Seguridad e igualdad en la utilización de los sistemas de identificación biométrica en remoto por parte de los cuerpos y fuerzas de seguridad del Estado en tiempos de pandemia

Pablo Gallego Rodríguez
Universidad de Córdoba. Profesor Ayudante Doctor

Sumario.- 1.- Introducción. 2.- La necesidad de identificación. 3.- La constitución española de 1978. 4.- La Estrategia Europea de Datos. 5.- ¿Qué es la inteligencia artificial?. 6.- ¿Qué es la biometría?. 7.- La Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. 8.- La Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la unión COM/2021/206 final. 9.- Voces discrepantes. 10.- A modo de conclusión.

1.- Introducción

El 11 de marzo de 2020 la Organización Mundial de la Salud reconoce como pandemia la situación de emergencia de salud pública ocasionada por el COVID-19.

Esta declaración escenifica el inicio de una nueva era en nuestra sociedad ya que la rapidez en la evolución de los hechos requirió, por parte de la comunidad nacional e internacional, la adopción de una serie de drásticas medidas para hacer frente a esta situación de emergencia de salud pública.

Se abandonaron las oficinas y las aulas y éstas dieron paso a las reuniones virtuales; al teletrabajo y a la educación en remoto. En igual sentido, las pruebas de diagnóstico (PCR) se volvieron habituales y los medios de comunicación informaban

puntualmente de las cifras nacionales e internacionales referentes a los efectos de la pandemia[1].

Dichas medidas afectaron en nuestro ámbito espacial, entre otras, a la libertad de circular por las vías de uso público; a la posibilidad de mantener reuniones privadas; a la libertad de elegir libremente la propia residencia, toda vez que dichas prohibiciones no se graduaron adecuadamente[2].

La Organización Mundial de la Salud ha publicado recientemente un cronograma "*A timeline of who's response to covid-19 in the who european región*" que pretende, por un lado, reflejar los hechos clave de la pandemia y, por otro, servir de punto partida para mejorar la preparación y respuesta ante futuras emergencias de tal magnitud[3].

En este escenario, las redes internacionales de delincuencia organizada han aprovechado la especial situación de indefensión -la mayor parte de los recursos se han destinado principalmente en la atención sanitaria- para burlar la ley haciendo propios los más modernos avances tecnológicos en incrementado las ciberamenazas (phishing; ransomware y DDoS; malware destinado a la obtención de datos; dominios malignos y desinformación entre otros).

En palabras del Secretario General de INTERPOL: "*Los ciberdelincuentes están creando nuevos ataques e intensificando su ejecución a un ritmo alarmante, aprovechándose del miedo y la incertidumbre provocados por la inestabilidad de la situación socioeconómica generada por la COVID-19*"[4].

En igual sentido el informe Panorama mundial de la ciberamenaza relacionada con la COVID-19 indica que: "*Un gran número de delincuentes oportunistas se están*

[1] PUEBLA MARTÍNEZ ÁRBOL, B. y VINADER SEGURA, R., Un año de investigación científica sobre los efectos de la pandemia en Ecosistema de una pandemia: COVID 19, la transformación mundial. Dykinson (2021). p. 21, disponible en: https://dialnet.unirioja.es/servlet/libro?codigo=828116&orden=0&info=open_link_libro [última consulta: 11-03-22].

[2] STC 148/2021 de 14 de julio (BOE núm. 182, de 31 de julio de 2021), disponible en: https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/26778 [última consulta: 11-03-22].

[3] El cronograma de la OMS "A timeline of who's response to covid-19 in the who european región", disponible en: https://www.tiki-toki.com/timeline/embed/1485106/5657264986/#vars!date=2019-12-19_17:06:22! [última consulta: 11-03-22].

[4] STOCK, J., disponible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19 [última consulta: 11-03-22].

aprovechando de la pandemia de COVID-19 para lanzar diversos tipos de ciberataques"[5].

Por ello, ante una situación de pandemia y de creciente expansión de las diversas formas de criminalidad es preciso valorar la dotación y formación de los cuerpos y fuerzas de seguridad en los más avanzados sistemas tecnológicos; entre ellos, el presente trabajo se centra en la identificación biométrica en remoto.

Para IZQUIERDO-CARRASCO los avances en la informática, en el procesamiento de las imágenes y en la inteligencia artificial han promovido importantes avances en los sistemas de reconocimiento facial automático. Su uso conjunto con otros sistemas -como los de videovigilancia- han permitido su utilización "*no sólo en la fase de investigación y persecución del delito, sino también con otros fines más 'amplios como la búsqueda de personas desaparecidas, el control en fronteras o incluso como un instrumento de carácter preventivo en materia de seguridad ciudadana*" [6] pudiendo llegar incidir/afectar a los derechos fundamentales (dignidad; protección datos personales; discriminación; el derecho a un recurso efectivo ante la ley y a un juicio justo; etc.)[7].

