febrero de 2017, entre otras.

a registrar, vigilar o realizar un seguimiento de sospechosos que hayan podido realizar alguna actividad delictiva[30].

2.2.4. Dispositivos técnicos de seguimiento y localización (balizas o *beepers*).

Esta medida de investigación tecnológica, regulada en el art. 588 quinquies b) y c) de la LECrim, consiste en instalar un dispositivo técnico que permite conocer la posición geográfica del investigado[31]. Así, permite controlar la posición del investigado incluso en el interior de espacios privados, lo que la hace una medida altamente intrusiva de derechos fundamentales, con especial injerencia en el derecho a la intimidad, lo cual hace preceptiva la previa autorización del juez competente especificando qué medio técnico se va a emplear.[32]

Esta diligencia debe estar muy bien perfilada, pues una medida de investigación de este tipo como, por ejemplo, la instalación de dispositivos de GPS en el vehículo del investigado, supone una afectación del derecho a la intimidad y -si se transcienden los límites tolerados e inobservan los principios rectores- puede suceder que la prueba devenga ilícita[33]. No obstante, el TEDH ha mantenido que ciertos ordenamientos jurídicos -como el alemán- que ni siquiera exigen autorización judicial para la adopción de esta medida no vulneran los principios del Convenio de Roma, siempre y cuando se defina legalmente la limitación temporal y se respete el principio de proporcionalidad[34].

Nuestra jurisprudencia nacional también ha avalado el empleo de estas técnicas sin autorización judicial con anterioridad a la reforma de 2015 y en casos muy concretos como, por ejemplo, en el supuesto de colocación de una baliza en el exterior de un barco para realizar el seguimiento de una embarcación en alta mar como consecuencia de fundada sospecha de tráfico de estupefacientes. Ello es así porque, al entender de nuestra jurisprudencia, la colocación de un dispositivo de seguimiento y localización en el exterior del barco no supone injerencia alguna en el derecho a la intimidad

[30] ARRABAL PLATERO, P., "Las diligencias de investigación tecnológica en el proceso penal español", *Revista de Ciencias Sociales: Facultad de Derecho*, 2020, p. 90.

[31] LÓPEZ-BARAJAS PEREA, I., "Aplicación de las tecnologías de la información y de la comunicación a la investigación criminal: la reforma de la Ley de Enjuiciamiento Criminal Española de 2015", *Sistemas, cibernética e informática*, 2016, p. 166.

[32] Vid. Art. 588 quinquies b) 2 LECrim.

[33] Caso United States v. Antoine Jones, 565 US

[34] Caso Uzun v. Alemania, 35623/05, TEDH 2010

constitucionalmente protegido[35], siempre y cuando no haya sido necesario acceder a un lugar reputado domicilio[36] para colocar los dispositivos de seguimiento y localización, ni haya supuesto una injerencia en las conversaciones o en cualquier otro derecho fundamental de los investigados.

De manera similar, el Tribunal Supremo ha argumentado que el uso de balizas de seguimiento no vulnera el derecho fundamental al secreto de las comunicaciones ni comporta una excesiva injerencia en el derecho fundamental a la intimidad como para exigir un control judicial previo, puesto que son diligencias de investigación tecnológica legítimas de acuerdo con la función constitucional de la Policía judicial.[37]

Sin embargo, recientemente el Tribunal Supremo ha puesto de manifiesto que, aunque el conocimiento de la posición geográfica del investigado por parte de los poderes públicos en el marco de una investigación procesal penal comporta una injerencia menor que otros actos de investigación, ello no puede llevarnos a banalizar la gran injerencia que supone el empleo de esta diligencia en los derechos fundamentales del investigado, en cualquier caso. A mi juicio, esta interpretación es acertada, pues al conocer la posición geográfica de una persona podemos acceder a información sensible como, por ejemplo, su asistencia a actos públicos de un determinado partido político, la práctica de una confesión religiosa o incluso la asistencia a lugares vinculados con su orientación sexual, entre otros.

Así, incluso aunque la vigente LECrim haya guardado silencio con respecto a los valores cuantitativos o cualitativos de gravedad del hecho delictivo que permitirían utilizar balizas o beepers en la investigación procesal penal, ello no puede interpretarse como una suavización de las exigencias constitucionales del art. 588 bis a LECrim, de manera que, en ocasiones, se ha llegado a estimar la ilicitud de una prueba adquirida a través de esta diligencia por el mero hecho de que ni el dictamen del Fiscal ni el auto judicial incluían motivadamente una ponderación de los derechos en conflicto después de que la Policía solicitara una injerencia en el derecho a la intimidad del investigado.[38]

[35] STS de 22 de junio de 2007
[36] Vid. Art. 554 LECrim
[37] STS de 5 de noviembre de 2013
[38] STS de 13 de mayo de 2020

2.2.5. Registro de dispositivos de almacenamiento masivo de información.

El registro de dispositivos de almacenamiento masivo de información, es decir, de dispositivos que combinan en un solo elemento su parte intangible (metadatos y datos) y su parte tangible (*hardware*)[39], requiere de autorización judicial previa en consonancia con los principios rectores recogidos a tenor del artículo 588 bis a) LECrim[40] y así lo ha corroborado nuestro Tribunal Supremo al poner de manifiesto que es necesaria una resolución judicial que permita la injerencia en el entorno digital del investigado.[41]

Aunque no tiene cabida un registro ilimitado puesto que ello comportaría una injerencia desproporcionada en los derechos fundamentales del investigado, realizar un registro perfectamente mesurado resulta una tarea de gran complejidad en la realidad práctica ya que, en ocasiones, no es posible conocer cuál es la información que guarda relación con el objeto de la investigación sin llevar a cabo una valoración previa de la totalidad de los datos contenidos en el dispositivo. De hecho, incluso con anterioridad a la reforma de 2015, el Tribunal Supremo señaló que el tratamiento jurídico de los datos que se almacenan en el dispositivo del investigado puede llegar a ser más adecuado si las imágenes, los mensajes y todos los datos reveladores de la intimidad del investigado se contemplan de forma unitaria.[42]

Pero es preciso destacar que la jurisprudencia ha reiterado que la intervención exclusiva de los elementos que tengan relación directa o indirecta con el objeto de la investigación exige un examen superficial previo que permita determinar qué datos pueden ser objeto de incautación[43], evitando la incautación de soportes físicos que contengan archivos o datos informáticos que puedan causar grave perjuicio al titular o propietario, siempre que sea posible obtener una copia en condiciones tales que garanticen la autenticidad e integridad de los datos[44].

No obstante, en aquellos casos de urgencia y siempre que sea imprescindible adoptar la medida, la Policía puede acceder a la información de un dispositivo incautado, siempre

[39] Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre registro de dispositivos y equipos informáticos.

[40] FERNÁNDEZ-GALLARDO, FERNÁNDEZ-GALLARDO, J.A., "Registro de dispositivos de almacenamiento masivo", *Dereito*, vol. 25, nº 2, 2016, p. 37

[41] STS de 10 de diciembre de 2015

[42] STS de 17 de abril de 2013

[43] STS de 15 de junio de 2020

[44] Vid. Art. 588 sexies c) 2 LECrim

y cuando lo comunique al Juez instructor en un plazo máximo de 24 horas, motivando la actuación y explicando el modo en que se ha accedido a esa información, así como los resultados arrojados.

Es importante, asimismo, destacar que el acceso a los datos almacenados en otro sistema informático que no se encuentren en el dispositivo registrado, pero a los que se puede acceder a través de él -por ejemplo, datos contenidos en la nube, servicios como *Dropbox,* o *Drive*- comportan una ampliación de la entidad del registro inicial del dispositivo, lo cual exige igualmente autorización judicial en caso de no haberlo previsto en la autorización inicial[45]. No obstante, si los datos contienen información a la que debe accederse urgentemente y se aprecia un interés constitucional, la Policía y el Ministerio Fiscal estarán legitimados para llevar a cabo la ampliación del registro de forma legítima, siempre que se ponga en conocimiento del Juez competente en un plazo máximo de 24 horas[46].

2.2.6. Registro remoto, registro online, *remote search* o *hacking* judicial.

Esta diligencia de investigación tecnológica es la que mayor injerencia supone en los derechos fundamentales del investigado: al ser un registro remoto no exige efectuar una entrada en el domicilio, de manera que el investigado no está presente durante la incautación ni es consciente de que su dispositivo está siendo interceptado, ya que el registro de los dispositivos se va a realizar de forma telemática tras la instalación de un *malware*[47]. Esto supone que esta diligencia requiera de gran motivación y detalle en cuanto al alcance de esta medida, pues de lo contrario comportaría una afección desproporcionada de los derechos fundamentales consagrados en el artículo 18 de nuestro texto constitucional, especialmente del derecho al secreto de comunicaciones y el derecho a la intimidad.

En cuanto a la normativa española, su regulación legal se ubica en el artículo 588 septies, letras a) a c) de nuestra LECrim. Sin embargo, en este articulado no encontramos

[45] Vid. Art. 588 sexies c) 3 LECrim
[46] Vid. Art. 588 sexies c) 4 LECrim
[47] Atendiendo a la conceptualización de AMÉRIGO SÁNCHEZ, un *malware* "es un concepto más amplio que el de virus informático, abarca también programas como los troyanos, el *spyware*, los *keyloggers*, etc."

cómo va a ser examinado exactamente el dispositivo del investigado, sino que ello viene precisado en la Circular 5/2019 donde se establece que esta diligencia estriba en "utilizar las contraseñas del investigado para acceder, no ya a su ordenador o sistema informático, que sería lo que proporcionaría un conocimiento más amplio de su entorno virtual, sino incluso a reductos de privacidad más limitados, pero igualmente útiles para la investigación, como su cuenta de correo electrónico o su cuenta de almacenamiento de datos en la nube."

Al ser una medida tan invasiva, la propia LECrim limita esta diligencia a un *numerus clausus* de delitos, en concreto: delitos cometidos en el seno de organizaciones criminales; delitos de terrorismo; delitos cometidos contra menores o personas con capacidad modificada judicialmente; delitos contra la Constitución, de traición y relativos a la defensa nacional y delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.[48]

No obstante, aunque aparentemente se configura como una especie de lista cerrada, el último de los delitos es una especie de "cajón de sastre" puesto que resulta indefinido. Esto puede derivar en "un uso encubierto y desmedido de esta diligencia"[49], lo que supondría avalar el uso de esta diligencia tan invasiva de derechos fundamentales ante la perpetración de cualquier tipo de delito. Todo ello nos lleva a la reflexión -en palabras de Bueno de Mata- de que no estamos ante un *numerus clausus*, ya que la propia ley deja este cajón de sastre abierto a que el Juez decida qué delitos tienen cabida bajo la calificación de delitos "cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación", lo cual -en mi opinión- genera un gran problema de inseguridad jurídica, teniendo en cuenta los derechos fundamentales que pueden verse potencialmente afectados.

