RECONOCIMIENTO FACIAL AUTOMATIZADO Y SISTEMAS DE IDENTIFICACIÓN BIOMÉTRICA BAJO LA REGULACIÓN SUPERPUESTA DE INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DE DATOS[1]

Lorenzo Cotino Hueso*

1 Realizado en el marco de los proyectos "Derecho, Cambio Climático y Big Data", Grupo de Investigación en Derecho Público y TIC; MICINN "Derechos y garantías públicas frente a las decisiones automatizadas y el sesgo y discriminación algorítmicas" (PID2022-136439OB-I00); MICINN Retos "Derechos y garantías frente a las decisiones automatizadas... (RTI2018-097172-B-C21); "La regulación de la transformación digital …" grupo de investigación de excelencia Generalitat Valenciana "Algoritmic law" (Prometeo/2021/009, 2021-24); "Transición digital de las Administraciones públicas e inteligencia artificial" (TED2021-132191B-I00) y "Algorithmic Decisions and the Law: Opening the Black Box" (TED2021-131472A-I00), del Plan de Recuperación, Transformación y Resiliencia. Estancia Generalitat Valenciana CIAEST/2022/1. Una versión simplificada de este estudio en formato ensayo, Cotino (2022 a).

* Catedrático de Derecho Constitucional, Universidad de Valencia, OdiseIA, Valgrai.

I. ALGUNOS EJEMPLOS MÁS SIGNIFICATIVOS PARA INTRODUCIR AL TEMA

Son ya bastantes los casos de uso de sistemas biométricos de identificación en el mundo democrático que se conocen[2]. En Reino Unido, desde 2017 la Policía de Gales del Sur llevó a cabo un proyecto "AFR *Locate*" para eventos como la final de la *Champions League*, partidos internacionales de rugby, conciertos, un día de Navidad en una concurrida calle comercial de Cardiff, etc. Se captaban las imágenes, se procesaban automatizadamente y se contrastaban con personas en listas de vigilancia. Su uso era anunciado con carteles y avisado en redes sociales. En 2019 los tribunales lo dieron por bueno[3], aunque la autoridad británica de datos y transparencia, el ICO, en 2021 ha señalado su uso inapropiado[4].

En Alemania, en Hamburgo con motivo de una reunión del G20 en 2017 se implantó un sistema de reconocimiento facial a partir de grabaciones para la detección e investigación de delitos. La autoridad de datos de Hamburgo lo consideró inadmisible[5], pero un tribunal anuló la suspensión[6] y está pendiente de los tribunales[7]. En Berlín en 2019, se probó el reconocimiento facial policial para detectar comportamientos sospechosos en la estación de tren de Südkreuz[8]. Asimismo, al menos 19 ciudades alemanas han recibido cámaras preparadas para la biometría capaces de reconocer el rostro en directo en un

2 EDRI, 2020; Pérez, 2021; Parlamento UE, 2021 a y b, entre otros.

3 Sobre el tema Davies, Innes y Dawson, 2019; Carrasco, 2020; FRA, 2000; Parlamento UE, 2021: 41; Pérez, 2021: 80 y ss. Así, la High Court of Justice (Divisional Court of Cardiff), Sala de lo Civil, Sección de apelación 4 de septiembre de 2019, EWCH 2341 (Admin), https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf

4 Así, en junio de 2021 de *Information's Comissioner Office* de Reino Unido expresa preocupación por el uso inapropiado.

5 Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, https://datenschutz-hamburg.de/assets/pdf/Anordnung_HmbBfDI_2018-12-18.pdf

6 Un tribunal de primera instancia anuló la orden, https://datenschutz-hamburg.de/assets/pdf/VG_Hamburg_17-k-203-19.pdf

7 Los documentos del procedimiento en https://datenschutz-hamburg.de/pages/anordnung_verf/

8 https://policyreview.info/articles/analysis/imminent-dystopia-media-coverage-algorithmic-surveillance-berlin-sudkreuz Puede seguirse Eireiner, 2020.

proyecto de "Mercado de la ciudad segura". En 2021 un Tribunal detuvo su funcionamiento en Colonia[9]. Una vez remitido este estudio, la sentencia de 16 de febrero de 2023 (1 BvR 1547/19, 1 BvR 2634/20) del TC alemán ha declarado inconstitucional la regulación en dos Länder de sistemas automatizados –no de IA– en el ámbito policial. Lo analizo con cierta profundidad en Cotino (2023a).

En Países Bajos, varios municipios utilizan reconocimiento facial durante los carnavales y otros grandes eventos. Desde 2016, la policía holandesa utiliza el sistema de reconocimiento facial CATCH a través de las imágenes de los teléfonos inteligentes, las cámaras corporales y la nube (EDRI, 2020). La autoridad de datos neerlandesa en 2019 ha criticado el insuficiente marco legal biométrico (DPA, 2019).

En Italia, desde 2019 se utiliza un *Sistema Automatico di Riconoscimento Immagini* (SARI), considerado inadmisible el 16 de abril de 2021 por la autoridad italiana de protección de datos[10].

En Suecia en 2021 la autoridad de datos sancionó que unos policías decidieran por su cuenta utilizar para fines policiales y de investigación un *software* de reconocimiento facial con imágenes de redes sociales y páginas web[11].

En Buenos Aires se empezó a implementar en 2019 un sistema con 300 cámaras activas que permitía la identificación de prófugos y generó unos 10 millones de consultas sobre personas no prófugas. Guillermo Federico Ibarrola fue erróneamente identificado como prófugo y estuvo detenido 6 días.

---

9 En una decisión del 18 de enero de 2021, el Tribunal Administrativo de Colonia emitió una orden judicial contra la Policía de Colonia para detener la videovigilancia de lugares principales de la ciudad, EDRI, 2020.

10 Ver https://www.poliziadistato.it/articolo/15557c52775a3724103220539 y https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877.

11 Así, la Autoridad sueca para la protección de la privacidad 10 de febrero de 2021, DI-2020-2719. https://gdprhub.eu/index.php?title=IMY_-_DI-2020-2719.

El 12 de abril de 2022 el sistema fue suspendido por un juez[12] y finalmente ha sido anulado por sentencia de 7 de septiembre de 2022[13].

En Brasil, el Metro de São Paulo implantó un sistema de control de seguridad de 4 millones de usuarios diarios, suspendido judicialmente el 22 de marzo de 2022[14].

En el ámbito educativo se vienen utilizando polémicos sistemas biométricos para el control de asistencia de estudiantes que ha generado problemas en España, Francia o Suecia.