Con ello, se podrá determinar de antemano si los riesgos de su utilización son "extremadamente elevados" y por lo tanto deben prohibirse o bien, al contrario, debe regularse y utilizarse como una herramienta indispensable para hacer frente al avance exponencial de las modernas formas criminalidad ante situaciones excepcionales (epidemias; eventos de gran magnitud; paso de fronteras; etc.).

2.- La necesidad de identificación

La necesidad de identificar[8] indubitadamente a una persona por lo que es (biometría) y no solo por lo que conoce o tiene es una necesidad de carácter histórico vinculada al concepto de seguridad.

---

[5] Panorama mundial de la ciberamenaza relacionada con la COVID-19 #WashYourCyberHands, disponible en https://www.interpol.int/es/content/download/15217/file/20COM0312-Cyberthreats-Campain_ProjectSheet%20-%20SP%20-2020-05.pdf [última consulta: 15-01-22].

[6] FRA-European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2020, p. 4., disponible en https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law [última consulta: 15-01-22].

[7] IZQUIERDO-CARRASCO, M., La utilización policial del reconocimiento facial automático en despliegues ocasionales en la vía pública y los derechos fundamentales. Capítulo III, en Inteligencia artificial y defensa. Nuevos horizontes. Thomson Reuters Aranzadi, (2021), p. 66.

* El presente trabajo se ha elaborado en el marco del grupo de Investigación PAIDI SEJ-372, "Democracia, Pluralismo y Ciudadanía" del que el autor es miembro.

En España, el germen normativo de la identificación antropométrica lo encontramos en el Real decreto de 14 de septiembre 1896[9], en virtud del cual y, ante la picaresca de los criminales para burlar la ley, se crea, en las cárceles del Reino, y, de un modo normal y regular, un novedoso sistema de identificación. Su finalidad era triple; por lado, se pretendía descubrir a los criminales de oficio a la vez que abreviar y economizar los procesos judiciales.

Dos siglos más tarde, los criminales siguen intentado delinquir, burlar la ley y pasar desapercibidos; no obstante, tecnológicamente hablando, nuestra sociedad ha evolucionado notablemente.

Nuestro sistema judicial-policial cuenta con una poderosa aliada la informática. El nacimiento de Internet, la existencia de bases de datos biométricas y el uso de la inteligencia artificial ha supuesto un avance sin precedentes en cuanto al almacenamiento y consulta de datos, haciendo posible consultar y verificar de forma prácticamente instantánea millones y millones de datos.

3.- La constitución española de 1978

Es innegable que vivimos en una sociedad altamente digitalizada, en la que la comunicación es prácticamente instantánea, y en la que los avances tecnológicos afectan positivamente al conjunto global de los ciudadanos repercutiendo directamente en sus hábitos y costumbres.

Las ilusiones más fantasiosas de las películas de ciencia ficción[10] parecen hacerse realidad a pasos agigantados y, en cierto modo, se podría afirmar que hemos evolucionado hacia un nuevo tipo de Estado digital y globalizado.

---

[8] Historia de los documentos de identidad. España 1820-2016. D.G. Policía; S.G. Logística. En España, a principios del siglo XIX, las cédulas de identidad y los pasaportes interiores incluían una descripción física de su titular con la que se le podía autorizar a transitar por el interior del territorio español, disponible en https://www.dnielectronico.es/PDFs/Historia_de_los_documentos_de_identidad.pdf [última consulta: 11-03-22].

[9] Gaceta de Madrid: núm. 258, de 14/09/1896, página 985, disponible en https://www.boe.es/datos/pdfs/BOE//1896/258/A00985-00985.pdf [última consulta: 11-03-22].

[10] MUSK, E. asegura que Neuralink empezará a implantar chips cerebrales en humanos en 2022 disponible en https://www.abc.es/ciencia/abci-elon-musk-asegura-neuralink-empezara-implantar-chips-cerebrales-humanos-2022-202112170110_noticia.html?ref=https%3A%2F%2Fwww.google.com%2F [última consulta: 11-03-22].

Los ciudadanos nos hemos adaptado rápidamente a este nuevo tipo de sociedad pasado de ser meros consumidores de contenidos a ser productores de los mismos. Además, todo parece valer para obtener un cierto reconocimiento digital.

Paralelamente a este hecho, las acciones que deberían resultar más sencillas y accesibles como solicitar una cita ante la administración implica, en numerosas ocasiones, implican unos conocimientos digitales - que no parecen respetar el contenido del artículo 9.2 CE-, generando nuevas formas de exclusión social.

Todo ello, unido al potencial peligro que conlleva su uso indiscriminado frente a nuestro régimen de derechos y libertades hace necesario, hoy más que nunca, disponer de un preciso marco legal tanto nacional como internacional capaz de adaptarse rápidamente a las nueva realidad digital en aras a la consecución de un eficaz sistema de garantía de las libertades y derechos fundamentales.

Nuestro vigente texto constitucional ha sido uno de los primeros en prestar una especial atención al uso de la informática "*dado que es precisamente en los años de su redacción cuando comienzan a apreciarse los peligros que puede entrañar el archivo y uso ilimitado de los datos informáticos*"[11].