Otra particularidad de esta innovadora diligencia de investigación es, según establece el propio artículo 588 septies a) LECrim, la especificidad que se exige a la resolución judicial preceptiva por la que se motiva la adopción de esta medida, teniendo incluso que detallar hasta el sistema informático empleado. Ello resulta incongruente con la necesidad de no revelar el *modus operandi* de la Policía Judicial para evitar que el investigado

[48] Vid. Art. 588 septies a) 1 LECrim

[49] BUENO DE MATA, F., *Las diligencias de investigación penal en la cuarta revolución industrial*, Aranzadi, Cizur Menor (Navarra), 2019, p.193

descubra cualquier tipo de mecanismo que podría usarse para frustrar el objeto de la investigación, ya que esto supondría una grave obstrucción para la justicia. Así, de forma acertada, la Circular 5/2019 ha aclarado que "bastará con indicar el tipo de programa que se utilice y, en su caso, su alcance potencial o funcionalidades, sin necesidad de facilitar otros datos técnicos específicos", de manera que bastaría simplemente con afirmar que se ha utilizado un troyano o un *keylogger*[50], sin necesidad de detallar datos o nombres técnicos concretos.

De igual manera, la ley prevé el deber de colaboración[51] de los prestadores de servicios de telecomunicaciones, los titulares o responsables del sistema informático o base de datos objeto del registro están obligados a asistir y colaborar con los agentes investigadores[52], teniendo la obligación de guardar secreto acerca de las actividades para las que las autoridades los hayan requerido.

Por último, la duración de esta medida es de un mes, prorrogable por periodos iguales hasta un máximo de tres meses[53], lo que la sitúa en la diligencia de investigación tecnológica de menor duración. De esta duración puede resultar que esta medida sea ineficaz, pues en ocasiones se precisa solicitar contraseñas y datos de acceso del investigado a un servidor -el cual tiene el deber de colaborar-, de manera que el tiempo de respuesta del servidor puede llegar a ser incluso superior al tiempo de duración de la medida. En este sentido, la Circular 5/2019 se ha pronunciado aclarando que el cómputo del plazo de duración se iniciará "desde la fecha del auto por el que se acuerde la medida y no desde la fecha de efectividad de la misma".

A este respecto, hemos de mostrarnos críticos con la postura por la que opta la Fiscalía y reprochar que, atendiendo a razones de mera eficacia de la medida de investigación tecnológica, sería conveniente que el cómputo del plazo iniciara una vez que la medida se haya implementado de forma efectiva, pues ello puede llevarnos a que nos quedemos desprovistos de tiempo[54], especialmente en casos en los que se necesite de

[50] Como aclara DELGADO MARTÍN, J., en "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015", *Diario la Ley*, Editorial La Ley, 2016, p.14: un *keylogger* es un instrumento que, a través de un *software*, almacena las pulsaciones realizadas en el teclado de un dispositivo electrónico.

[51] Vid. Art. 588 septies b) LECrim

[52] Excepto el investigado o encausado, las personas dispensadas por razón de parentesco y las que no puedan declarar en virtud del secreto profesional, de conformidad con el art. 416.2 LECrim.

[53] Vid. Art. 588 septies c) LECrim

[54] BUENO DE MATA, F., *Las diligencias de investigación penal en la cuarta revolución industrial*, op., cit., p.199

la colaboración de servidores para que nos faciliten datos y contraseñas del usuario investigado.

2.2.7. El agente encubierto informático.

La reforma procesal de la LO 13/2015 ha abordado esta figura *ex novo*, en particular en el apartado 6 del artículo 282 bis LECrim, como muestra de un esfuerzo del legislador por "adaptar el texto legal a la sociedad digitalizada en la que nos encontramos inmersos"[55], lo cual resulta acertado, puesto que España se posiciona como el 13º país más atacado en el espacio cibernético a nivel mundial[56]. No obstante, a pesar de que resultaba necesaria la incorporación de esta figura a nuestro Derecho positivo, la jurisprudencia ya la venía admitiendo reiteradamente con anterioridad.[57]

La posición que ocupa esta figura en el articulado de nuestra LECrim no es trivial, a mi juicio, sino que tiene su razón de ser: esta figura implica la intromisión de un agente en organizaciones criminales[58], mientras que en el resto de las diligencias analizadas no concurre esta circunstancia. Su función, así, extrapolando el concepto de "agente encubierto" de la esfera física a la virtual, consiste en ocultar la identidad policial para poder establecer una relación cercana con el investigado de tal manera que -tras ganarse la confianza de éste- podrán obtener a información oculta que les ayudará a descubrir al supuesto delincuente.[59]

Por lo que respecta a la necesidad de autorización judicial, ésta deberá ser otorgada por el Juez de Instrucción[60] requiriéndose, además, una autorización específica para

[55] STS de 13 de marzo de 2019

[56] Accesible en: https://cybermap.kaspersky.com/es último acceso: 12 de abril de 2022

[57] En este sentido la STS 236/2008, de 9 de mayo, establece que "al verificar los rastreos la Policía Judicial estaba cumpliendo su función de perseguir delitos y detener a los delincuentes que los cometen, siendo legítimos y regulares los rastreos efectuados". En el mismo sentido se pronuncia la STS 725/2010, de 14 de julio: "es cierto que el agente actuó de forma encubierta, haciéndose pasar por un usuario más en la red, pero ello no infringe ningún derecho del acusado […] luego se trataba de una actividad de investigación policial".

[58] El artículo 282 bis 4 LECrim nos define la *delincuencia organizada* en los siguientes términos: "se considerará como delincuencia organizada la asociación de tres o más personas para realizar, de forma permanente o reiterada, conductas" que sean susceptibles de calificarse en los tipos penales que el mismo artículo detalla o "cualquier delito de los previstos en el artículo 588 ter a LECrim", según aclara su apartado sexto.

[59] BUENO DE MATA, F., "El agente encubierto en Internet: mentiras virtuales para alcanzar la justicia", *Los retos del Poder Judicial ante la sociedad globalizada*, Actas del IV Congreso Gallego de Derecho Procesal, Universidad de A Coruña, 2012, p. 297

[60] Vid. Art. 282 bis 6 LECrim

intercambiar o enviar archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos que se hubieran aplicado para identificar tales archivos ilícitos.

En mi opinión, no obstante, esta regulación resulta poco concreta, pues la ley no aporta qué se entiende por "archivo ilícito", de manera que podría entenderse que son tanto vídeos, como fotos, como incluso troyanos o cualquier tipo de *malware* que pudiera atentar contra el honor o la intimidad de la persona, en cuyo caso concreto los derechos fundamentales del investigado deberían ponderarse en un modo diverso.

Por último, haciendo referencia a la duración de la medida, el propio artículo 282 bis LECrim, en su apartado primero, establece que durará un plazo de seis meses, que podrán prorrogarse por periodos de otros seis meses.

3. Biometría como diligencia de investigación.

El vocablo *biometría* resulta cada vez más familiar en el ámbito de la justicia, pues su aplicación se ha extendido de manera progresiva en la práctica legal en los últimos años. Esta técnica se basa en recolectar dos tipos de datos que son susceptibles de ser digitalizados y que, además, resultan inmutables a lo largo del tiempo por su propia naturaleza: los datos fisiológicos y los conductuales, según los cuales, todos los individuos somos individualizables.

Así, podemos definir la biometría como una técnica que permite identificar a un individuo de forma automática a través de características fisiológicas o de comportamiento que resultan atribuibles únicamente a ese individuo.[61] Esta técnica, a pesar de que puede resultarnos un tanto exótica, se utiliza cada vez con mayor frecuencia como una diligencia de investigación tecnológica, pues permite tanto identificar a sujetos que han cometido un ilícito y necesitan ser localizados, como a los potenciales delincuentes. Esto se logra a partir de la digitalización de los datos biométricos para su posterior cotejo con una base de datos, la cual creará una alerta en caso de que los datos biométricos introducidos presenten coincidencias con los que figuren en la base de datos como pertenecientes a delincuentes o sospechosos.

[61] SÁNCHEZ CALLE, A. *Aplicaciones de la visión artificial y la biometría*, Editorial Dykinson, Madrid, 2005, p. 10

La biometría, como toda ciencia, se sustenta sobre unos principios rectores, siendo estos: universalidad, pues todos contamos con rasgos fisiológicos o de conducta susceptibles de ser cuantificados biométricamente; singularidad, puesto que la biometría se encarga de características que resultan particulares de un sujeto en exclusiva y permanencia, en tanto que son elementos que se mantienen inalterables a lo largo del tiempo.[62]

Cabe aclarar, sin embargo, que no es una técnica utilizada de forma exclusiva en las diligencias de los procesos penales[63], sino que resulta también frecuente su aplicación en materia probatoria, como método de identificación en documentos financieros o como forma de identificación de individuos para evitar que se produzcan fraudes a entidades de crédito. No obstante, en consonancia con el objeto del presente TFG, me referiré exclusivamente al tratamiento procesal penal de la Biometría.

En este apartado analizaré, por consiguiente, las diferentes modalidades biométricas que pueden ser empleadas como diligencias de investigación y su incidencia en el proceso penal español. Para esto, en primer lugar, llevaré a cabo un estudio minucioso de las técnicas biométricas que emplean datos fisiológicos que, como el propio término indica, son aquellas basadas en obtener datos fisiológicos de un sujeto; seguidamente, realizaré un somero análisis de las diferentes modalidades biométricas de comportamiento, estas últimas vinculadas a conductas del sujeto que permiten su identificación.

Existen, además, otras técnicas biométricas como la termografía facial, en las cuales no me detendré porque considero que resultan aún un tanto innovadoras en nuestro país debido a su alto coste y a la poca implementación que tienen en España en la actualidad. Ello, no obstante, las mencionaré brevemente para quedar reflejo de su existencia, a pesar de su baja incidencia en el proceso penal español actual.

3.1.Modalidades biométricas fisiológicas.

3.1.1. Reconocimiento de huellas dactilares.

[62] CONTRERAS GARCÉS, J., "Transcendencia de los informes periciales de dactiloscopia en los tribunales de justicia", *Ciencia policial: revista del Instituto de Estudios de Policía*, nº 119, 2013, pág. 24

[63] Para ver distintos ámbitos de aplicación de las técnicas biométricas, consultar: VÁZQUEZ DÍAZ, M.Á., "Sistemas de identificación, verificación y autentificación biométricos, una realidad emergente", *Ciencia policial: revista del Instituto de Estudios de Policía*, nº 112, 2012, págs. 30-33.