En España ha destacado el (mal) uso de sistemas biométricos en el sector privado. Así, el uso de sistemas de reconocimiento facial por servicios de seguridad privada no fue admitido por la AEPD en 2019[15]. En 2020 la AEPD rechazó el uso del reconocimiento facial para evitar el fraude en exámenes por universidades *online* (*e-proctoring*)[16]. Y Mercadona fue fuertemente sancionada en 2021 por implantar un sistema inteligente biométrico que controlaba si quienes accedían a algunos establecimientos estaban en sus listas de búsqueda por motivos judiciales previos[17]. No obstante, algún tribunal ha autorizado sistemas biométricos en

12 Acceso en https://srfp.odia.legal/cautelar.pdf

13 Se estimó el amparo y anuló por inconstitucional todo lo actuado por el Ministerio de Justicia y Seguridad de la ciudad sistema en una amplia resolución https://www.cels.org.ar/web/wp-content/uploads/2022/09/reconocimientofacialsentencia070922.pdf

14 https://www.accessnow.org/cms/assets/uploads/2022/04/Ac%CC%A7a%CC%83o-Civil-Pu%CC%81blica-Companhia-do-Metropolitano-de-Sa%CC%83o-Paulo-.pdf

15 Informe 010308/2019 AEPD sobre la licitud de incorporar sistemas de reconocimiento facial en los servicios de videovigilancia proporcionados por empresas seguridad privada, https://www.aepd.es/es/documento/2019-0031.pdf

16 Informe 0036/2020 AEPD sobre reconocimiento facial en los exámenes. pág. 16. https://www.aepd.es/es/documento/2020-0036.pdf
Véase también la resolución de advertencia n.º: E/05454/2021 de la AEPD dirigida a la Universidad Internacional de La Rioja (UNIR).

17 AEPD, Resolución procedimiento sancionador PS 120/2022, https://www.aepd.es/es/documento/ps-00120-2021.pdf

tiendas[18]. También en el ámbito privado, el 12 de agosto de 2019 un Tribunal de Ámsterdam no permitió utilizar escáneres de huellas dactilares en las cajas registradoras de una cadena de zapaterías en aquella ciudad[19].

Más allá del uso de sistemas biométricos para la identificación, los sistemas inteligentes biométricos permiten el reconocimiento de emociones, categorizar a las personas, detectar comportamientos, pensamientos o valorar la personalidad. El uso de estos sistemas biométricos con IA en fronteras no es nuevo. Desde hace más de 10 años hay precedentes en Arizona. Más recientemente, en EEUU el Agente Virtual Automatizado para la Evaluación de la Verdad en Tiempo Real (AVATAR) analiza el comportamiento no verbal y verbal de los viajeros y al parecer, el sistema también se ha probado en el aeropuerto de Bucarest. La Comisión Europea financió el proyecto *Intelligent Portable Control System* (*iBorderCtrl*)[20], con herramientas de detección del engaño y de evaluación basada en el riesgo que ha generado una relativa reacción desde la sociedad civil, una iniciativa ciudadana europea y la campaña *reclaimyourface.eu*.

El 7 mayo 2021 el Tribunal de Justicia de São Paulo prohibió a la concesionaria del Metro de Sao Paulo que utilizara el "Sistema Digital Interactivo de Puertas" (DID) con reconocimiento facial, el sistema infería emociones, género y edad de las personas para personalizar la publicidad[21].

Grandes empresas y plataformas disponen de sistemas de reconocimiento biométrico y facial no sólo para identificar personas sino para detectar emociones, estados de ánimo, etc. En junio de 2022, Microsoft ha anunciado que retira sus sistemas *Azure Face*[22], previamente había dejado de vender este tipo

18 Sentencia del Juzgado de lo Penal número 2 de San Sebastián en 2019. https://www.lavanguardia.com/vida/20190614/462862950020/permiten-a-una-tienda-sistema-de-reconocimiento-facial-para-evitar-2-ladronas.html

19 Tribunal de Primera instancia de Ámsterdam, 7728204 CV VERZ 19-9686. Ver https://gdprhub.eu/index.php?title=Rb._Amsterdam_-_7728204_CV_VERZ_19-9686

20 Sobre el uso en fronteras, entre otros Begault (2019), Sánchez-Monedero y Dencik (2020).

21 https://www.accessnow.org/sao-paulo-court-bans-facial-recognition-cameras-in-metro/

22 https://azure.microsoft.com/es-es/products/cognitive-services/face/

de tecnología a la policía de EEUU. Meta-Facebook dispone desde 2017 de patentes de reconocimiento de emociones[23]. En noviembre de 2021 eliminó el polémico uso del reconocimiento facial[24].

Y esto es lo que más o menos se sabe en el mundo democrático. Si bien, los sistemas más vinculados a la defensa, inteligencia y seguridad nacional que posiblemente sean los más impactantes, nos resultan desconocidos. Y mejor ahora no entrar en el detalle del uso de sistemas inteligentes biométricos y de reconocimiento facial en China[25] para el sistema de crédito social[26], control policial, de la lealtad al partido[27] o en el ámbito educativo[28]. La realidad supera la ficción.

II. DE QUÉ TECNOLOGÍAS Y DATOS BIOMÉTRICOS Y RECONOCIMIENTO FACIAL HABLAMOS

II.1. Tecnologías, datos biométricos y datos basados en la biometría

El reconocimiento facial automático o automatizado hay que incluirlo dentro de toda una serie de "técnicas biométricas" ("identificación biométrica", "categorización biométrica", "detección de comportamientos", "reconocimiento de emociones", tratamiento de "datos biométricos", "elaboración de perfiles biométricos", etc.; Parlamento UE, 2021 b: 23).

Se vienen definiendo como sistemas de identificación biométrica a los procesos automatizados utilizados para reconocer a un individuo a partir de medir, almacenar y comparar sus datos biométricos relativos a sus características

23 https://www.cbinsights.com/research/facebook-emotion-patents-analysis/

24 https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/

25 https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/?itid=lk_inline_manual_10

26 https://nhglobalpartners.com/china-social-credit-system-explained/

27 https://www.telegraph.co.uk/world-news/2022/07/04/china-uses-mind-reading-ai-test-loyalty-communist-party-members/

28 https://globalvoices.org/2022/08/05/china-surveillance-tech-is-extending-from-the-classroom-to-kids-summer-holidays/

físicas, fisiológicas o de comportamiento[29]. Estas características biométricas son universales –las tienen todos los humanos–, singulares y únicas e invariables a lo largo de la vida.