El artículo 18.4 CE, cuya aprobación no estuvo exenta de un rico debate parlamentario, subraya la especial atención que debe prestar el legislador en cuanto al uso de la informática y como la ley debe limitar su uso para que el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos queden debidamente garantizados.

Para nuestro Tribunal Constitucional la informática ha sido una preocupación constante.

En una primera fase se consideró que este derecho se encontraba íntimamente vinculado al derecho a la intimidad pero, en un momento posterior, STC 254/1993 de 20 de julio, se consideró que el texto constitucional había incorporado una nueva garantía en respuesta a una nueva amenaza a la dignidad y a los derechos de la persona[12].

---

[11] ELVIRA PERALES, A., y actualizado (2011) por GONZÁLEZ ESCUDERO, A., *Sinopsis artículo 18.* Congreso de los Diputados, disponible en https://app.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2 [última consulta: 11-03-22].

[12] STC 254/1993, de 20 de julio (BOE núm. 197 de 18 de agosto de 1993) disponible en https://hj.tribunalconstitucional.es/docs/BOE/BOE-T-1993-21425.pdf [última consulta: 11-03-22].

La STC 94/1998, de 4 de mayo, que a su vez hace referencia a la STC 254/1993, hace propia la declaración de que el artículo 18.4 CE incorpora una nueva garantía a los derechos y libertades fundamentales, con una especial referencia al derecho al honor y a la intimidad.

De igual forma, la sentencia hace referencia a un denominado "*habeas data*" que se concreta en el derecho a controlar el uso de estos una vez que se han incorporado en un programa informático así como la posible oposición por parte de los ciudadanos a que estos datos de carácter personal sean utilizados con fines diferentes a los que dieron origen a su obtención.

La sentencia incide en que el uso informatizado de datos con fines diferentes a los autorizados podrían constituir un "*grave atentado a los derechos fundamentales de la persona*" y, por lo tanto esta utilización indebida podría ser objeto de la oportuna demanda de amparo.

Seguidamente la sentencia hace referencia a la legislación que desarrolla lo previsto en el artículo 18.4 y hace especial mención a modo de "*principio cardinal*" de la protección de datos a los principios de congruencia y racionalidad en su utilización, haciendo una especial mención a modo de tutela reforzada respecto de los datos sensibles, a la vez que prohíbe taxativamente su uso para finalidades diferentes a aquellas que motivaron su obtención legítima a la vez que reconoce una tutela reforzada respecto de los datos sensibles[13].

La STC17/2013, de 31 de enero concreta jurídicamente la posible oposición del ciudadano a que determinados datos personales sean utilizados indiscriminadamente para fines distintos de aquel legítimo que justificó su obtención ya sea por el propio Estado o un particular[14].

Respecto al debate sobre si las imágenes grabadas en un soporte físico constituyen o no un dato de carácter personal bajo el amparo del artículo 18.4 de nuestro texto constitucional la STC 29/2013, de 11 de febrero reconoce que estas constituyen un dato de carácter personal que queda integrado en la cobertura del art. 18.4 CE, puesto que el derecho fundamental amplía la garantía constitucional a todos los datos que identifiquen

[13] STC 94/1998, de 4 de mayo (BOE núm. 137 de 09 de junio de 1998), disponible en https://hj.tribunalconstitucional.es/docs/BOE/BOE-T-1998-13334.pdf [última consulta: 11-03-22].
[14] STC 17/2013, de 31 de enero (BOE núm. 49 de 26 de febrero de 2013), disponible en https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/23272 [última consulta: 11-03-22].

o permitan la identificación de la persona y que, a su vez, puedan servir para la confeccionar un perfil personal o para cualquier otra actividad que pueda llegar a constituir una amenaza para sus derechos[15].

La recientemente la STC 27/2020, de 24 de febrero analiza la vulneración del derecho a la propia imagen ante un reportaje periodístico que se documenta con una fotografía extraída de un perfil personal de Facebook (utilización no autorizada de la imagen ajena en la denominada sociedad digital). La sentencia hace hincapié en que en la era digital los usuarios continúan siendo titulares de derechos fundamentales y que su contenido es el mismo que en la era analógica.

Otro área a tener en cuenta es la progresiva y cada vez mayor europeización de este ámbito que partiendo del Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del Consejo de Europa que significó el primer instrumento internacional jurídicamente vinculante en el ámbito de la protección de datos. En virtud del Convenio, las Partes deben adoptar las medidas necesarias en su Derecho nacional para aplicar sus principios, a fin de garantizar, en su territorio, el respeto de los derechos humanos fundamentales en el ámbito de la aplicación de la protección de datos[16].

Por su parte, el citado derecho se encuentra reconocido en la Carta de los Derechos Fundamentales de la Unión Europea en su artículo 8[17] y en artículo 16.1 del Tratado de Funcionamiento de la Unión Europea se consagra como uno de los principios de la Unión.