El reconocimiento de huellas dactilares ha sido una de las técnicas biométricas empleadas con mayor frecuencia en el proceso penal. Como muestra de ello, existe una gran amalgama de sentencias cuyo fundamento jurídico hace referencia a la admisión a prueba de la identificación biométrica de las huellas dactilares del investigado, las cuales han sido obtenidas previamente en la fase de diligencias de investigación.[64]

Esta modalidad biométrica consiste en analizar las denominadas "crestas papilares"[65], unos repliegues localizados en las yemas de los dedos de la mano que comienzan a formarse durante la sexta semana de vida intrauterina y se mantienen inmutables hasta la muerte, simplemente sufriendo un aumento de tamaño proporcional al crecimiento del sujeto[66]. Este rasgo de la inmutabilidad es lo que ciertamente ha dotado a esta técnica biométrica de gran precisión en tanto que diligencia de investigación, convirtiéndola en el método identificativo por excelencia ya que todos poseemos un sistema decadactilar individual con características únicas que hacen imposible hallar a dos sujetos con crestas papilares iguales, ni siquiera los gemelos homocigóticos.[67]

No obstante, esta diligencia de investigación presenta ciertos inconvenientes[68], ya que existe un sector de la población que no presenta huellas dactilares que puedan ser aptas para identificarlos. Este es el caso, por ejemplo, de trabajadores manuales cuyas. huellas dactilares se han visto deterioradas a raíz de la destrucción de la capa profunda o basal del dedo, o bien de sujetos que carecen de dedos debido a una amputación, hayan perdido sus huellas debido a quemaduras o incluso que carezcan de huellas dactilares debido a una mutación genética.[69]

[64] El fallo de STS de 1 de octubre de 2020 atribuye la autoría de un delito de robo con intimidación en casa habitada a partir de la existencia de una huella dactilar que permite imputar los hechos al acusado. Más ejemplos que avalan el uso de esta técnica en los tribunales son STS de 31 de octubre de 2014, así como STS 557/2000 de 4 de septiembre que afirma que se ha "admitido por la jurisprudencia el valor probatorio de las huellas dactilares, coincidentes con las del acusado."

[65] Consultar ANEXO I para observar los diferentes elementos que componen la huella dactilar.

[66] *Avances en la identificación de personas mediante las huellas dactilares* (s.f.) (Últ. Consulta) el 08/04/2022 de https://ciencia.unam.mx/leer/994/avances-en-la-identificacion-de-personas-mediante-las-huellas-dactilares

[67] Huellas dactilares (s.f.) (Últ. Consulta) el 08/04/2022 de https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Huellas-dactilares

[68] ALONSO FERNÁNDEZ, F., COOMONTE BELMONTE, R., ORTEGA GARCÍA, J., Biometría y Seguridad, Cuadernos Cátedra ISDEFE-UPM, FUNDETEL, 2008, p. 32.

[69] *El extraño caso de la familia sin huellas dactilares* (s.f.) (Últ. Consulta) el 08/04/2022 de https://www.elmundo.es/elmundosalud/2011/08/04/pielsana/1312482983.html

3.1.2. Análisis comparativo de ADN.

Como es bien sabido, el ADN se ha convertido en uno de los métodos más utilizados para la identificación y posterior atribución de la autoría de hechos ilícitos a un determinado sujeto -siempre que le sea causalmente imputable- debido a su alto grado de fiabilidad[70].

Es cierto que no resulta una técnica tan futurista, probablemente debido a su gran instauración en el proceso penal español y a que no requiere un gran uso de tecnología innovadora. Ello, no obstante, algunos autores han decidido catalogarla como una técnica biométrica más debido a que se basa en la obtención de datos fisiológicos inmutables (como puede ser un pelo, saliva, sangre) que se utilizan para compararlos con los datos genéticos del sospechoso,[71] los cuales deberán ser obtenidos garantizando todos los derechos fundamentales. De esta manera, tras cotejarlo se podrá verificar si, efectivamente, guarda relación alguna con los hechos ilícitos por los que se le investiga. Además, los datos genéticos del sospechoso ingresarán en la base de datos del banco policial de perfiles de ADN, lo cual servirá para investigaciones criminales presentes, anteriores y futuras.

Está tan extendido el uso del ADN para estos fines, que la actual LECrim contempla en su cuerpo legal la posibilidad de esta diligencia de investigación al determinar que el Juez de Instrucción puede acordar a través de resolución motivada la obtención de muestras biológicas de un sospechoso, siempre que éstas resulten indispensables para determinar su perfil de ADN, pudiéndose realizar todo tipo de actos de inspección, reconocimiento e intervención necesarios y adecuados a los principios de proporcionalidad y razonabilidad.[72]

No obstante, este artículo no observa los problemas constitucionales que la obtención de muestras de ADN supone, pues el sospechoso siempre puede oponerse -tras la asistencia de su Letrado- al sometimiento a técnicas que tengan por objeto la obtención de su ADN, pues ello podrá constituirse en una prueba que servirá para inculparlo. Sin embargo, los derechos fundamentales no son derechos absolutos, por lo que incluso

[70] CABEZUDO BAJO, M.J., "La regulación del 'uso forense de la tecnología del ADN' en España y en la Unión Europea", *FODERTICS, Estudios sobre Derecho y nuevas tecnologías,* Santiago de Compostela, 2012, p. 103

[71] CABEZUDO BAJO, M.J., "La regulación.., op., cit., p. 107

[72] Vid. Art. 363 LECrim

aunque el investigado se opusiera, en casos de presuntos terroristas[73], sería posible la obtención de muestras de ADN de manera forzosa aplicando las medidas coactivas mínimas indispensables. En todo caso, ello se haría en respeto de la dignidad del investigado y observando el principio de proporcionalidad.

Así, incluso en aquellos supuestos en que un presunto terrorista se opusiera a la obtención de una muestra de su ADN para su posterior cotejo se podrá de igual modo, por ejemplo, aplicar la técnica del frotis bucal de modo forzoso. En esta línea, encontramos que la jurisprudencia del Tribunal Constitucional ha admitido como prueba lícita una pericial consistente en una muestra de saliva recogida de un esputo que el investigado realizó en calle lo cual, conforme a la doctrina asentada, respeta las exigencias constitucionales y no lesiona el derecho a la intimidad del art. 18.1 CE.[74]

3.1.3. Geometría de la mano.

La técnica biométrica de la geometría de la mano se basa en la medición de la forma de la mano tras situar las manos del sujeto que se quiera autenticar sobre un dispositivo lector con unas guías que marcan la posición correcta para la lectura[75]. Así, se toman como datos la longitud y el grosor de los dedos de la mano, su curvatura, el tamaño y la forma de la palma, entre otros. No se tienen en cuenta, en cualquier caso, detalles que puedan variar a lo largo del tiempo, tales como cicatrices superficiales o la longitud de las uñas.

Sin embargo, considero que la fiabilidad de esta técnica biométrica no resulta elevada, pues es objeto de crítica el hecho de que no existen estudios detallados que puedan constatar la unicidad ni la estabilidad de la geometría de la mano[76] puesto que puede sufrir modificaciones por diversos motivos como, por ejemplo, variaciones de peso, que desvirtuarían la capacidad probatoria.

[73] Vid. Art. 129 bis CP

[74] En este sentido, consultar doctrina jurisprudencial de SSTC 43/2014, 199/2013, y STS 355/2006.

[75] Consultar ANEXO II para ilustrar esta técnica.

[76] SÁNCHEZ ÁVILA, C. (2012). *Aplicaciones de la biometría en seguridad* en: "VIII Ciclo de Conferencias UPM TASSI (Temas Avanzados en Seguridad y Sociedad de la Información)", Campus Sur UPM, Madrid, 2012, p. 62.

3.1.4. Reconocimiento facial.

Esta técnica biométrica, recientemente utilizada también para la identificación de usuarios en dispositivos *smartphone*, consiste en reconocer a un sujeto a partir de su identificación con una imagen o fotografía. Para esto, en el ámbito de las diligencias de investigación penal, se realiza una combinación de las imágenes almacenadas en la base de datos policiales con un *software* automatizado de identificación biométrica, el cual utiliza diferentes puntos nodales del rostro[77] como parámetros: ancho de la nariz, ubicación de cejas u ojos, distancia de los ojos a la boca, o la longitud de la línea de la mandíbula, entre otros.[78]

A pesar de ser una técnica biométrica altamente empleada gracias a la gran calidad y precisión de la fotografía digital y de vídeo multimedia, he de precisar, no obstante, que resulta mucho menos eficaz que el reconocimiento de huellas dactilares, debido a que los rasgos faciales no son permanentes, sino que pueden ser fácilmente alterados[79], pues cualquiera puede modificar su cara de manera muy sencilla, por ejemplo, dejándose crecer la barba o incluso mediante técnicas de cirugía estética.

Asimismo, otro inconveniente atiende al hecho de que el reconocimiento facial a través de datos biométricos puede ser un arma tecnológica muy peligrosa, pues estamos hablando de una tecnología muy intrusiva y que requiere un tratamiento jurídico muy garantista pues, de lo contrario, acarreará efectos adversos en los derechos fundamentales de los sujetos.[80]

Además, esta técnica de reconocimiento facial presenta una serie de limitaciones, pues no podemos olvidar que estamos hablando de reconocimientos que se basan en la similitud o divergencia entre imágenes, de manera que para aplicar esta técnica con una fiabilidad del 100% deberíamos utilizar imágenes tomadas en condiciones exactas, esto

[77] Consultar ANEXO III para observar los distintos puntos nodales utilizados como parámetros en los sistemas biométricos.

[78] CORTÉS OSORIO, J.A., MEDINA AGUIRRE, F.A., MURIEL ESCOBAR J.A., "Sistemas de seguridad basados en biometría", *Scientia et Technica*, nº 46, Pereira (Colombia), 2010, p. 99.

[79] En este sentido *Reconocimiento facial* (s.f.) (Últ. Consulta) el 08/04/2022 de https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Reconocimiento-facial determina que "el reconocimiento facial debe tener en cuenta diversos factores como envejecimiento, cirugía plástica, cosméticos, efectos del consumo excesivo de drogas o tabaco y pose de la persona."

[80] A este respecto, conviene consultar el Auto de 15 de febrero de 2021 de la Audiencia Provincial de Barcelona, donde se denegó a la mercantil MERCADONA S.A. el empleo de tecnologías que captaban datos biométricos para reconocer la entrada de dos condenados al establecimiento debido a que el tratamiento de estos datos suponía una elevada incursión en los derechos fundamentales de los condenados.

es, desde una misma distancia, utilizando la misma lente, con la misma luminosidad, entre otras. Las limitaciones más comunes que pueden derivarse de esta técnica son el llamado *efecto barril* y las *variaciones en el ángulo de captura*[81].