Los datos biométricos cuentan con la misma definición en la Directiva (UE) 2016/680[30] (art. 3.13), el artículo 4. 14 RGPD[31] y, en principio, la misma en el futuro Reglamento IA, en adelante AIA[32] (art. 3.33º). Se trata de "aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".

Hablamos así de identificadores a partir de características físicas, fisiológicas o de comportamiento. Se llega a distinguir entre identificadores "fuertes" especialmente utilizados con las tecnologías de primera generación especialmente destinadas a la identificación (huellas dactilares, ADN, estructura del iris, rostros, voz) e identificadores "débiles" que cada vez cobran más protagonismo (formas de andar, patrones de vasos sanguíneos, pulsaciones de teclas etc.). Con la nueva generación de tecnologías se va más allá de la finalidad de identificación y se habla de "biometría del comportamiento" para el perfilado, reconocimiento de emociones o categorización de personas. Es por ello que, frente a los datos biométricos ligados únicamente a la identificación, se propone el concepto más amplio inclusivo de "datos basados en la biometría"[33].

---

29 Entre otros, una recopilación de conceptos afines, en Gallego, 2022: 234 y ss.

30 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de estos datos. En adelante, Directiva (UE) 2016/680.

31 Reglamento (UE) 2016/679 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.

32 Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas sobre la inteligencia artificial (Ley de Inteligencia Artificial). Una visión general en Cotino, 2021.

33 (Parlamento UE, 2021 a: 23). Se propone para el AIA el concepto (33 bis) "datos basados en la biometría": los datos personales resultantes del tratamiento técnico específico de señales o características físicas, fisiológicas o de comportamiento de una persona física, como las expresiones

La cuestión es importante porque sólo los datos biométricos para la identificación son datos especialmente protegidos bajo el régimen especial del artículo 9 RGPD o art. 10 Directiva (UE) 2016/680. El CEPD (2022: nº 14, 7) sigue siendo claro en el sentido de que, si no se vinculan a la identificación, no son datos sensibles. Llama poderosamente la atención que no estén entre las categorías especiales de datos los que revelan nuestras emociones, los pensamientos y las intenciones[34]. También procede manejar el concepto de "inferencias biométricas" relativas a las conclusiones o resultados de los tratamientos permanentes o a largo plazo de estos datos basados en la biometría.

II.2. El salto cualitativo que supone tratamiento de datos biométricos y reconocimiento facial con tecnologías como la inteligencia artificial

Los datos biométricos se someten a un "tratamiento técnico específico" (art. 4.14 RGPD). En ocasiones se suele hacer referencia a tratamiento "automático" o "automatizado". El simple tratamiento de vídeos y fotografías sin sistemas automatizados para extraer datos biométricos, sin cotejo con una base de datos adicional quedaría fuera del ámbito de interés de este estudio (al respecto ver el Dictamen 3/2012 G29). Ello sin perjuicio de que la "simple" videovigilancia pública o privada sea importante y presente no pocos problemas (por todos, Gutiérrez, 2020; Parlamento UE, 2021: 7). Lo que aquí más interesa es la utilización de componentes de inteligencia artificial o aprendizaje automático, que cada vez es lo más frecuente y que supone un salto cualitativo. Estos sistemas de identificación biométrica automatizados son proclives a la vigilancia masiva o exhaustiva, son difíciles de restringir, los datos que manejan son sensibles, las inferencias y conclusiones que pueden resultar de los mismos pueden tener un enorme impacto, la duración del tratamiento puede ser muy amplia y es bien posible que sean utilizados para finalidades no conocidas. Pues bien, baste ya apuntar que la regulación hoy día existente para tratamientos "simples" de videovigilancia en modo alguno

faciales, los movimientos, la frecuencia del pulso, la voz, las pulsaciones o la forma de andar, que pueden permitir o no la identificación única de una persona física.

34 Sobre la expansión o insuficiencia de la categoría de datos especialmente protegidos, como en el caso de salud, Cotino, 2020.

sirve para habilitar legalmente a los tratamientos con sistemas biométricos con IA y reconocimiento facial (Informe 31/2019 AEPD)[35].

Dentro del genérico de los datos biométricos sin duda que se da una especial atracción por las técnicas de reconocimiento facial basadas en sistemas de IA. Como recuerda el CEPD (2022: nº 15) el "reconocimiento facial" es una funcionalidad de *software* que puede implementarse dentro de los sistemas existentes y que puede conectarse o interconectarse con una multitud de sistemas, y combinarse con otras funcionalidades. Y apunta Simó que lo que suele concentrar la atención es el sistema de reconocimiento facial automático que implica el tratamiento de datos personales especialmente protegidos de las personas que se incluyen en la lista de observación (por ejemplo, personas buscadas por la Justicia), pero también de las personas cuyas imágenes son capturadas y procesadas por el equipo para la extracción de la plantilla biométrica (ciudadanos, etc.) y la comparación con la lista de vigilancia, aunque esos datos no sean archivados y sean inmediatamente eliminados si el resultado de la comparación no es positivo.

Las técnicas de reconocimiento facial basadas en sistemas de IA en buena medida son el estandarte de esta tecnología y de los peligros que presenta y respecto de las que mayores reticencias se han visibilizado. De hecho, las líneas rojas y riesgos inaceptables se plantean en ocasiones con relación al reconocimiento facial (CEPD-SEPD, 2021). Pese al especial interés del reconocimiento facial, el régimen jurídico aplicable es el más general de los sistemas biométricos, no sólo de patrones del rostro.

II.3. La especial protección sólo se aplica a los sistemas de identificación biométrica y no a los tanto o más peligrosos de categorización, reconocimiento de emociones y evaluación de la personalidad

Hasta ahora el elemento esencial definitorio de los sistemas biométricos –y de reconocimiento facial– pasa por su finalidad de identificación de personas. Hay que distinguir en lo posible entre la identificación biométrica (*uno a varios*)

35 "los tratamientos de videovigilancia regulados en la LOPDGDD y en la LSP, se refieren exclusivamente a los tratamientos dirigidos a captar y grabar imágenes y sonidos, pero no incluyen los tratamientos de reconocimiento facial, que es un tratamiento radicalmente distinto al incorporar un dato biométrico".

y la autenticación o verificación biométrica (*uno a uno*). Así lo han hecho las autoridades de protección de datos desde antiguo. Según lo han definido el Grupo del Artículo 29 o la AEPD[36], la identificación biométrica es el proceso de comparar los datos biométricos de un individuo, adquiridos en el momento de la identificación, con una serie de plantillas biométricas almacenadas en una base de datos de personas generalmente identificadas, esto es, un proceso de búsqueda de correspondencias uno-a-varios.