Su inclusión en la Carta de los Derechos Fundamentales de la Unión Europea ha originado diferentes Sentencias del Tribunal de Justicia de la Unión Europea; entre ellas las de fecha 8 de abril de 2014 "*Digital Rights Ireland, Seitlinger Tschohl y otros*"[18]; la de 13 de mayo de 2014 "*Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González. Petición de decisión prejudicial*

---

[15] STC 29/2013, de 11 de febrero. (BOE núm. 61 de 12 de marzo de 2013), disponible en https://hj.tribunalconstitucional.es/docs/BOE/BOE-A-2013-2712.pdf [última consulta: 11-03-22].

[16] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), disponible en https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108 [última consulta: 11-03-22].

[17] Carta de los Derechos Fundamentales de la Unión Europea. (2000/C 364/01). Diario Oficial de las Comunidades Europeas, disponible en https://www.europarl.europa.eu/charter/pdf/text_es.pdf [última consulta: 11-03-22]. "*Artículo 8 Protección de datos de carácter personal*"

[18] Sentencia del Tribunal de Justicia de la Unión Europea de fecha 8 de abril de 2014 "*Digital Rights Ireland, Seitlinger Tschohl y otros.*" disponible en https://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=ES [última consulta: 11-03-22].

planteada por la Audiencia Nacional."[19] y la de 6 octubre de 2015 fecha "*Maximillian Schrems y Data Protection Commissioner*"[20].

Por su parte, el Tribunal Europeo de Derecho Humanos ha producido una importantísima base jurisprudencial. No es objeto del presente trabajo una análisis detallado de la misma y, dada la importancia del mismo al objeto del presente estudio, se hace una referencia en este momento a la "*Guide to the Case-Law of the of the European Court of Human Rights. Data protection. Genetic and biometric data*"[21].

4.- La Estrategia Europea de Datos

La innovación basada en los datos implicará mejoras en diversas áreas entre las que se podrían destacar la seguridad, la medicina y la movilidad. Cada día generamos mayores cantidades de datos por lo que es sumamente importante la forma en la que estos se recogen y utilizan ya que solo confiaremos en estas innovaciones en la medida en que estas estén sujetas "*al pleno respeto de sus estrictas normas en materia de protección de datos*"[22].

La Estrategia Europea de Datos prevé que para el año 2025 la cifras serán las siguientes[23]:

- 530 % – incremento del volumen global de datos. de 33 zetabytes en 2018 a 175 zetabytes.
- 829.000 millones de euros. valor de la economía de los datos en la EU27 frente a 301.000 millones de euros (2,4 % del PIB de la UE) en 2018

---

[19] Sentencia del Tribunal de Justicia de la Unión Europea de fecha 13 de mayo de 2014 "*Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González. Petición de decisión prejudicial planteada por la Audiencia Nacional.*", disponible en https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:62012CJ0131 [última consulta: 11-03-22].

[20] Sentencia del Tribunal de Justicia de la Unión Europea de fecha 6 de octubre de 2015 "*Maximillian Schrems y Data Protection Commissioner*", disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62014CJ0362 [última consulta: 11-03-22].

[21] Guide to the Case-Law of the of the European Court of Human Rights. Data protection (Updated on 30 April 2021). European Court of Human Rights (Tribunal Europeo de Derechos Humanos; TEDH), disponible en https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf [última consulta: 11-03-22].

[22] Una Estrategia Europea de Datos. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Bruselas, 19.2.2020. COM(2020) 66 final, disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066 [última consulta: 11-03-22].

[23] Disponible en https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es [última consulta: 11-03-22].

- 10,9 millones de profesionales de los datos en la EU27. frente a 5,7 millones en 2018
- 65 % porcentaje de población de la UE con competencias digitales básicas. frente al 57 % en 2018

A este respecto es preciso indicar que hoy en día, un reducido número de grandes empresas posee la mayor parte de los datos del mundo.

Dada la ingente magnitud de los datos se hace preciso un sistema, una herramienta, que nos auxilie en la búsqueda de la información pertinente y para ello podríamos contar con la inteligencia artificial y que a nuestro parecer debe ser entendida como una herramienta más que proporciona una valiosísima información tanto dentro como fuera en el ámbito penal.

5.- ¿Qué es la inteligencia artificial?

La inteligencia artificial dista mucho de ser un tipo avanzado de software o un tipo de programa informático, ya que estos únicamente se conforman por líneas o árboles de comandos sin posibilidad ni capacidad de salirse de ellos mientras que, a grandes rasgos, la inteligencia artificial busca soluciones sin la intervención humana en base a los datos que tiene a su alcance.

Su origen aunque pueda parecernos reciente lo podemos encontrar, según un novedoso estudio realizado en la Universidad de Stanfor, en los poetas griegos[24].

Para el Parlamento Europeo la inteligencia artificial podría definirse como: "*(...) la habilidad de una máquina de presentar las mismas capacidades que los seres humanos, como el razonamiento, el aprendizaje, la creatividad y la capacidad de planear. La IA permite que los sistemas tecnológicos perciban su entorno, se relacionen con él, resuelvan problemas y actúen con un fin específico. La máquina recibe datos (ya preparados o recopilados a través de sus propios sensores, por ejemplo, una cámara), los procesa y responde a ellos. Los sistemas de IA son capaces de adaptar su*

[24] MAYOR A., *Gods and Robots: Myths, Machines, and Ancient Dreams of Technology*, Princenton. University Press, 2018.

comportamiento en cierta medida, analizar los efectos de acciones previas y de trabajar de manera autónoma."[25].