Por lo que respecta al efecto barril, éste consiste en una distorsión de la imagen -especialmente protuberante en las zonas periféricas- debida a la lente de la cámara que curva el rostro de las personas que aparecen en la imagen lo que supone, por ende, un límite a la identificación del sujeto a través de esta técnica.

Por otra parte, las variaciones en el ángulo de captura son aquellas distorsiones que se producen cuando se capta una imagen desde un plano vertical, pues al colocar la cámara a una determinada altitud se alteran las distancias entre los distintos puntos nodales del rostro, lo que comporta, nuevamente, un límite a la eficacia del reconocimiento facial.

Todo ello, unido con las propias deficiencias del sistema utilizado por nuestra Policía Nacional, pone de manifiesto la ingente necesidad de mejorar nuestros programas de reconocimiento facial para contar con una tecnología competente y eficiente[82].

3.1.5. Reconocimiento de iris.

La utilización del iris como diligencia de investigación para la identificación de posibles delincuentes ha tenido una gran acogida. Ello se debe a que este método biométrico se basa en datos relacionados con el iris, siendo éste una membrana con cualidades individuales que no están determinadas genéticamente, sino que resultan individuales para cada sujeto y permanecen estables a lo largo del tiempo.[83] Ello dota a la técnica biométrica del reconocimiento de iris de un alto grado de fiabilidad y de una

[81] BUENO DE MATA, F., "Biometría e investigación criminal", *Revista Eletrônica de Direito Processual*, nº 3, Río de Janeiro, 2020, p. 130

[82] Como señala BUENO DE MATA, F., "Biometría e Investigación Criminal", op., cit., p.131, encontramos limitaciones en tanto que la posición de la cara "debe ser preferiblemente de frente y con no más de una curvatura de 15 grados" siendo recomendable que "la expresión de la cara sea neutra, con lo que una simple sonrisa o una persona estrábica o con los ojos cerrados no podrían ser nunca identificadas por el programa informático."

[83] CALCEDO MARMOLEJO, L.F., CHAMORRO CARVAJAL, C.E., CRUZ ARDILLA, J.C., VALENCIA MURILLO, J.F., "Extracción de características del iris como mecanismo de identificación biométrica", *Revista Virtual Universidad Católica del Norte*, 2014, p. 185

alta prevención ante ataques de suplantación de identidad, pues las características del iris son únicas, de manera que no se pueden replicar ni alterar.

Ahora bien, para obtener datos biométricos que nos puedan servir como una diligencia de investigación en un proceso penal, la imagen del iris debe someterse a un procedimiento complejo que permita transformarla en un patrón biométrico.

Este procedimiento[84] se inicia con la adquisición de la imagen del iris, a la cual deberá de eliminarse los elementos que aportan "ruido" a la imagen, esto es, los párpados, las pestañas y todas las zonas que forman parte de la cara, pero no del iris, las cuales se deberán eliminar. Así, en un primer momento se procede a detectar el círculo de la pupila y, en segundo lugar, se detecta el círculo del iris, que es lo que va a resultar relevante a efectos de la investigación.

Una vez que se obtiene la imagen completamente libre de "ruido", es decir, simplemente la imagen del iris, lo que se hace es transformar esa imagen en una imagen rectangular de dimensiones constantes, la cual -una vez extraída la información más discriminatoria- se codificará. Una vez que esta información ya se encuentra codificada, la Policía podrá compararla con la información almacenada en la base de datos para poder determinar la identificación del sujeto.

3.2.Modalidades biométricas de comportamiento.

3.2.1. Reconocimiento de firma manuscrita.

Por lo que respecta a la firma manuscrita, aunque parezca que se está quedando obsoleta debido a la gran presencia de la firma electrónica en la actualidad, es preciso mencionar brevemente que a través de las técnicas biométricas y del peritaje caligráfico es posible identificar al sujeto firmante, e incluso en qué condiciones firmó, llegando incluso a determinar si el sujeto firmó bajo miedo insuperable o coacción[85].

En este caso, los datos a los que se da un tratamiento biométrico son, principalmente, la forma, la presión del bolígrafo, la velocidad y los cambios producidos en la velocidad

[84] Para una lectura más detallada del procedimiento, consultar GUTIÉRREZ NÚÑEZ, C., PELÁEZ GUEVARA, J. "El iris humano como método de identificación forense", *Advocatus*, nº 36, 2021, págs.191-196

[85] BUENO DE MATA, F., "Biometría e Investigación Criminal", op., cit., p.126.

y la presión durante la elaboración de la firma, ya que estas características sólo pueden ser reproducidas a manos del firmante original.

3.2.2. Reconocimiento de voz.

También la voz ha sido empleada en diligencias de investigación como un elemento que, a partir de su tratamiento biométrico, nos permite identificar a sujeto. Si bien es cierto que la voz tiene un componente de carácter fisiológico determinado por la entonación o la frecuencia de un sujeto al hablar, también presenta un sesgo de comportamiento, y es por ello por lo que se puede clasificar como una modalidad biométrica de comportamiento.[86]

Atendiendo a los rasgos relacionados con el comportamiento del locutor, estos pueden suponer que se produzcan variaciones de la voz en función de distintas circunstancias: enfermedad (por ejemplo, resfriado o faringitis), edad, contexto social, estado de ánimo, etc. En este sentido, se ha puesto de manifiesto que la voz puede ser conscientemente manipulada por el sujeto, ya que puede intentar imitar otra voz distinta de la suya. Ello supondría un límite frente a este uso de la biometría como diligencia de investigación; pero, sin embargo, la tecnología más innovadora no se ciñe a analizar la frecuencia vocal, sino que permite analizar incluso el ritmo del habla, la entonación, la jerga, el léxico y el uso de expresiones lingüísticas características del investigado,[87] lo cual dota a esta técnica biométrica de fiabilidad.

Tal es así, que estamos ante una diligencia de investigación electrónica utilizada de forma reiterada por la Justicia, con especial relevancia en casos de escucha ambiental o interceptación de comunicaciones.[88]

3.2.3. Reconocimiento del tecleo de usuarios de equipos informáticos.

[86] ALONSO FERNÁNDEZ, F., COOMONTE BELMONTE, R., ORTEGA GARCÍA, J., *Biometría y Seguridad*, op. cit. p. 33.

[87] ALONSO FERNÁNDEZ, F., COOMONTE BELMONTE, R., ORTEGA GARCÍA, J., *Biometría y Seguridad*, op. cit. p. 34.

[88] Consultar STS 248/2004, donde se lleva a cabo un reconocimiento y cotejo de voz de unas grabaciones aportadas en fase de instrucción que sirven posteriormente como prueba judicial para determinar la responsabilidad criminal respecto de los hechos delictivos.

Nos encontramos en una era donde la innovación tecnológica es tal que un gran número de actividades cotidianas -como la celebración de un contrato- tienen lugar en la red, lo cual acarrea, consecuentemente, un mayor número de delitos en el ciberespacio. Así, resulta indiscutible que el delincuente contemporáneo cuenta con la posibilidad de perpetrar hechos delictivos detrás de una pantalla, y esto se traduce en que las diligencias de investigación penal encaminadas a descubrir la autoría de hechos delictivos no puedan ignorar las particularidades del espacio cibernético.

En este contexto, el principal medio a través del cual un individuo se relaciona con un equipo informático es el teclado. En base a esto, la técnica biométrica del reconocimiento del tecleo de usuarios de equipos informáticos analiza la velocidad que un sujeto emplea para identificarse (introducir usuario y contraseña) en la red, analizando el tiempo transcurrido entre pulsar una y otra tecla, así como el tiempo que mantiene presionada una tecla.[89]

Una vez obtenidos estos datos -y tras haber creado un patrón biométrico- se cotejan con datos recogidos anteriormente y referentes a entradas del sujeto en el equipo informático para identificarse. De este modo, se establece si, efectivamente, el sujeto que está tras la pantalla es el usuario legítimo, lo que aporta una gran seguridad en la red, particularmente en el ámbito del comercio electrónico.

3.3.Otras técnicas biométricas.

En este último apartado, me gustaría hacer referencia a técnicas biométricas que, si bien es cierto aun resultan muy novedosas en el ámbito de la investigación procesal penal española, están empezando a aplicarse cada vez con mayor frecuencia. Así, aunque su uso es limitado, ya que plantean ciertos problemas de implantación como una menor eficacia, costes elevados o la exigencia de esfuerzos mayores a la hora de procesar los datos biométricos, es preciso hacer una mención sucinta de los mismos para evidenciar todo lo que nos queda por innovar en el campo de la investigación para poder situarnos a la vanguardia tecnológica.[90]

[89] MARTÍN BRAÑAS, C., *Reconocimiento del delincuente: nuevas diligencias de identificación*, Boletín del Ministerio de Justicia, nº 2182, 2015, p. 43.

[90] BUENO DE MATA, F., "Biometría e Investigación Criminal", op., cit., p.132

Estas técnicas son, en primer lugar, la forma del pabellón de la oreja, que tiene una forma de identificación similar a la de la huella dactilar, y que presenta ciertas ventajas con respecto al reconocimiento facial, como que no adolece de los problemas de iluminación que puede adolecer una fotografía debido a que la propia cabeza alrededor de la cabeza actúa como "fondo" de la fotografía.

De igual manera, destaco la técnica de reconocimiento mediante venas de la palma de la mano y la técnica de escáner de retina, ambas de gran fiabilidad puesto que no se pueden alterar con facilidad. Sin embargo, el escáner de retina exige un grado de cooperación por parte del investigado muy elevado al ser necesario que posicione su ojo a escasa distancia de un sensor que emite luz infrarroja[91]. Ello, junto con el hecho de que puede relevar algunas enfermedades como la hipertensión, hace que se considere una técnica invasiva.[92]

Otra técnica biométrica que destacar la conforma el modo de caminar del investigado, una técnica de biometría informática caracterizada por la facilidad de capturar este tipo de datos y por la falta de necesidad de cooperación por parte del investigado, ya que la propia la LECrim, concretamente en su artículo 588 quinquies a), permite la videovigilancia en el proceso penal. De modo un poco más futurista, por último, destacan la biometría aplicada al movimiento de los labios del investigado o bien a su olor corporal.

4. Especial referencia a los delitos de terrorismo.

4.1.El empleo de la biometría como respuesta a la amenaza terrorista.

Los responsables de los ataques terroristas del 11-S, de acuerdo con la investigación penal llevada a cabo, fueron capaces de entrar en el territorio de EE.UU. utilizando sus documentos de identificación, es decir, bajo su propia identidad.[93] Ello puso en entredicho la seguridad de la población civil frente a las organizaciones terroristas, pues estos sujetos eran ya conocidos como "sospechosos terroristas" por las autoridades americanas y, sin embargo, fracasaron a la hora de identificarlos.