Por el contrario, tradicionalmente no se ha considerado como tratamiento de datos sensibles bajo el especial régimen del artículo 9 RGPD la "verificación" o "autenticación" biométrica "uno a uno", esto es, el proceso de confirmar que un individuo es quien dice ser en el que se comparan los datos únicamente con la identidad que se quiere contrastar (por ejemplo, la identificación con el teléfono móvil personal a través de la huella o el rostro que tiene registrado).

En estas verificaciones uno a uno, como señala la AEPD, "si bien también realiza un tratamiento de datos personales, no llega a procesar la información contra una base de datos previa que permita o confirme la identificación de personas de uno a varios" (Procedimiento sancionador PS/00120/2021: 28).

Así las cosas, el artículo 9. 1º RGPD incluye entre los especialmente protegidos los "datos biométricos dirigidos a identificar de manera unívoca a una persona física". Y se ha venido interpretando como que el uso de datos biométricos sólo quedaba bajo el régimen de datos especialmente protegidos en las identificaciones uno a varios y no las identificaciones uno a uno.

Ahora bien, en mayo 2022 el CEPD (2022, nº 11-12, 7) parece haber variado su tradicional posición. Después de distinguir autentificación-verificación de la identificación, afirma que ambos casos "constituyen un tratamiento de datos personales, y más concretamente un tratamiento de categorías especiales de datos personales." Como señalaba Santiesteban (2021: 511), la distinción "no se sostiene". No obstante, ciertamente es un cambio bastante drástico que

36 Así, el Grupo del Artículo 29 desde el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas o la AEPD en sus diversas guías. En todo caso, especialmente hay que seguir la diferencia en FRA, 2020, en especial apartado 7º, 23-32. Y en particular Parlamento, 2021: 20 y ss.

habrá que digerir y proyectar, además de la necesidad de su posible ratificación judicial o en su caso, regulatoria.

Como se ha adelantado, el uso de datos basados en la tecnología de reconocimiento facial y otras tecnologías biométricas no se detiene en la identificación. Estas tecnologías y datos pueden utilizarse para inferir emociones, detectar o predecir comportamientos, orientaciones, si se dice o no la verdad, etc.

El futuro AIA define un "sistema de reconocimiento de emociones" como "un sistema de IA destinado a identificar o inferir emociones o intenciones de personas físicas a partir de sus datos biométricos" (art. 3.33º). Se ha apuntado que en la definición deben incluirse los "pensamientos", dado que ello parece posible a través de las *interfaces* cerebro-ordenador.

Y según se ha dicho, el tratamiento de estos datos que no sea para la identificación no cuenta con el régimen de los datos especialmente protegidos. Como señala el Parlamento UE (2021) "no parece normal que queden bajo el régimen general las emociones, los pensamientos y las intenciones". Sin embargo, en mayo de 2022 sigue siendo contundente (CEPD, 2022: Nº 14, 7): aunque se traten datos biométricos, si no son para la identificación, quedan fuera del ámbito de los datos especialmente protegidos[37]. El FRA (2020) ya señaló la especial sensibilidad de estos sistemas. El CEPD y el SEPD quieren en general prohibirlos, se considera que su uso "es muy indeseable y debe prohibirse, excepto en determinados casos de uso bien especificados, a saber, con fines sanitarios o de investigación (por ejemplo, pacientes donde el reconocimiento de emociones es importante), siempre con las garantías adecuadas y, por supuesto, sujeto a todas las demás condiciones y límites de protección de datos, incluida la limitación de la finalidad" (CEPD-SEPD, 2020, nº 35). Sin embargo, en el futuro AIA puede considerarse que en general no sólo no están prohibidos, sino que en principio sólo son de alto riesgo salvo en algunos supuestos particulares, como los casos del uso de estos sistemas para

37 Se afirma que las "técnicas digitales de detección de comportamientos anómalos o de sucesos violentos, o de reconocimiento de emociones faciales o incluso de siluetas, no pueden considerarse sistemas biométricos que traten categorías especiales de datos personales, siempre que no tengan por objeto la identificación exclusiva de una persona y que el tratamiento de datos personales de que se trate no incluya otras categorías especiales de datos personales." (traducción propia).

evaluaciones de riesgo determinado o predicción de comportamientos futuros independientes de la propia voluntad (Anexo III).

También resulta especialmente sensible un "sistema de categorización biométrica" que el futuro AIA define (art. 3. 35º) como "un sistema de IA destinado a asignar a las personas físicas a categorías específicas, como sexo, edad, color de pelo, color de ojos, tatuajes, salud, rasgos personales, origen étnico u orientación sexual o política, sobre la base de sus datos biométricos". Se ha propuesto añadir categorías como la capacidad mental y rasgos de comportamiento (Parlamento UE, 2021).

La categorización clasifica a las personas a partir de la biometría (reconocimiento facial) en grupos según su etnia, género y orientación política o sexual. Su impacto también puede ser enorme. También se ha pedido que se prohíban totalmente las aplicaciones que permiten la "categorización biométrica" (EDRI, 2021).

Desde el Parlamento UE (2021: 81-82), se propone una regulación específica que califique el uso de los sistemas de reconocimiento de emociones y de categorización biométrica como prácticas restringidas de IA y los someta a un enfoque normativo muy similar al de la identificación biométrica remota en tiempo real.

III. LOS MUCHOS PRINCIPIOS Y DERECHOS EN JUEGO Y LAS VARIABLES DE LOS SISTEMAS BIOMÉTRICOS PARA SU PONDERACIÓN

III.1. Los muchos principios y derechos en juego

El variado uso de las tecnologías biométricas y en particular el reconocimiento facial tiene el potencial de impactar prácticamente en todos los derechos fundamentales de las personas.

Entre otros, en un amplio análisis el FRA menciona los siguientes derechos: "la dignidad humana, al respeto de la vida privada, la protección datos personales, la no discriminación, los derechos del niño y de los mayores, los derechos de las personas con discapacidad, la libertad de reunión y asociación, la libertad de expresión, el derecho a una buena administración, y el

derecho a un recurso efectivo ante la ley y a un juicio justo" (FRA, 2020: 4, en especial, FRA, 2018: 81-98, también Consejo de Europa, 2021). Y no hay que olvidar impactos específicos en libertad religiosa y los derechos del niño, mayores, salud, discapacitados, etc.