Para el Libro Blanco sobre inteligencia artificial esta se está desarrollando de una forma vertiginosa y "*Cambiará nuestras vidas, pues mejorará la atención sanitaria (por ejemplo, incrementando la precisión de los diagnósticos y permitiendo una mejor prevención de las enfermedades), aumentará la eficiencia de la agricultura, contribuirá a la mitigación del cambio climático y a la correspondiente adaptación, mejorará la eficiencia de los sistemas de producción a través de un mantenimiento predictivo, aumentará la seguridad de los europeos y nos aportará otros muchos cambios que de momento solo podemos intuir.*"; de igual forma "*conlleva una serie de riesgos potenciales, como la opacidad en la toma de decisiones, la discriminación de género o de otro tipo, la intromisión en nuestras vidas privadas o su uso con fines delictivos.*"[26].

6.- ¿Qué es la biometría?

Para el Instituto Nacional de Ciberseguridad español la biometría es "*un método de reconocimiento de personas basado en sus características fisiológicas o de comportamiento"* y, por ello, "s*e trata de un proceso similar al que habitualmente realiza el ser humano reconociendo e identificando a sus congéneres por su aspecto físico, su voz, su forma de andar*"[27].

En cuanto a sus características y las tecnologías para medirlas estas son[28]:

- Características: universalidad: todos los individuos las tienen; singularidad o univocidad: distinguen a cada individuo; permanencia en el tiempo y en distintas condiciones ambientales; medibles de forma cuantitativa
- Tecnología: rendimiento: nivel de exactitud; aceptación: por parte del usuario; resistencia al fraude y usurpación

---

[25] Parlamento Europeo, disponible en https://www.europarl.europa.eu/news/es/headlines/society/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa [última consulta: 11-03-22].

[26] Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza. Bruselas, 19.2.2020, COM(2020) 65 final, disponible en https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf [última consulta: 11-03-22].

[27] *Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario*. INCIBE (Instituto Nacional de Ciberseguridad) 2016 p. 4, disponible en https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf [última consulta: 11-03-22].

[28] *Ibidem* p. 5.

En el proceso de autenticación se captura una muestra biométrica y esta se compara con la base o plantilla de la previamente registrada con el objeto de lograr su identificación[29]. Este proceso puede realizarse de dos formas diferentes[30]:

- Identificación: la comparación de la muestra recogida se realiza frente a una base de datos de rasgos biométricos registrados previamente. No hay una identificación previa por lo que el método requiere de un proceso de cálculo complejo ya que es necesario comparar la muestra con todas y cada una de las almacenadas hasta localizar la que coincida.
- Verificación: el proceso es más sencillo ya que en un primer momento se aporta un registro que puede ser un nombre de usuario, tarjeta o algún otro método. Este registro selecciona de la base de datos un patrón anteriormente registrado y se procede a la comparación cuyo resultado es positivo o negativo.

Dentro de las tecnologías biométricas nos encontramos con diferentes tipos[31]:

- aquellas que analizan su comportamiento: reconocimiento de firma; reconocimiento de escritura de teclado; reconocimiento de voz; reconocimiento de la forma de andar
- aquellas que analizan características fisiológicas de las personas: huella dactilar; reconocimiento facial; reconocimiento de iris; reconocimiento de la geometría de la mano; reconocimiento de retina; reconocimiento vascular
- Otras: líneas de la palma de la mano; forma de las orejas; piel, textura de la superficie dérmica; ADN, patrones personales en el genoma humano; composición química del olor corporal.

Como podemos observar y lejos de lo que inicialmente podríamos pensar, las diversas tecnologías biométricas que nos encontramos son sumamente numerosas.

Por otro lado, son numerosos los equívocos y bulos que se dan con relación a la identificación y a la autenticación biométrica. Por ejemplo, la idea general es que la

[29] MORENO DÍAZ, A. B., Reconocimiento facial automático mediante técnicas de visión tridimensional, disponible en https://oa.upm.es/625/ [última consulta: 11-03-22].
[30] *Ibidem* p. 6.
[31] *Ibidem* pp. 7-12.

autenticación biométrica es fuerte cuando es un sistema débil -un sistema de autenticación fuerte es aquel que requiere que se proporcione, al menos, dos de los siguientes elementos: algo que se sabe, algo que se tiene o algo que se es (biometría)- o que todo tratamiento biométrico implica identificación/autenticación y no es así de forma estrictamente necesaria ya que por ejemplo, el tratamiento biométrico del movimiento del ratón utilizado para determinar si es un humano o un robot el que está accediendo a una página web, implica tratar la información biométrica para diferenciar humano de máquina[32].