[91] ALONSO FERNÁNDEZ, F., COOMONTE BELMONTE, R., ORTEGA GARCÍA, J., *Biometría y Seguridad*, op. cit. p. 38.

[92] En este sentido lo manifiesta BUENO DE MATA, F., "Biometría e Investigación Criminal", op., cit., p.132.

[93] WOODWARD, J. D., "Biometrics: facing up to terrorism", *Military Review*, 2001, p. 7

Este caso particular evidenció, así, la necesidad de encontrar nuevos métodos de identificación que pudieran detectar a terroristas o sospechosos de delitos de terrorismo con precisión, lo cual permitiría detener y/o frustrar futuras amenazas terroristas. Fue así como se empezó a plantear, por primera vez, la necesidad de aplicar técnicas biométricas para la identificación tanto de autores de un delito de terrorismo, como de sospechosos del mismo.

Centrándonos en el caso español, la llegada de la democracia experimentó una gran expansión de los delitos de terrorismo protagonizada, de la forma más violenta, por el grupo terrorista ETA[94], que operó en el territorio nacional durante 50 años, aproximadamente. Aunque la vuelta a la democracia supuso la promulgación de una ley antiterrorista especial[95], lo cierto es que muy pronto resultó derogada para incluir los delitos de terrorismo en la materia regulada en el Código Penal común, donde se mantienen ubicados en la actualidad.

Esto no ha supuesto, no obstante, traba alguna al incesante esfuerzo público en la lucha contra el terrorismo, lo cual ha conducido a la justicia española al empleo de la biometría al ser éste uno de los medios más prometedores para acabar con esta lacra.

En este sentido, podemos afirmar que el terrorismo y la biometría forman un único sistema, pues la base de cualquier organización terrorista consiste, efectivamente, en desdibujar la línea que permite distinguir "víctimas" de "responsables", "civiles" de "combatientes", o incluso espacios privados de espacios públicos. Así, la estrategia terrorista opera desde la ubicuidad: consiste en persuadir al enemigo -necesariamente desde el anonimato- de que un espacio cualquiera puede transformarse en un lugar de combate en cualquier momento[96]. Tal es así, que cuanto más se subvierta el principio procesal de la presunción de inocencia, aparentando ser sujetos muy cercanos al ciudadano que respeta escrupulosamente nuestro ordenamiento jurídico y sus leyes, mayor será la operatividad de los ataques terroristas.

[94] Manifiesta LADRÓN DE GUEVARA PASCUAL, C., en "El derecho a la verdad de las víctimas del terrorismo" p. 7, que existen "853 víctimas mortales asesinadas por la organización terrorista ETA", aunque existen discrepancias con relación a esta cifra basadas en los criterios utilizados por los distintos organismos públicos a la hora de atribuir la autoría de los crímenes terroristas.

[95] Accesible en https://www.boe.es/buscar/doc.php?id=BOE-A-1985-63

[96] FOESSEL, M., GARAPON, A., "Biométrie: les nouvelles formes de l'identité", *Espirit*, 2006, p. 167

Paradójicamente, este anonimato y esta falta de identificación deben venir sucedidas por una brutal publicidad operada por los medios de comunicación. Es en este punto -entre el anonimato y la publicidad violenta- dónde se sitúa la biometría, ya que ésta favorece la aplicación de criterios de identificación estables al tomar como referencia elementos fisiológicos o de conducta individualizados. Sin embargo, ¿qué elementos deben utilizarse para luchar efectivamente contra los delitos de terrorismo?

Los elementos físicos pueden mutar en el tiempo o incluso a través del uso de la cirugía contemporánea. Es por ello, por lo que la biometría aplicada en la lucha contra el terrorismo se centra en estructuras biológicas inalterables y que se pueden objetivar a través de parámetros informáticos, de tal manera que se mantengan constantes en el tiempo, siendo el reconocimiento facial o la huella digital los datos biométricos más empleados para la identificación de terroristas.

4.2.El empleo de la videovigilancia en la identificación de terroristas.

Como adelanté en el apartado segundo del presente TFG, la técnica de la videovigilancia ha sido regulada por nuestra LECrim como una diligencia de investigación tecnológica, estando incluso dispensada de autorización judicial en tanto en cuanto las imágenes se obtengan de lugares públicos. En este sentido, el empleo de la videovigilancia en espacios públicos, a pesar de ser una técnica un tanto antigua, es cada vez mayor debido a su bajo coste y a que los datos recogidos a partir de técnicas de videovigilancia, tras ser cotejados con técnicas biométricas, son una tecnología clave para la lucha contra el terrorismo.[97]

Tal es así que el empleo de la videovigilancia ha sido una de las primeras técnicas utilizadas para recoger datos biométricos que, comparados con una base de datos biométricos a nivel mundial, han permitido la identificación de autores de delitos de terrorismo, como en el ejemplo que paso a exponer a continuación.

En el marco de la investigación procesal de los ataques terroristas del 11-S, uno de los más mortíferos de la historia de la humanidad, se desarrolló el *caso del secuestrador*

[97] *Berlín defiende la videovigilancia con reconocimiento facial contra terroristas* (s.f.) (Últ. Consulta) el 23/04/2022 de https://www.dw.com/es/berl%C3%ADn-defiende-videovigilancia-con-reconocimiento-facial-contra-terroristas/a-40224938

número 20 de los atentados del 11-S[98]. En este caso, Mohamed Al Kahtani fue interrogado por las Fuerzas y Cuerpos de seguridad estadounidenses al resultar sospechoso de un delito de terrorismo a raíz de que sus huellas resultaran compatibles con las del secuestrador número 20, quien se encontraba en paradero desconocido.

En su testifical, Mohamed negó reiteradamente haber participado en los ataques terroristas que tuvieron lugar el 11 de septiembre, apoyando su alegato inocente en una identidad falsa.

Mientras se encontraba bajo la custodia de las FFCCSE estadounidenses, el FBI tomó sus datos biométricos, concretamente las huellas dactilares de sus diez dedos de la mano, y las remitió a la base de datos biométricos para su estudio. De forma casi inmediata, la tecnología alertó de que unos datos biométricos referidos a huellas dactilares con alta similitud habían resultado rechazados en la frontera del *Orlando International Airport* el 4 de agosto de 2001, donde figuraba que dichos datos biométricos correspondían a un posible terrorista. Más concretamente, se estimó que las huellas tomadas a Mohamed Al Kahtani eran compatibles con las huellas pertenecientes a un sujeto al que se había denominado "secuestrador número 20" en la investigación de los atentados del 11 de septiembre.

En realidad, este secuestrador número 20 nunca accedió al territorio estadounidense, pero lo que sucedió es que las fuentes policiales disponían de pruebas suficientes que demostraban que los terroristas que efectivamente realizaron los actos del 11-S contaban con él, pues su llegada estaba programada para el mismo día en que llegó al aeropuerto (el 4 de agosto de 2001); pero, sin embargo, nunca efectuó su llegada debido a que la coincidencia de los datos biométricos con los de un sospechoso terrorista hicieron que se le denegase el ingreso al país y se le ofreciera una salida voluntaria.

Fue así como el uso de la videovigilancia, unido a la recopilación de datos biométricos y su cotejo con los datos biométricos ya almacenados en la base de datos, permitió concluir a los investigadores estadounidenses que Kahtani era el "número 20" que no habían podido identificar en el curso de la investigación de los ataques terroristas del 11-S.[99]

[98] También referenciado como *the missing 20th hijacker in the terrorist attacks of 11th September 2001*.

[99] WOODWARD, J. D., "Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism", *Military Review*, 2005, p. 30.

No obstante, a pesar de lo beneficiosa que puede resultar la aplicación de esta técnica en materia de terrorismo, se ha cuestionado si la videovigilancia continuada de espacios públicos puede poner en entredicho el derecho a la intimidad de la ciudadanía. En este sentido, existen opiniones divergentes en cuanto a si el empleo de esta técnica resulta -o no- intrusivo de derechos fundamentales. Así, encontramos dos posicionamientos dominantes, de manera que una parte de la opinión pública entiende que la videovigilancia permanente de espacios públicos arroja resultados positivos, ya que puede constituir evidencias en un proceso penal además de disuadir la comisión de actos ilícitos[100] y, por otra parte, una perspectiva diversa se ubica en la creencia de que el derecho a la intimidad no puede desaparecer al abandonar nuestro domicilio, de manera que esta tendencia entiende que la videovigilancia de espacios públicos comporta un control exacerbado de los individuos que atenta contra libertades individuales.[101]

A pesar de estos posicionamientos dispares, los beneficios arrojados por las técnicas de videovigilancia -con su subsiguiente tratamiento biométrico- a la hora de determinar la autoría de delitos de terrorismo resultan incontrovertibles. Para la consecución de este fin, no obstante, es necesario que los sistemas de videovigilancia instalados cumplan ciertos requisitos como una calidad de imagen estratégica que permita un uso funcional de las imágenes obtenidas y una delimitación del entorno en que se colocan los dispositivos de videovigilancia.[102]

Así, en atención a las exigencias judiciales a la hora de llevar a cabo unas diligencias de investigación, los sistemas de videovigilancia responden a diversas tipologías, entre ellas los sistemas de *Facial Recognition* Capabiliy, que son aquellos que permiten la obtención de imágenes nítidas, lo cual facilitará la aplicación de técnicas biométricas; los sistemas de *Subject Recognition Capability,* más apropiados para trazar al sujeto en un entorno urbano, aunque en el caso de que el sujeto se situara a una distancia mínima del dispositivo, sería posible también la obtención de imágenes nítidas del mismo; los sistemas de *Tracking Recognition* Capability, los cuales no permiten la aplicación de

[100] En este sentido, ULL SALCEDO, M. V., "El derecho a la intimidad como límite de la videovigilancia", *Revista de Derecho Político,* nº 63, 2005, p. 180, pone de manifiesto cómo incluso el propio Consejo de Estado se pronunció en este sentido en su dictamen 549/99, donde destaca que el recurso a la videovigilancia afecta a "un importante elenco de valores e intereses constitucionalmente protegidos."

[101] GUDE FERNÁNDEZ, A., "Videovigilancia privada en lugares de acceso público y derecho a la protección de datos: el caso alemán", *Estudios de Deusto*, 2016, p.74

[102] NÁJERA BAILÓN, S., "Análisis espacial de la videovigilancia como respuesta táctica a los fenómenos del terrorismo y crimen organizado: Caso práctico de Madrid", *Revista del Instituto Español de Estudios Estratégicos,* nº 5, 2015, p. 9

técnicas biométricas *a priori* al adolecer de una baja calidad de imagen pero que, no obstante, cuando se consigue definir al sujeto por diversas imágenes captadas, este tipo de tecnología se usa para determinar otro tipo de cuestiones como, por ejemplo, si el sujeto penetró en el interior del campo visual protegido por este sistema de videovigilancia; y los sistemas de *Plate Recognition Capability*, que tienen una aplicabilidad muy específica, pues sólo cuentan con la calidad necesaria para la identificación de matrículas, de manera que las imágenes que recogen no son aptas para la aplicación de técnicas biométricas de reconocimiento facial.