Como he tenido ocasión de exponer con detenimiento (Cotino, 2022 b), no sólo hay que apreciar el impacto concreto de estos sistemas en los derechos fundamentales como derechos subjetivos de personas determinadas. El uso de sistemas biométricos impacta en el ser humano y en la misma la dignidad y se produce de forma colectiva, no sólo en perspectiva meramente individual, puede quedar afectado el orden político y la paz social (art. 10. 1 CE). Jurídicamente ello puede canalizarse a través de la dignidad de la persona y la dimensión objetiva de los derechos fundamentales. En esta línea, se afirma la afectación de la dignidad dado que la cuantificación o ratificación de la persona y sus rasgos para hacerla legible por máquinas implica una cosificación (CEPD, 2022: nº 40, 13). También, que el potencial control generalizado lleva a que el impacto en las personas puede ser tan importante que afecte a su capacidad de vivir una vida digna. Subraya el CEPD, que el reconocimiento facial implica un "debilitamiento" del anonimato, con "grave efecto amedrentador". El simple hecho de caminar por la calle dará lugar a la recogida de datos por las fuerzas policiales y una comparación con sus bases de datos. Recuerda con razón que "una situación en la que se hiciera lo mismo tomando huellas dactilares sería claramente desproporcionada". Además, "la identificación biométrica [...] trata a todo el mundo como un sospechoso potencial"; la incomodidad de las personas puede llevarlas a cambiar su comportamiento. (2022: nº 40 y en especial, 45).

Asimismo, bajo esta visión supraindividual y colectiva hay que tener muy presente la afectación a principios esenciales como el principio democrático y la seguridad jurídica (CEPD-SEPD, 2020: nº 31). La mera posibilidad de estos sistemas puede inhibirnos de participar o ejercer nuestras libertades, puede llevarnos a cambiar comportamientos y retirarnos de la vida social, cultural o participativa y dificultar el libre albedrío (Parlamento UE, 2021 a: 7). El mismo AIA afirma que estos sistemas pueden "evocar una sensación de vigilancia constante y disuadir indirectamente del ejercicio de la libertad de reunión y otros derechos fundamentales" (considerando nº 18). Así pues, estos sistemas pueden impactar en la libertad de expresión, de reunión, de asociación y de circulación.

Como señala Carrasco (2019: 69) para el caso de Gales, no es razonable que por ir a un partido de fútbol se verifique si sobre el aficionado recae una orden de búsqueda y captura por un delito. Ni siquiera registrando huellas dactilares entre los asistentes al partido la policía conseguiría esta inmediata identificación.

En todo caso, el uso de tecnologías biométricas y el reconocimiento facial impactan especialmente en la vida privada, la protección de datos y el derecho a la no discriminación. Como señala el CEPD (2022: nº 37, 12-13, también CEPD-SEPD, 2020), el tratamiento de datos biométricos en cualquier circunstancia constituye una interferencia grave en sí misma, injerencia incluso si la plantilla biométrica se elimina inmediatamente después de que el cotejo con una base de datos policial dé como resultado un resultado no positivo, aunque el tratamiento de datos sea sólo por unos milisegundos.

Y frente a la presunción de inocencia, los sistemas biométricos nos tratan a todos como sospechosos potenciales. Se imponen con independencia de la conducta individual de la persona o de las circunstancias particulares, siendo que estadísticamente, casi todos los afectados son personas respetuosas de la ley (CEPD, 2022: 46 y ss.). Y a los que el sistema identifica como sospechosos les impone una mayor carga de demostrar su inocencia (Parlamento UE 2021 a): 7).

Obviamente la vida privada queda también afectada cuando se trata de grabaciones sistemáticas o permanentes del espacio público[38]. También, señala el TEDH que la mera conservación y el almacenamiento de datos personales por parte de las autoridades públicas, independientemente de cómo se hayan obtenido, debe considerarse que tiene un impacto directo en el interés de la vida privada de una persona afectada, con independencia de que se haga un uso posterior de los datos[39]. No obstante, en algún supuesto se consideró "pertinente y suficiente" la conservación de las huellas dactilares, perfiles de

38 STEDH de 25 de septiembre de 2001, *asunto* P.C. y J.H. v. *United Kingdom* nº 155. Ver STEHD 4 de diciembre de 2008 S. y Marper contra el Reino Unido.

39 STEHD, 31 de julio de 2012, Van der Velden v. Países Bajos: "la conservación sistemática de ese material va más allá del ámbito de los elementos de identificación neutros, como las huellas dactilares, y es lo suficientemente intrusiva como para constituir una injerencia en el derecho al respeto de la vida privada establecido en el artículo 8 § 1 del Convenio".

ADN de condenados por delitos menores y las imágenes faciales durante 25 años, sin la posibilidad de solicitar la supresión de estos datos[40].

Es más, deben hacerse nuevas interpretaciones de los derechos vinculados a la privacidad. Por ejemplo, el tratamiento masivo de datos incluso desvinculados de personas concretas "*considerados en su conjunto*, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los círculos sociales que frecuentan" (ap. 27)[41]. De igual modo, no puede admitirse la tradicional doctrina del Tribunal Supremo de Estados Unidos por la que la policía "no necesita una sospecha razonable para "observar o investigar personas en público y los datos públicos… para detectar a las personas que cometen crímenes" y se pueden manejar las informaciones captadas a "simple vista" (*naked eye*)[42]. Ahora con los datos que se aprecian en la vía pública se puede identificar personas, además de conocerse nuestras emociones o intenciones, por ejemplo.

El impacto de las tecnologías biométricas y el reconocimiento facial en el derecho a la no discriminación puede ser muy habitual (especialmente FRA, 2019; Parlamento UE 2021 a): 14 y ss., 163 y ss., ap. 3.3.2 y en general Consejo de Europa, 2019)[43]. Normalmente se tratará de discriminaciones indirectas, no voluntarias, producidas por manejar datos de entrenamiento no representativos, de sesgos en los esquemas de etiquetado de datos y de funciones matemáticas

40 STEHD 13 de febrero de 2020, Gaughran v. Reino Unido, nº 97.

41 STJUE (Gran Sala) de 8 de abril de 2014, Digital Rights Asuntos C-293/12 y C-594/12. También, STJUE (Gran Sala), de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB y Secretary of State for the Home Department y otros, ap. 99.