De igual forma, debemos prestar una especial atención a nuestros datos biométricos, ya que estos permanecen, salvo causas excepcionales como accidentes, lesiones, etc., inmutables y no podemos modificarlos o cambiarlos a nuestro antojo tal y como podríamos hacer con la clave de acceso a nuestra cuenta de correo.

7.- La Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

El preámbulo comienza haciendo referencia a las crecientes amenazas para la seguridad en el contexto nacional e internacional y al componente transfronterizo de las mismas y como este hecho justifica, a modo de objetivo ineludible, la cooperación internacional y la transmisión de información de carácter personal entre los servicios policiales y judiciales de los diferentes países.

Respecto a los datos biométricos, -huellas dactilares; imagen facial- objeto de la presente investigación, éstos no siempre forman parte de la denominada categoría especial y sólo forman parte de ella, cuando su tratamiento está dirigido a la identificación de manera unívoca de una persona física, que resulta necesaria para poder singularizar a los autores o partícipes de una infracción penal y de esta forma atribuir o exonerar, sin género de dudas, su participación en determinados hechos, gracias a posibles indicios o vestigios biométricos.

[32] 14 equívocos con relación a la identificación y autenticación biométrica. 2020. AEDP (Agencia española de protección de datos) pp. 3-4, disponible en https://www.aepd.es/sites/default/files/2020-06/nota-equivocos-biometria.pdf [última consulta: 11-03-22].

El objeto de la Ley se recoge en el artículo 1 y no es otro que el de establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal con unos fines determinados que son:

- a prevención,
- la detección,
- la investigación y
- el enjuiciamiento

de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

Este tratamiento se realiza por parte de las denominadas "autoridades competentes" descritas en el artículo 4 y que es toda autoridad pública que tenga competencias encomendadas legalmente para el tratamiento de datos personales con alguno de los fines previstos por la Ley. Es decir, en el ámbito de sus respectivas competencias, autoridades competentes serían: Las Fuerzas y Cuerpos de Seguridad; Las Administraciones Penitenciarias; la Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria; el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y la Comisión de Vigilancia de Actividades de Financiación del Terrorismo a las que habría que añadir a las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal.

Con todo ello, queda bien claro el objeto -tratamiento de datos personales- así como los fines -prevención; detección; investigación y el enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública-.

En el artículo 5 encontramos la definición de «datos biométricos» y esta hace referencia a datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

El artículo 13 se encuentra en consonancia con el artículo 10 de la Directiva 2016/680 y que hace referencia al tratamiento de categorías especiales de datos personales.

Según se desprende de su contenido el tratamiento de datos biométricos dirigidos a identificar de manera unívoca a una persona física sólo se permitirán cuando sea estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado y cuando se cumplan alguna de las siguientes circunstancias:

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

Respecto al apartado c) datos que el interesado haya hecho manifiestamente públicos *motu propio* no es posible tratar los datos que figuran en un boletín oficial como manifiestamente públicos ya que la Agencia Española de Protección de datos ha entendido que estos datos han sido publicados por imperativo legal y no por la propia voluntad del interesado. Por otro lado, como nos indican "*si alguien publica en las redes sociales en abierto que es simpatizante de una opción política x, podría llegar a ampararse el uso de los datos si se cumplen el resto de los presupuestos*"[33].

Para los citados autores "*es impensable que los cuerpos policiales o el resto de autorizades competentes tengan un fichero con datos de opiniones políticas o convicciones religiosas de las personas por el mero hecho de tenerlas*" salvo que éstas tengan "*una serie de opiniones políticas extremistas que hagan apología del odio o se tratan de una investigación por terrorismo en el que se dan las circunstancias que hagan necesario tratar datos*" en cuyo caso y "*en una infinidad de ejemplos*" similares nos indican que su opinión se podrían tratar esos datos ya que existe el amparo legal "*claro*" para realizarlo[34].

Por otro lado, es el segundo apartado el que nos indica quienes podrán tratar estos datos, las autoridades competentes a las que nos hemos referido en el anteriormente y a los meros fines de prevención, investigación, detección de infracciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

[33] AYLLÓN SANTIAGO, H. S. y FERNÁNDEZ GONZÁLEZ, C. M. Tratamiento de datos de carácter personal en el ámbito policial, Reus, 2021, p. 104.
[34] *Ibidem*, p. 105.

El artículo 14 de la Ley Orgánica hace referencia a los mecanismos de decisión individual automatizado, prohibiendo las decisiones basadas únicamente en un tratamiento automatizado en el que se incluye la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o que le afecten significativamente.

A su vez, en el citado artículo se contiene una posible habilitación que pasaría por la autorización expresa por una norma nacional con rango de ley o por el Derecho de la Unión Europea. Dicha norma -norma habilitante para el tratamiento- deberá establecer las medidas adecuadas para la salvaguarda de los derechos y libertades e incluir el derecho a obtener la intervención humana en el proceso de revisión de la decisión adoptada.