De esta manera, sólo aquellas tecnologías que presentan una calidad de imagen alta y pueden proporcionar imágenes nítidas aseguran -potencialmente- la aplicación de técnicas biométricas de reconocimiento facial para la identificación de terroristas con éxito.

Desde el punto de vista de nuestro Derecho positivo, a pesar de que la videovigilancia de lugares públicos esté prevista en nuestra legislación, las técnicas biométricas de reconocimiento facial requieren una mención especial en nuestro ordenamiento. Es por ello por lo que el Reglamento General de Protección de Datos (en adelante, RGPD) hace una referencia específica al tratamiento biométrico de los datos obtenidos a partir de sistemas de videovigilancia, incluyéndolos en una categoría especial de protección.

De esta manera, aunque el tenor literal del mismo RGPD establezca una prohibición general al afirmar que "quedan prohibidos el tratamiento de datos biométricos dirigidos a identificar de manera unívoca a una persona física"[103], establece una excepción específica en su apartado segundo, de modo que la prohibición relativa a los datos biométricos no será de aplicación cuando las FFCCSE utilicen dichos datos en el ejercicio de sus funciones[104], con el debido respeto a los derechos y privacidad de las personas afectadas.

Así, considero que los supuestos de uso de datos biométricos recogidos por dispositivos de videovigilancia para combatir el terrorismo quedarían amparados por esta excepción, ya que es evidente que hay un interés público en juego.

[103] Vid. Art. 9.1. Reglamento General de Protección de Datos
[104] Vid. Art. 9.2. g) Reglamento General de Protección de Datos

4.3. Aplicación policial de técnicas biométricas fronterizas en la lucha contra el terrorismo.

El terrorismo abarca una amalgama de complejas amenazas incitando, en ocasiones, a que los sujetos abandonen los países en que se encuentran asentados para desplegar la actividad terrorista en otro Estado extranjero. Es por ello por lo que se ha implementado el uso fronterizo de datos biométricos que, compartidos con los organismos policiales internacionales que luchan contra las redes de terrorismo transnacional, permiten la identificación de terroristas evitando, así, que lleguen a atravesar las fronteras.[105]

La aplicación de las técnicas biométricas se inicia, incluso, en un momento mucho anterior a la llegada del sujeto a la frontera, pues la mayoría de los Estados establecen como requisito previo la emisión de ciertos documentos -por ejemplo, visados- que los sujetos proporcionen atributos de identidad biográfica (como fecha y lugar de nacimiento) y biométrica, como pueden ser una fotografía nítida del rostro con un fondo blanco -que facilitará la aplicación de técnicas biométricas de reconocimiento facial puesto que reduce el efecto barril y las variaciones en el ángulo de captura- y las huellas dactilares tomadas por la autoridad policial competente. En ese momento en que se aportan las huellas dactilares y la fotografía, todo ello se analiza de forma previa a la emisión del visado, lo cual supone la verificación de los datos biométricos aportados en un listado de alerta biométrico.[106]

Sin embargo, interesa centrarse en la capacidad del Cuerpo de Policía de identificar a delincuentes terroristas con un alto grado de precisión y de forma inmediata cuando, por ejemplo, tratan de atravesar una frontera.[107] Esto es posible gracias a la implementación de las tecnologías biométricas, un complemento necesario a los controles de documentos de viaje y de identificación que acabo de mencionar.

---

[105] *Terrorismo* (s.f.) (Últ. Consulta) el 08/04/2022 de https://www.interpol.int/es/Delitos/Terrorismo

[106] *Compendio de prácticas recomendadas de las Naciones Unidas* (s.f.) (Últ. Consulta) el 25/05/2022 de https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_on_biometrics_es.pdf p. 58

[107] *Biometría para la policía de primera línea.* (s.f.) (Últ. Consulta) el 30/05/2022 de https://www.interpol.int/es/Como-trabajamos/I-Core-nuestra-idea-del-cambio/Biometria-para-la-policia-de-primera-linea

Cabe la posibilidad de que la Policía intercambie datos biométricos[108] gracias a acuerdos bilaterales, multilaterales o incluso regionales, y es así como se forman las bases de datos biométricos que facilitan la cooperación policial internacional y, a su vez, la detección de sujetos terroristas al contar con una gran abundancia de datos. Para dotar de gran riqueza estas bases de datos biométricos, la Policía ha creado un proyecto denominado FIRST[109] cuyo objetivo es fomentar el tráfico de datos biométricos relativos a terroristas o presuntos terroristas entre diferentes países.[110]

Además, para asegurar el éxito de este proyecto, se instruye a los funcionarios sobre cómo registrar -y compartir- datos biométricos de sujetos que hayan sido condenados por delitos de terrorismo, lo cual se traduce en una mayor capacidad de los responsables de la Administración de justicia a la hora de localizar a terroristas y efectuar enjuiciamientos e investigaciones con mayor rigor.

Resulta crucial la existencia de los listados de alerta biométricos para posibilitar la identificación de terroristas.[111] Estos listados incluyen las técnicas biométricas de reconocimiento de huellas dactilares, reconocimiento facial e incluso las de reconocimiento de iris en algunos países, y tienen como función la identificación de terroristas o sujetos sospechosos de serlo.

A este fin, se emplean equipos de registro biométrico que tienen incorporados un *software* de búsqueda y un *software* de comparación, de tal manera que esta tecnología contrasta los datos del viajero con los datos biométricos que figuran en una base de datos de INTERPOL denominada "EUROPOL-EIS", la cual incorpora información delictiva y de inteligencia artificial de delitos de terrorismo[112]. En el momento en que los datos del viajero coinciden con alguno de los datos biométricos almacenados en la base de datos, el sistema alerta a las autoridades de la existencia de una amenaza terrorista.

---

[108] De acuerdo con *Compendio de prácticas recomendadas de las Naciones Unidas* op. cit. p. 64, INTERPOL cuenta con tres bases de datos biométricos actualmente, los cuales pueden ser utilizados por 190 países miembros: los relativos a la identificación facial (con información referente a fugitivos y desaparecidos, personas desconocidas de interés, personas cuya imagen aparece en medios de comunicación y fotografías de identificación policial), huellas dactilares y ADN.

[109] Del inglés *Facial, Imaging, Recognition, Searching and Tracking.*

[110] *Identificación de presuntos terroristas* (s.f.) (Últ. Consulta) el 08/04/2022 de https://www.interpol.int/es/Delitos/Terrorismo/Identificacion-de-presuntos-terroristas

[111] *Compendio de prácticas recomendadas de las Naciones Unidas* op. cit. p. 66

[112] *Europol Information System (EIS) A system for information on serious internacional crime* (s.f.) (Últ. Consulta) el 08/04/2022 de https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-information-system

Por último, es preciso traer a colación la implantación de estas técnicas biométricas de reconocimiento facial en el aeropuerto de Barajas, un proyecto iniciado por las compañías aéreas Iberia y Aena. Este sistema biométrico permite que los viajeros puedan efectuar su embarque tras someterse a un reconocimiento facial, y habiendo registrado sus datos faciales en la aplicación de la aerolínea con anterioridad.[113]

El uso adecuado de estos datos biométricos que se empiezan a recoger gracias a la tecnología instaurada en Barajas ha quedado acotado en el articulado del RGPD. De esta manera, en el caso de que no se adoptaran las necesarias medidas de protección de estos datos y ello generase daños indemnizables (por ejemplo, porque los datos de un individuo se difundieran de forma ilícita), ello generará una responsabilidad civil y su correlativo derecho a indemnización.[114] Además, el sujeto cuyo derecho fundamental a la protección de datos se ha visto dañado podría interponer la acción civil contra el responsable o encargado del tratamiento de sus datos haciendo uso del foro de la residencia habitual[115] (esto es, en los tribunales en los que el perjudicado tenga su residencia habitual).

No obstante, cabe señalar que no se prevé la transferencia internacional de los datos biométricos recogidos a partir del sistema de reconocimiento facial instaurado en el aeropuerto de Barajas, salvo obligación legal.[116] Ello contribuye, en última instancia, al vaciamiento de las bases de datos y dificulta a la posibilidad de contar con una base de datos biométricos actualizada a nivel internacional que permita, por ejemplo, conocer la localización exacta o la última frontera frecuentada por un sujeto responsable o sospechoso de un delito de terrorismo.

4.4.Reflexiones finales.

Actualmente, nos encontramos en un momento histórico en el que las tecnologías avanzan a un ritmo frenético, irrumpiendo con fuerza en nuestra cotidianidad. El estudio del Derecho no puede obviar esta nueva realidad social y debe, necesariamente, adaptarse a la misma de la manera más eficiente posible.

[113] PLATERO ALCÓN, A., "El sistema de reconocimiento facial instaurado en el aeropuerto de Barajas: análisis del tratamiento de datos realizado", *Fodertics 9.0*, Granada, 2021, p. 376.
[114] Vid. Art. 82 Reglamento General de Protección de Datos.
[115] Vid. Art. 79.2 Reglamento General de Protección de Datos.
[116] PLATERO ALCÓN, A., "El sistema de reconocimiento facial.., op., cit., p. 377

Derivado de ello, la realidad jurídica actual ha comenzado a servirse de las nuevas tecnologías de la información y de las ventajas que éstas pueden aportar, resultando particularmente destacable el incremento de la aplicación de la biometría para la investigación de delitos de terrorismo. Para que este uso de la biometría resulte fructífero, sin embargo, es necesaria una cooperación interestatal incesante, pues sólo así es posible contrarrestar la amenaza terrorista. Así, el empleo de tecnologías biométricas hace necesario que cada Estado comparta los datos biométricos recolectados diariamente con el resto de los Estados,[117] de tal manera que sea posible confeccionar una base de datos biométricos universal, actualizada y completa.

En este sentido, se hace necesario formular recomendaciones a los diferentes Estados no sólo para que optimicen el uso de las bases de datos biométricos ofrecidos por INTERPOL en el territorio nacional, sino también para que intercambien sus datos biométricos con los diferentes Estados.