42 The police are "not restricted by being required to have a reasonable suspicion to observe or investigate persons in public and public data . . . to detect those [persons] who commit crime." (*United States v. Steinhorn*, 739 F. Supp. 268, 1265, 1272, D. Md. 1990). Asimismo, se pueden hacer seguimientos de individuos en áreas de alta criminalidad. Igualmente, los policías no tienen que cerrar los ojos cuando pasan por delante de una casa, de modo que se admiten las informaciones captadas a "simple vista" naked eye (*Kyllo v. United States*, 533 U.S. 4, 27, 2001). Cabe seguir a Joh (2014).

43 Sobre la discriminación algorítmica cabe remitir a los diferentes estudios de Soriano (2021, 2022), así como Cotino (2023).

defectuosas o inadecuadas. Serán habituales resultados algorítmicos aparentemente neutros pero [de hecho] discriminatorios [...]". En 2020 el Comité de Supervisión y Reforma del Congreso de los Estados Unidos afirmó que se identifica erróneamente a las mujeres y las minorías y a una tasa mucho más alta que a los hombres blancos, lo que aumenta el riesgo de sesgo racial y de género"[44].

III.2. Las muchas variables relevantes para la regulación y la ponderación jurídica de los sistemas inteligente biométricos

El uso de estas técnicas puede ir desde el escaso impacto de una verificación personal con datos del rostro o huella digital para el acceso al celular personal, voluntario y bajo el control del interesado, hasta el reconocimiento de un ciudadano normal en la vía pública o en una manifestación para analizar si está en alguna base de datos específica, georreferenciarlo y mantener los datos para, por ejemplo, reconstruir sus recorridos, interacciones con otras personas y evaluar su comportamiento.

La variedad de finalidades de los usos y circunstancias puede ser casi infinita[45] y son un elemento esencial en su regulación, así como para ponderar jurídicamente el impacto. Quizá lo peor –y de ahí el gran potencial peligro– es que se destine el sistema y los datos para finalidades diferentes a las inicialmente concebidas o declaradas. De ahí también el peligro ínsito o inherente de la mera existencia de estos sistemas.

A la hora de valorar el impacto de estos sistemas debe recordarse que en los habituales supuestos de control en espacios de acceso público, los afectados o interesados son no sólo las personas "buscadas" o que se quiere monitorear o evaluar (criminales, huidos de la justicia, sospechosos, etc.), sino también todas las personas analizadas[46]. Como recuerda el Grupo de Expertos de

44 Carrasco, 2020: 64, ver también http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

45 Resulta de especial interés apreciar las variables sistemáticamente expuesta en el Anexo I Parlamento UE, 2021 a).

46 El SEPD-CEPD lo critica especialmente en su análisis del AIA "parece omitir que al monitorear áreas abiertas, las obligaciones bajo la ley de protección de datos de la UE deben cumplirse no solo para los sospechosos, sino para todos aquellos que en la práctica son monitoreados." (nº 31).

Alto Nivel en IA hay que diferenciar entre la identificación, o el rastreo y seguimiento de una persona, así como entre la vigilancia selectiva y la vigilancia masiva (HLEG, 2019: nº 33). Aunque los procesamientos de los datos sean de décimas de segundos, se tratan masas de datos enormes, incluyendo entre otros, menores, discapacitados u otros colectivos sensibles, así como los trabajadores de los lugares monitoreados. Ello fue importante en el mencionado Caso Mercadona en España (AEPD, PS 120/2022).

Un elemento esencial es la escala del tratamiento efectuado. En este sentido la falta de delimitación de las personas o colectivos sobre los que se aplica, que se realiza con independencia de la conducta o circunstancias de la persona si el tratamiento de datos abarca una parte significativa de la población respecto de quienes no hay pruebas ni indicios de ilegalidad que se persigue y este elemento dificulta sin duda la justificación de la injerencia[47].

Los habituales usos vinculados con la prevención, detección o persecución penal pueden afectar especialmente los derechos y garantías el ámbito penal y sancionador. En este contexto es también fundamental la naturaleza y gravedad de los delitos que justifican el procesamiento[48].

El uso de los sistemas biométricos con finalidades laborales también puede ser muy variado: utilización para verificar la asistencia y cumplimiento de jornada, para evaluar, controlar y asignar tareas, para decidir la contratación, despidos, sanciones, etc. Muchos de estos usos se consideran de alto riesgo en el futuro AIA. En los contextos laborales también pueden quedar especialmente atraídas y afectadas las libertades sindicales, de huelga o de negociación colectiva.

El uso de estas tecnologías en el ámbito educativo y universitario es ya habitual para el control de asistencia, para evitar el fraude en exámenes o para la admisión, atención, así como la evaluación educativa. En muchos casos se considerará de alto riesgo para el AIA y los derechos y libertades de la comunidad educativa pueden quedar especialmente afectados.

47 STJUE (Gran Sala) de 8 de abril de 2014, Digital Rights Asuntos C-293/12 y C-594/12, párr. 58.

48 *Ibidem*, párr. 60-61.

Otro elemento de gran relevancia para determinar el impacto del uso de sistemas biométricos reside en el lugar donde se produzca[49].

Especialmente son sensibles la vía pública, así como el "espacio de acceso público" (Artículo 3. 1º 39º. AIA): "cualquier lugar físico que sea accesible a un número indeterminado de personas físicas, el público, e independientemente de que el lugar en cuestión sea de propiedad privada o pública. e independientemente de la actividad para la que se utilice el lugar, como el comercio (por ejemplo, tiendas, restaurantes, cafés), los servicios (por ejemplo, bancos, actividades profesionales, hostelería), el deporte (por ejemplo, piscinas, gimnasios, estadios), el transporte (por ejemplo, estaciones de autobús, metro y ferrocarril, aeropuertos, medios de transporte), el entretenimiento (por ejemplo, cines, teatros, museos, salas de conciertos y conferencias) el ocio u otros (por ejemplo, vías y plazas públicas, parques, bosques, zonas de juego)"[50].

También hay lugares más sensibles respecto de algunos derechos: espacios de afluencia habitual religiosa, espacios educativos y de profesorado, espacios de concurrencia de menores y discapacitados, espacios especialmente destinados a la actividad sindical, centros sanitarios, de mayores, de ayuda social, de periodistas y abogados, etc. (CEPD, 2022: 47). Y, en cualquier caso, cualquier rastreo en el espacio público puede afectar a sujetos especialmente caracterizados (*ídem*).