El contenido del artículo 14.2 es sumamente interesante y a nuestro criterio podría contener el presupuesto habilitante para utilización de los mecanismos automatizados, ya que indica que éstas no se basarán en las categorías especiales entre las que encontramos los datos biométricos salvo y aquí viene lo realmente importante a nuestros efectos que se hayan tomados las medidas adecuadas para la salvaguarda de los derechos y libertades y los intereses legítimos de los interesados. Para nosotros este punto es especialmente importante y debe conectarse con el contenido de los artículos 35 y 36 que hacen referencia respectivamente a la evaluación del impacto y a consulta previa.

Por último el tercer apartado del artículo 14 prohíbe la elaboración de perfiles que dé lugar a una discriminación de las personas físicas sobre la base de categorías especiales de datos personales establecidas en el artículo 13. Lo cual al mismo tiempo constituye una garantía ya que en este apartado, en el que se incluye la biometría, no se recoge ninguna posible habilitación.

El tratamiento de los datos personales en el ámbito de la videovigilancia por Fuerzas y Cuerpos de seguridad se recoge de forma exhaustiva en la sección 2ª del Capítulo II (artículos 15 a 19). Su tramitación ha generado un amplio debate parlamentario hasta el punto de que el Dictamen del Consejo de Estado[35] propició modificaciones al texto inicialmente presentado.

[35] Dictamen del Consejo de Estado de 28 de enero de 2021 (675/2020 (INTERIOR), disponible en https://www.boe.es/buscar/doc.php?id=CE-D-2020-675 [última consulta: 11-03-22].

Por nuestra parte, dadas las importantísimas implicaciones para la protección de los derechos y libertades en cuanto a la utilización de sistemas de grabación de imágenes y sonido por los Cuerpos y Fuerzas de Seguridad en lugares públicos y para clarificar el régimen jurídico aplicable coincidimos con MARCOS AYJON en que "*debería publicarse una norma que aglutine todo el régimen jurídico del tratamiento de los datos personales procedentes de la utilización de estos instrumentos de grabación de imágenes y sonidos*"[36].

La Ley Orgánica en el artículo 35 establece una salvaguarda en la protección de los derechos y libertades de las personas físicas, ya que exige una previa evaluación de impacto cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, que suponga por su naturaleza, alcance, contexto o fines, un alto riesgo para los derechos y libertades de las personas físicas.

Otra de las salvaguardas contenidas en la ley es la que se recoge en el artículo 36, por la que se obliga al responsable o el encargado del tratamiento de datos personales que, vayan a formar parte de un nuevo fichero, a realizar una consulta previa a la autoridad de protección de datos antes de tratar datos que hayan sido calificados como alto nivel de riesgo o cuando debido a la utilización de tecnologías, mecanismos o procedimientos novedosos se pueda generar un alto nivel de riesgo para los derechos y libertades de los interesados.

Con todo ello, consideramos que en nuestro ordenamiento existen las herramientas oportunas para la protección de los derechos y libertades al tiempo que lo organismos internaciones están haciendo un notable esfuerzo para su consecución.

8.- La Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la unión COM/2021/206 final

La Propuesta de Reglamento se encuentra, como su nombre indica, en fase de debate por lo que únicamente nos detendremos en dos de sus aspectos de especial

[36] MARCOS AYJON, M., «La nueva Ley Orgánica para la protección de datos personales en la prevención, investigación, enjuiciamiento de delitos y ejecución de penas» La Ley privacidad, N.º 8, 2021, p. 12.

relevancia para la presente investigación dejando su estudio para una posterior investigación.

En el artículo 5 se detallan las prácticas de inteligencia artificial que se encuentran prohibidas entre las que encontramos aquellas que se sirvan de técnicas subliminales; aquellas que aprovechen la vulnerabilidad de un grupo de personas para alterar de manera sustancial su comportamiento; aquellas que tengan por finalidad evaluar y clasificar la fiabilidad de las personas y, lo más relevante para el presente estudio el uso de los sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público. Salvo que su uso sea estrictamente necesario para alcanzar alguno de objetivos siguientes:

- la búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos;
- la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista;
- la detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI del Consejo 62 , para el que la normativa en vigor en el Estado miembro implicado imponga una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de tres años, según determine el Derecho de dicho Estado miembro.

El artículo continúa haciendo referencia al uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público que deberán tener en cuenta:

- a) la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema;
- b) las consecuencias que utilizar el sistema tendría para los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias.

Resulta especialmente relevante el contenido del apartado 3 ya que el uso del sistema de identificación biométrico remoto y en tiempo real estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente del Estado miembro donde vaya a utilizarse dicho sistema.

El apartado 4 parece fijar una cláusula de salvaguarda, ya que nos indica que ante una en una situación de urgencia debidamente justificada, se podrá empezar a utilizar el sistema antes de obtener la autorización correspondiente, que podrá solicitarse durante el uso o después.

A nuestro criterio, este apartado no está exento de riesgos para la protección de los derechos y libertades fundamentales de las personas por mucho que se indique que la autoridad judicial o administrativa competente únicamente concederá la autorización cuando esté convencida, atendiendo a las pruebas objetivas o a los indicios claros que se le presenten, de que el uso del sistema de identificación biométrica remota «en tiempo real» es necesario y proporcionado.