De igual modo, se vuelve preceptivo advertir a todos los Estados -ya que cada uno cuenta con idiosincrasia, derecho interno y políticas públicas propias- de la necesidad de observar escrupulosamente la legislación internacional en materia de derechos humanos en lo referido al tratamiento de datos tan sensibles como los datos biométricos. Esto hace imperativo una investigación exhaustiva de las coincidencias de datos biométricos para evitar que, efectivamente, se tomen decisiones precipitadas ante una mera coincidencia de datos biométricos que puede resultar no cierta, pues la tecnología también puede incurrir en errores.

Por último, interesa también fomentar medidas que, a nivel nacional, pongan de manifiesto la gran relevancia que la ciencia forense y biométrica comportan en la lucha contra el terrorismo, siendo ambas herramientas indispensables para combatir el terrorismo no sólo a nivel nacional, sino transnacional.

5. Conclusiones.

[117] *Intercambio de datos biométricos a través de INTERPOL para ayudar a limitar los desplazamientos terroristas* (s.f.) (Últ. Consulta) el 08/04/2022 de https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2019/Intercambio-de-datos-biometricos-a-traves-de-INTERPOL-para-ayudar-a-limitar-los-desplazamientos-terroristas

En el presente Trabajo de Fin de Grado, he tratado de poner de manifiesto la relevancia que presentan las diligencias de investigación tecnológica y la biometría en el esclarecimiento de los hechos delictivos en el mundo contemporáneo, incidiendo en el caso particular de los delitos de terrorismo. Así, la confección de este TFG me ha permitido extraer las siguientes conclusiones:

PRIMERA. Nuestra moderna Ley de Enjuiciamiento Criminal contempla diferentes diligencias de investigación tecnológica, para las que prevé un régimen general que resulta de aplicación subsidiaria con respecto a regulaciones específicas. Ello no es más que una muestra del interés del legislador en dejar atrás la vetusta LECrim, incorporando las tecnologías más disruptivas a nuestro moderno proceso penal a través de una regulación legal estrictamente sujeta a los principios rectores de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad.

SEGUNDA. Los sistemas de videovigilancia, a pesar de no ser una tecnología excesivamente innovadora, presentan ventajas como su bajo coste o la posibilidad de aplicar técnicas biométricas. No obstante, para aplicar técnicas biométricas a las imágenes obtenidas es necesario que las cámaras presenten unas características técnicas elevadas que permitan la captación de imágenes con gran nitidez, mitigando todo tipo de distorsión como, por ejemplo, el efecto barril. Ello debe ser tenido en cuenta con anterioridad a la implantación de un sistema de videovigilancia con potenciales aplicaciones biométricas, evitando así la inserción de sistemas con baja eficacia a nivel procesal penal.

TERCERA. Con respecto al tratamiento Procesal Penal de los presuntos terroristas, he apreciado un cierto adelantamiento de la intervención procesal penal, pues se permite la afección de derechos fundamentales a través de las diligencias procesales de investigación incluso sin autoridad judicial preceptiva. Así, no es preciso que se hayan lesionado bienes jurídicos individuales en particular, sino que en casos de terrorismo tiene cabida la intervención procesal penal simplemente por ser un presunto miembro integrante de un grupo terrorista o estarse formando para ser terrorista, pudiendo hacer uso de las diligencias de investigación tecnológica analizadas por el mero hecho de sospechas fundadas acerca de la existencia de un delito de terrorismo.

CUARTA. En la actualidad, contamos con técnicas biométricas cuya exactitud es tan elevada que prácticamente no cuentan con un margen de error como, por ejemplo, las técnicas de reconocimiento de iris o de la estructura de la retina. No obstante, como he

reflejado en el presente Trabajo de Fin de Grado, y concordando plenamente con lo manifestado por Bueno de Mata[118], son técnicas que tienen costes más elevados, implican una mayor colaboración del investigado y pueden resultar más intrusivas.

Es por ello que, a pesar de su alta precisión y los beneficios que podrían reportar, tienen aplicaciones muy residuales en España. En este sentido, sería deseable un estudio que ofrezca soluciones sobre cómo incorporar dichas técnicas al proceso penal español para dotarlo de mayor precisión y solventar, así, las disfunciones advertidas.

QUINTA. Es cierto que la biometría no puede erradicar al completo el terrorismo, pero sí reducirlo e incrementar la seguridad ciudadana. Es posible, así, aplicar la biometría como técnica preventiva ante ataques terroristas en tanto que puede ser utilizada en un contexto fronterizo para reducir los desplazamientos de los terroristas o bien localizar a sospechosos.

No obstante, considero que es preciso incidir en la necesidad de realizar un análisis y verificar pormenorizadamente los datos biométricos que resulten coincidentes para llevar a cabo esta función preventiva de ataques terroristas. Ello es necesario porque es posible que estemos ante un caso de falsa coincidencia de datos biométricos e identifiquemos a un sujeto como un posible terrorista sin serlo, llegando incluso a tomar acciones de forma precipitada y causar graves afectaciones de DDFF de un presunto terrorista que, eventualmente, resulta no serlo.

SEXTA. Tras advertir que no se prevé la obligación de los Estados de compartir datos biométricos con el resto de los Estados, resulta de especial interés la elaboración de un instrumento internacional que garantice la confección de una base de datos biométricos actualizada y universal a la que todos los Estados deban ceder sus datos biométricos y que, a su vez, obligue a la totalidad de los Estados a respetar las libertades individuales de los ciudadanos cuyos datos biométricos han sido compartidos. Sólo así será posible la aplicación de las técnicas biométricas en la lucha contra el terrorismo de forma satisfactoria.

SÉPTIMA. A pesar de lo acertada que resulta una regulación garantista de diligencias de investigación tan intrusivas como las que han sido objeto de estudio, en ocasiones, la limitada duración de las medidas opera en detrimento de la eficacia de la propia medida.

[118] BUENO DE MATA, F., "Biometría e Investigación Criminal", op., cit., p.132

Esto se ve claramente en la diligencia de registro remoto judicial, donde su escasa duración dificulta la aplicación de la medida, pudiendo incluso imposibilitar la aplicación en su totalidad puesto que, en ocasiones, el servidor no ha proporcionado los datos requeridos para la investigación y la medida ya ha expirado.

Es por ello que debemos mostrarnos críticos a este respecto y señalar que, aunque estas diligencias tan intrusivas no permitan la adopción de plazos excesivamente amplios, es esencial que el cómputo de los plazos sea funcional. Así, creemos que los plazos deberían iniciar su cómputo, en todo caso, desde la fecha en que la medida de investigación resultare efectiva, y no desde la fecha en que el Juez acordare formalmente la medida, pues ello supone que, en ocasiones, la investigación no sólo no arroje ningún resultado concluyente, sino que ni siquiera se llegue a iniciar como consecuencia de la expiración de un plazo tan reducido.

BIBLIOGRAFÍA

ALONSO FERNÁNDEZ, F., COOMONTE BELMONTE, R., ORTEGA GARCÍA, J., *Biometría y Seguridad*, Cuadernos Cátedra ISDEFE-UPM, FUNDETEL, 2008.

AMÉRIGO SÁNCHEZ, J.L., "El régimen jurídico del *malware* según la Ley de Propiedad Intelectual", *Diario La Ley*, nº 8436, 2014.

ARRABAL PLATERO, P., "Las diligencias de investigación tecnológica en el proceso penal español", Revista de Ciencias Sociales: Facultad de Derecho, 2020, págs. 67-108.

BUENO DE MATA, F., "Biometría e investigación criminal", *Revista Eletrônica de Direito Processual*, nº 3, Río de Janeiro, 2020, págs. 121-134.

BUENO DE MATA, F., "El agente encubierto en Internet: mentiras virtuales para alcanzar la justicia", *Los retos del Poder Judicial ante la sociedad globalizada*, Actas del IV Congreso Gallego de Derecho Procesal, Universidad de A Coruña, 2012, págs. 295-306

BUENO DE MATA, F., *Las diligencias de investigación penal en la cuarta revolución industrial*, Aranzadi, Cizur Menor (Navarra), 2019

BUENO DE MATA, F., "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 [BOE n. o 239, 6-X-2015]", *Ars Iuris Salmanticensis*, 2016.

CABEZUDO BAJO, M.J., "La regulación del 'uso forense de la tecnología del ADN' en España y en la Unión Europea", *FODERTICS, Estudios sobre Derecho y nuevas tecnologías,* Santiago de Compostela, 2012, p. 103

CALCEDO MARMOLEJO, L.F., CHAMORRO CARVAJAL, C.E., CRUZ ARDILLA, J.C., VALENCIA MURILLO, J.F., "Extracción de características del iris como mecanismo de identificación biométrica", *Revista Virtual Universidad Católica del Norte*, 2014, págs. 182-196.

CONTRERAS GARCÉS, J., "Transcendencia de los informes periciales de dactiloscopia en los tribunales de justicia", *Ciencia policial: revista del Instituto de Estudios de Policía*, nº 119, 2013, págs. 22-69

CORTÉS OSORIO, J.A., MEDINA AGUIRRE, F.A., MURIEL ESCOBAR J.A., "Sistemas de seguridad basados en biometría", *Scientia et Technica*, nº 46, Pereira (Colombia), 2010, págs. 98-102.

CUETO PERUYERO, R., "La identificación lofoscópica", *Ciencia policial: revista del Instituto de Estudios de Policía*, nº 74, 2004, págs. 29-41.

DELGADO MARTÍN, J., "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015", *Diario la Ley*, Editorial La Ley, 2016, p.14

FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J.A., "Registro de dispositivos de almacenamiento masivo", *Dereito*, vol. 25, nº 2, 2016, p. 37

FOESSEL, M., GARAPON, A., "Biométrie: les nouvelles formes de l'identité", *Espirit*, 2006, págs. 165-172

GIMENO SENDRA, V., "Las intervenciones telefónicas en la jurisprudencia del Tribunal Constitucional y del Tribunal Supremo", *Diario la Ley*, 1996.

GONZÁLEZ-CUÉLLAR SERRANO, N., MARCHENA GÓMEZ, M., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Castillo de Luna, Madrid, 2015

GUDE FERNÁNDEZ, A., "Videovigilancia privada en lugares de acceso público y derecho a la protección de datos: el caso alemán", *Estudios de Deusto*, nº 62, 2016, págs. 74 -116

GUTIÉRREZ NÚÑEZ, C., PELÁEZ GUEVARA, J. "El iris humano como método de identificación forense", *Advocatus*, nº 36, 2021, págs. 181-202

LADRÓN DE GUEVARA PASCUAL, C. *El derecho a la verdad de las víctimas del terrorismo*. Secretaría General de Derechos Humanos, Convivencia y Cooperación, Gobierno Vasco, 2018.