La naturaleza y procedencia de los datos biométricos puede también ser determinante: datos biométricos recogidos legítimamente para finalidades que sean o no incompatibles, datos procedentes de redes sociales, de bancos de datos de propósito general o particulares, de entidades privadas o públicas, etc.

Un factor determinante para el futuro AIA es que el tratamiento se realice o no en tiempo real, como luego se expone. La duración del tratamiento y el mantenimiento de datos es un elemento también muy relevante. Es relevante

49 *Ibidem*, párr. 68.

50 AIA versión 2022, versión República Checha, Considerando 9.

el tiempo de conservación, que sólo sea el necesario y los criterios claros y objetivos para su determinación[51]. También es muy importante para ponderar la restricción el posible tratamiento posterior de los datos extraídos –así como los inferidos–, así como si se da una conservación más o menos general e indiscriminada[52]. En los supuestos habituales de identificación uno a varios, en ocasiones se aduce que el tratamiento de datos de la persona es sólo por unos milisegundos, esto es, el tiempo en hacer el patrón de su rostro y compararlo con los de las personas buscadas. En el caso de no haber coincidencia el dato se elimina. De este modo la afectación sería inapreciable. El CEPD-SEPD (2020, nº 32) descartan la identificación remota a gran escala, aunque el tratamiento de datos tenga poca duración o no haya almacenamiento de los datos de "todos" (también CEPD, 2022: nº 37, 12-13). Sin embargo, para Carrasco (2020: 22) no se aprecia una clara posición cuando afirma que por sí misma la implantación de estos despliegues no presenta un problema claro o sistemático de déficit de proporcionalidad.

La realización del tratamiento por sujetos públicos o privados puede ser relevante por diversos factores: la diversa exigencia del principio de legalidad, la importancia que pueda tener el consentimiento de los afectados, la ajenidad de las finalidades de seguridad de las entidades privadas. De igual modo, la peligrosidad del tratamiento es variable según las capacidades tecnológicas y acceso a datos de quien realice el tratamiento.

Son "fuertes indicios" de la afectación, la menor transparencia y explicabilidad de los tratamientos por las autoridades policiales (CEPD, 2022: 47). En el caso de Gales se tuvo favorablemente en cuenta que el sistema había sido anunciado. Además, puede ser variable y relevante el grado de control de las personas sobre sus datos personales, de los medios efectivos de que disponen para ejercer dicho control, las posibilidades de ejercer garantías y recursos en su caso ante autoridades y especialmente judiciales y de su derecho de iniciativa para activar y utilizar esta tecnología. Otra variable a tener en cuenta es

51 STJUE (Gran Sala) de 8 de abril de 2014, Digital Rights Asuntos C-293/12 y C-594/12, párr. 64.

52 Así, respecto de comunicaciones electrónicas, STJUE C-512/18, (Gran Sala) de 6 de octubre de 2020, párrafo 209 y siguientes.

que se respecten los principios de protección y seguridad de los datos y que se limite efectivamente el acceso a los datos[53].

IV. LOS SISTEMAS DE IDENTIFICACIÓN BIOMÉTRICA EN EL FUTURO REGLAMENTO IA. MÁS QUE PROHIBIDOS, SON SISTEMAS DE ALTO RIESGO

IV.1. La superposición normativa y el futuro AIA

Respecto del uso de tecnologías y datos biométricos hay una importante concurrencia y superposición de regímenes jurídicos. Como punto de partida, hay que tener bien presente el efecto directo de los principios constitucionales y los muy variados derechos fundamentales en juego. No en vano, la regulación legal si la hay, tiene importantes lagunas, así como exclusiones de aplicación para el ámbito de la defensa, inteligencia y seguridad nacional. Obviamente estas exclusiones no impiden la aplicación de la Constitución y los derechos fundamentales, como por ejemplo recuerda la sentencia del TC alemán de 19 de mayo de 2020 (1 BvR 2835/17)[54].

Si descendemos a la legislación aplicable, se hace preciso superponer futura normativa de IA con la(s) normativa(s) de protección de datos, así como diversa normativa sectorial.

Procede iniciar el análisis con el futuro AIA, dado que parte de una teórica prohibición bastante general del uso de sistemas IA de identificación biométrica. Los que no estén totalmente prohibidos en general son de alto riesgo y quedan bajo la intensa regulación del AIA y a esta regulación se sumará la posible aplicación de la normativa de protección de datos y otras normas.

La técnica de la prohibición –al menos teórica– se ha dado en EEUU. A falta de un enfoque federal general, San Francisco, Boston, Portland y Oregón[55],

53 STJUE (Gran Sala) de 8 de abril de 2014, Digital Rights Asuntos C-293/12 y C-594/12, párr. 40.

54 https://www.bundesverfassungsgericht.de/e/rs20200519_1bvr283517.html

55 Sobre la regulación en EEUU, Congressional Research Service, 2020; U.S. Government Accountability Office, 2021; Parlamento UE 2021 b); Pérez, 2021.

han prohibido la tecnología de reconocimiento facial en los espacios públicos. Massachusetts ha implicado a los jueces en algunos supuestos de 2021. California ha hecho una moratoria de 3 años. En Italia en abril de 2021 se ha propuesto la suspensión hasta que exista legislación específica[56].

Hay que llamar la atención que el futuro AIA no se aplica a sistemas para "actividades con fines militares, de defensa o de seguridad nacional, con independencia del tipo de entidad que realice dichas actividades" (art. 2.3º). Hay que entender que esta exclusión no alcanza a la seguridad pública, puesto que de lo contrario dejaría de tener sentido buena parte de la regulación de los sistemas de alto riesgo del AIA que están pensados para este ámbito. Además de los sistemas de IA biométricos, claramente están vinculados a la seguridad pública los sistemas de alto riesgo relativos a la aplicación de la ley.

Teóricamente el AIA supone un sistema de semáforo. Rojo: prohíbe algunos usos de IA (art. 5). Amarillo: fija algunos usos (Anexos II y III) como de "alto riesgo" y éstos deben cumplir numerosas obligaciones que ocupan el grueso del AIA. Verde: no es obligatorio cumplir la regulación del AIA. Como excepción, algunos sistemas IA tienen algunas obligaciones particulares (art. 53).

IV.2. El alcance de la "prohibición" del AIA y los muchos sistemas de identificación que no están prohibidos

Los "sistemas de identificación biométrica" que en principio estarán prohibidos son "en tiempo real", en espacios de acceso público y con fines policiales. En la versión Presidencia Francia y Chequia, también se incluye "en nombre" de autoridades policiales.