Al mismo tiempo creemos que la propuesta de Reglamento debería ser más prolija, aun a riesgo de "*sufrir*" dificultades en cuanto a su aprobación en el desarrollo del apartado 4 en el que se establece que los Estados miembros podrán decidir contemplar la posibilidad de autorizar, ya sea total o parcialmente, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público y que a tal fin, tendrán que establecer en sus respectivos Derechos internos las normas detalladas necesarias aplicables a la solicitud, la concesión y el ejercicio de las autorizaciones.

Por último, en el artículo 6 se establecen las reglas de clasificación para los sistemas que se consideran de alto riesgo.

Como hemos indicado anteriormente, no es objeto de la presente investigación hacer un estudio detallado de la Propuesta de Reglamento, que en líneas generales parece limitar la habilitación legal para la utilización de los denominados sistema de identificación biométrica remota «en tiempo real». Por otro lado, es evidente que estos sistemas pueden comportar importantísimas ventajas en la prevención, detección, investigación y enjuiciamiento de infracciones penales a la vez que pueden comportar serías repercusiones negativas para los derechos fundamentales de las personas.

9.- Voces discrepantes

Europa ha mantenido una posición dubitativa respecto al uso de la inteligencia artificial, según se desprende del informe National strategies on Artificial Intelligence: A European perspective[37] y algunos países como Suecia han multado el uso del reconocimiento facial para controlar la asistencia -escuela de Skelleftea- mientras que otros como Francia proponen a través de CNIL -Commission Nationale de l'Informatique et des Libertés[38]- distinguir cuándo un reconocimiento facial es necesario y cuando no.

Hoy en día existen voces discrepantes que abogan por la prohibición absoluta de su uso y férreos defensores.

Cada vez son más los colectivos que abogan por la supervisión humana de los sistemas de inteligencia artificial. Por ejemplo, la Eurocámara votó en octubre de 2021 una resolución no vinculante sobre los modelos de inteligencia artificial empleados por los cuerpos policiales para facilitar el reconocimiento a través de datos biométricos, así como para garantizar sistemas de vigilancia masivos. La resolución prosperó por 377 votos a favor, 248 en contra y 62 abstenciones analiza los riesgos que conllevan los sesgos en algoritmos a la vez que enfatiza en la necesidad de que estos modelos estén bajo supervisión humana y sometidos a un intenso escrutinio legal, sobre todo en contextos transfronterizos[39].

10.- A modo de conclusión

La sociedad española de los años 70 no estaba familiarizada con el uso de la informática; no obstante, los padres de la Constitución de 1978, conscientes de los posibles riesgos que podría entrañar prestaron especial atención a su regulación.

El Tribunal Constitucional por su parte ha reconocido una nueva garantía constitucional a la vez que reitera que los usuarios continúan siendo titulares de derechos fundamentales y que su contenido continúa siendo el mismo que en la era analógica.

---

[37] VAN ROY, V., ROSSETTI, F., PERSET, K. and GALINDO-ROMERO, L., AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition, EUR 30745 EN, Publications Office of the European Union, Luxembourg, 2021, disponible en https://publications.jrc.ec.europa.eu/repository/handle/JRC122684 [última consulta: 11-03-22].

[38] Disponible en https://www.cnil.fr/

[39] European Parliament. News Use of artificial intelligence by the police: MEPs oppose mass surveillance, disponible en https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance [última consulta: 11-03-22].

Hoy en día vivimos en un nuevo tipo de Estado, el Estado digital en el que ciudadanía manifiesta un alto grado de dependencia digital.

De igual forma las redes de delincuencia organizada constituyen negocios multimillonarios que operan a escala internacional utilizando los últimos avances tecnológicos para tartar de burlar la ley.

La sociedad se encuentra altamente polarizada entre los que consideran legitima cualquier utilización de los sistemas de identificación biométrica en remoto por parte de los cuerpos y fuerzas de seguridad del Estado en tiempos de pandemia ya que estas pueden ofrecer mayor confianza; seguridad; transparencia y agilización de las investigaciones con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección frente a las amenazas contra la seguridad pública y los que consideran que éstas pueden ocasionar una intromisión ilegítima y desproporcionada en el ámbito de los derechos y libertades fundamentales.

Ante esta situación nuestro marco legal tanto nacional como internacional se muestra impreciso e ineficaz limitándose, en muchas ocasiones, a parchear el sistema.

Por ello, es preceptiva la constitución de equipos multidisciplinares que aborden e integren las diferentes tecnologías existentes -bases de datos biométricas; computación cuántica; inteligencia artificial- y que ofrezcan una respuesta legal global que dote a nuestros cuerpos y fuerzas de seguridad de las herramientas oportunas -formación; confianza, trazabilidad- para una rápida, eficaz y adecuada persecución de los delitos a la vez que doten a nuestro sistema judicial de una más que necesaria modernización y que respeten y protejan los derechos fundamentales de las personas a la vez que pongan fin a desigualdades de los colectivos más desfavorecidos a los que una sociedad plural no debe desatender.