LÓPEZ-BARAJAS PEREA, I., "Aplicación de las tecnologías de la información y de la comunicación a la investigación criminal: la reforma de la Ley de Enjuiciamiento Criminal Española de 2015", *Sistemas, cibernética e informática*, 2016, págs. 163-7

MARTÍN BRAÑAS, C., *Reconocimiento del delincuente: nuevas diligencias de identificación*, Boletín del Ministerio de Justicia, nº 2182, 2015.

MARTÍN MORALES, R., El régimen constitucional del seguimiento directo de personas, Comares, Granada, 2015.

MORENO CATENA, V., "Garantías de los derechos fundamentales en la investigación penal", Revista del Poder Judicial, número 2, 1988, págs. 131-172

NÁJERA BAILÓN, S., "Análisis espacial de la videovigilancia como respuesta táctica a los fenómenos del terrorismo y crimen organizado: Caso práctico de Madrid", *Revista del Instituto Español de Estudios Estratégicos,* nº 5, 2015, págs. 1-26

PLATERO ALCÓN, A., "El sistema de reconocimiento facial instaurado en el aeropuerto de Barajas: análisis del tratamiento de datos realizado", *Fodertics 9.0,* Granada, 2021, págs. 371-380.

RUÍZ DOMÍNGUEZ, F., "Evidencias genéticas militares y persecución penal de los combatientes terroristas extranjeros", *Revista jurídica de Castilla y León,* nº 56, 2022, págs. 81-108.

SÁNCHEZ ÁVILA, C. (2012). Aplicaciones de la biometría en seguridad en: "VIII Ciclo de Conferencias UPM TASSI (Temas Avanzados en Seguridad y Sociedad de la Información)", Campus Sur UPM, Madrid, 2012, págs. 1-78.

SÁNCHEZ CALLE, A. *Aplicaciones de la visión artificial y la biometría*, Editorial Dykinson, Madrid, 2005.

SANTOS MARTÍNEZ, A. M., *Medidas de investigación tecnológica en la instrucción penal*, Bosh-Wolters Kluwer, Barcelona, 2017.

ULL SALCEDO, M. V., "El derecho a la intimidad como límite de la videovigilancia", *Revista de Derecho Político*, nº 63, 2005, págs. 179-201.

VÁZQUEZ DÍAZ, M.Á., "Sistemas de identificación, verificación y autentificación biométricos, una realidad emergente", *Ciencia policial: revista del Instituto de Estudios de Policía,* nº 112, 2012, págs. 29-56.

VEGAS TORRES, J., "Las medidas de investigación tecnológica", *Nuevas tecnologías y derechos fundamentales en el proceso*, Coord. Cedeño Hernán, Aranzadi, Cizur Menor, 2017, págs. 21-47.

WOODWARD, J. D., "Biometrics: facing up to terrorism", *Military Review*, 2001, págs. 1-22.

WOODWARD, J. D., "Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism", *Military Review*, 2005, págs. 30-34.

WEBGRAFÍA

Avances en la identificación de personas mediante las huellas dactilares (s.f.) (Últ. Consulta) el 08/04/2022 de https://ciencia.unam.mx/leer/994/avances-en-la-identificacion-de-personas-mediante-las-huellas-dactilares

Berlín defiende la videovigilancia con reconocimiento facial contra terroristas (s.f.) (Últ. Consulta) el 23/04/2022 de https://www.dw.com/es/berl%C3%ADn-defiende-videovigilancia-con-reconocimiento-facial-contra-terroristas/a-40224938

Biometría para la policía de primera línea. (s.f.) (Últ. Consulta) el 08/04/2022 de https://www.interpol.int/es/Como-trabajamos/I-Core-nuestra-idea-del-cambio/Biometria-para-la-policia-de-primera-linea

Compendio de prácticas recomendadas de las Naciones Unidas (s.f.) (Últ. Consulta) el 12/04/2022 de https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_on_biometrics_es.pdf

El extraño caso de la familia sin huellas dactilares (s.f.) (Últ. Consulta) el 08/04/2022 de https://www.elmundo.es/elmundosalud/2011/08/04/pielsana/1312482983.html

Identificación de presuntos terroristas (s.f.) (Últ. Consulta) el 08/04/2022 de https://www.interpol.int/es/Delitos/Terrorismo/Identificacion-de-presuntos-terroristas

Reconocimiento facial (s.f.) (Últ. Consulta) el 08/04/2022 de https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Reconocimiento-facial

LEGISLACIÓN

Circular 2/2019, de 6 de marzo, de la Fiscal General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas.

Circular 4/2019, de 6 de marzo, de la Fiscal General del Estado, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, BOE núm. 70, de 22 de marzo de 2019, págs. 30138 – 30158

Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre sobre registro de dispositivos y equipos informáticos, BOE núm. 70, de 22 de marzo de 2019, págs. 30159 – 30197

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

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.

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)

RELACIÓN DE SENTENCIAS

SENTENCIAS DEL TRIBUNAL CONSTITUCIONAL

STC 25/2011, 14 de marzo de 2011

STC 199/2013, de 5 de diciembre de 2013

STC 43/2014, de 27 de marzo de 2014

STC 145/2014 de 22 de diciembre de 2014

STC 39/2016 de 3 de marzo de 2016

SENTENCIAS DEL TRIBUNAL SUPREMO

STS 557/2000, 4 de septiembre de 2000

STS 354/2003, 13 de marzo de 2003

STS 248/2004, 26 de febrero de 2004

STS 355/2006, 20 de marzo de 2006

STS 218/2007, 5 de marzo de 2007

STS 562/2007 de 22 de junio de 2007

STS 342/2013 de 17 de abril de 2013

STS 798/2013 de 5 de noviembre de 2013

STS 4742/2014, 31 de octubre de 2014

STS 864/2015 de 10 de diciembre de 2015

STS 77/2017 de 31 de enero de 2017

STS 86/2017 de 1 de febrero de 2017

STS 96/2017 de 2 de febrero de 2017

STS 140/2019 de 13 de marzo de 2019

STS 141/2020 de 13 de mayo de 2020

STS 311/2020, 15 de junio de 2020

STS 3041/2020, 1 de octubre de 2020

SENTENCIAS DE TRIBUNALES EXTRANJEROS

Caso United States v. Antoine Jones, 565 US

Caso Uzun v. Alemania, 35623/05, TEDH 2010

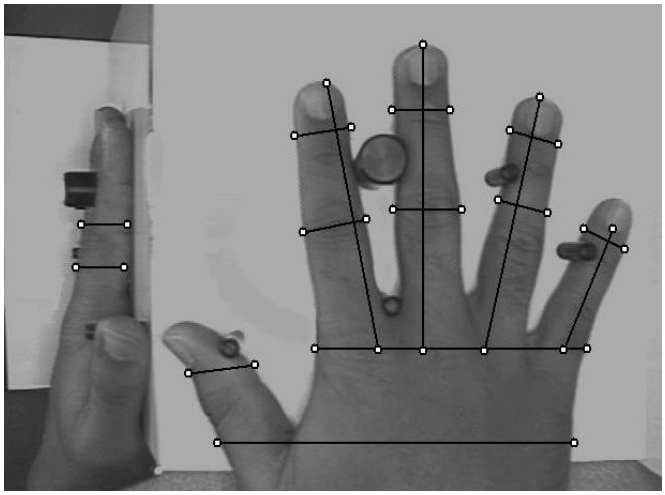
Sentencia del Tribunal de Justicia de la Unión Europea, de 2 de octubre de 2018 (asunto C- 207/16)

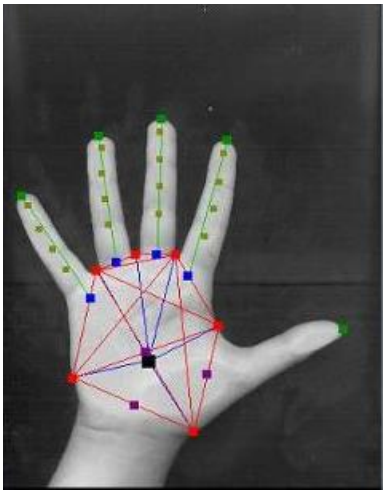
ANEXOS

ANEXO I

Fuente: https://sites.google.com/site/militarcriminalistica/home/dactiloscopia

ANEXO II

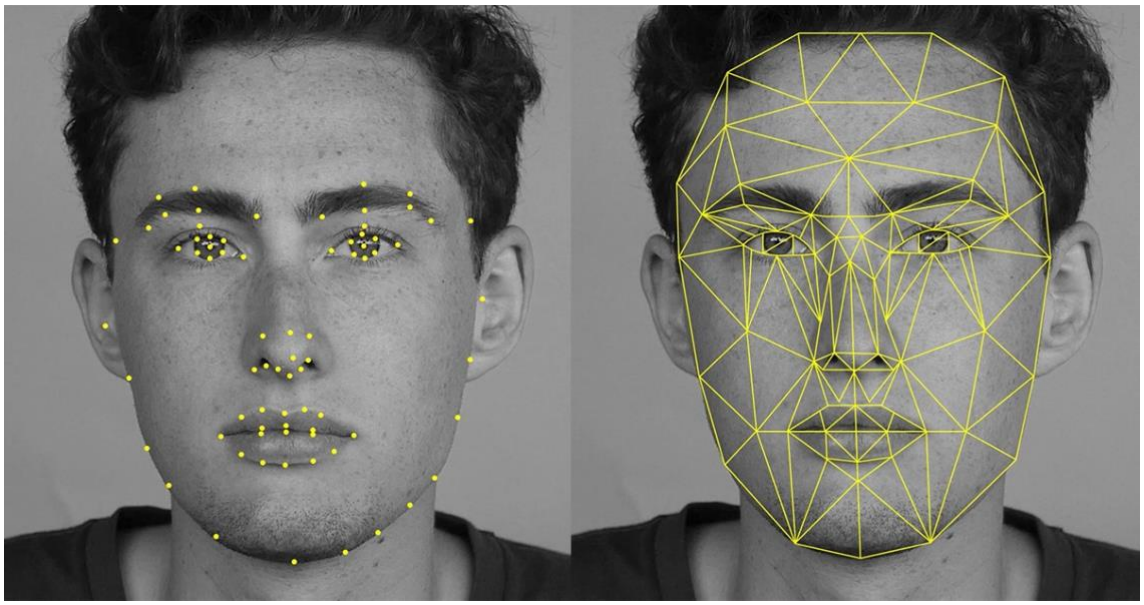




Fuentes: https://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/doc-unixsec/unixsec-html/node120.html

http://dis.um.es/~lopezquesada/documentos/IES_1415/SAD/curso/UT3/ActividadesAlumnos/grupo3/link/preparacion.html

ANEXO III



Fuente: https://silvianane.medium.com/reconocimiento-facial-e-inteligencia-artificial-es-necesario-abrir-el-debate-ciudadano-9bb5ffd5e381