El considerando 17 recuerda que la prohibición del uso de sistemas biométricos en tiempo real es "en vivo" o "casi en vivo", sin retraso significativo. En principio, que el sistema no actúe en tiempo real llevaría a sistemas que sólo se utilicen puntualmente (Parlamento UE, 2021 a). Sin embargo, CEPD-SEPD

56 Proyecto de Ley C. 3009 Presentado el 12 de abril de 2021 que propone la moratoria del reconocimiento facial en espacios públicos https://www.camera.it/leg18/126?tab=1&leg=18&idDocumento=3009&sede&tipo

(2021: nº 31) no dan tanta importancia a que el sistema opere en tiempo real, "teniendo en cuenta que un sistema de identificación masiva es capaz de identificar miles de personas en sólo unas pocas horas. Además, la intrusividad del procesamiento no siempre depende de que la identificación se realice en tiempo real o no". Y el efecto inhibidor de los controles es el mismo aunque sea a posteriori. Para Parlamento UE (2021 a) esto "no es convincente", aunque las garantías de protección de datos en estos casos pueden ser suficientes. Cabe apuntar también que la referencia inicial "a distancia" ha desaparecido en la versión francesa.

La reacción de autoridades garantes y de sociedad civil ya ha llevado a ir restringiendo algunas excepciones que inicialmente se podían dar en las versiones del Consejo de la UE de Francia y Chequia, y ello a la espera de los miles de enmiendas al AIA. Ello ha sucedido especialmente respecto de la prohibición de uso en "espacios de acceso público". En la versión checa en principio sí que quedaría prohibido el uso de sistemas biométricos a los muchos lugares a los que pueda acceder un número indeterminado de personas (Considerando 9). En cualquier caso, la prohibición no alcanzaría a locales de empresas y fábricas, como oficinas y lugares de trabajo, las prisiones, zonas de control fronterizo y espacios en línea tampoco están prohibidos (Considerando 9).

La prohibición de los sistemas de identificación biométrica se limita a los que tengan fines policiales. En la versión Presidencia Francia y Chequia, también se incluye "en nombre" de autoridades policiales. Asimismo, los usos de estos sistemas en el ámbito de "migración o de asilo" parecen admitirse (art. 5.4 AIA, versión Presidencia checa 2022).

Además, cabe entender que no están prohibidos por el artículo 5 los usos no policiales. De ahí que el AIA no prohibiría el uso de sistemas biométricos por agentes privados en accesos a lugares de acceso público como supermercados, transporte, estadios, escuelas, etc. Ahora bien, como sucede en el caso Mercadona, no es el futuro AIA quien prohíbe el uso por sujetos privados, sino la normativa de protección de datos y la falta de regulación habilitante expresa.

En la versión francesa del Anexo III. 1º apareció que no serían de alto riesgo los sistemas biométricos o reconocimientos faciales para los que el afectado ha

dado su consentimiento. Como luego se expone, se debe entender como un error que no tiene continuidad y que ya no se aprecia en la versión posterior checa.

IV.3. Los requisitos para admitir los sistemas teóricamente prohibidos: un "no es no" que es un "sí se puede"

Lo cierto es que no hay ni prohibición ni un semáforo rojo real respecto de los sistemas de identificación biométricos. Los teóricamente prohibidos por el artículo 5 se entienden como excepciones que pueden darse si se cumplen particulares presupuestos y garantías.

Como punto de partida, para el uso de estos sistemas *prohibidos* se requiere autorización previa obligatoria y motivada por autoridad judicial o administrativa independiente. A este respecto, el AIA remite a cada Estado sus "normas detalladas necesarias para la solicitud, la expedición y el ejercicio de las autorizaciones". La autorización previa sólo puede eludirse en situaciones de urgencia debidamente justificadas.

Los requisitos y presupuestos para esta autorización previa vienen predeterminados por el AIA. Como punto de partida general se precisa que el uso del sistema sea "estrictamente necesario". La regulación también establece requisitos a tener en cuenta para la autorización relativos a: la necesidad y proporcionalidad, tener en cuenta el lugar, las consecuencias de no usar el sistema, y el impacto a los derechos de todos los afectados.

Los fines posibles son bien amplios: la búsqueda de víctimas de delitos, la prevención de una amenaza inminente específica para la vida, "la prevención de una amenaza específica, sustancial" "para las infraestructuras críticas, la vida, la salud o la seguridad física de las personas físicas o la prevención de ataque terrorista"; "la localización, o identificación de una persona física con el fin de llevar a cabo una investigación penal, un proceso o la ejecución de una sanción penal" de delitos con pena de más de 3 años (Decisión marco 2002/584/JAI) o 5 años según legislación nacional. En la versión inicial AIA se incluía el "chantaje emocional" del uso para la búsqueda selectiva de posibles víctimas de delitos, incluidos los niños desaparecidos.

Así pues, son muchos los supuestos de sistemas IA de identificación biométrica que o no están prohibidos por el artículo 5 o que sí lo están pueden ser autorizados. Todos estos sistemas IA de identificación biométrica han de considerarse sistemas de alto riesgo en razón del apartado 1 del Anexo III y, como consecuencia les será aplicable el régimen del AIA.

IV.4. Los sistemas de IA biométricos de emociones y categorización biométrica: ni prohibidos, ni de alto riesgo

Más complejo puede resultar el régimen de los sistemas de reconocimiento de emociones y los de categorización o clasificación de los individuos. Los mismos en principio no son sistemas de identificación y por tanto no son IA de alto riesgo. En principio, del AIA sólo se les aplicarán las hoy escasas obligaciones de comunicación ("transparencia", artículo 52 AIA: "deberán informar del funcionamiento del sistema a las personas físicas expuestas al mismo"). Ello ha sido especialmente criticado por EDPB – EDPS (2021), quienes recomiendan que se prohíban (tanto a las autoridades públicas como a las entidades privadas) los sistemas de IA (incluido el reconocimiento facial) que se utilicen para clasificar a las personas en función de su origen étnico o de su sexo, así como de su orientación política o sexual, ya que ello puede dar lugar a una discriminación injusta.

Además, justo respecto de estos sistemas que no son para la identificación, en general no será aplicable el régimen singular de garantías de los datos biométricos como especialmente protegidos. Pues bien, desde Parlamento UE (2021 b) se propone una regulación específica y restrictiva. De un lado, se apuesta por incluirlos expresamente en el punto 1 del Anexo III como sistemas de alto riesgo. Del otro lado, desde el Parlamento UE se apuesta porque expresamente se sumen las garantías de los datos especialmente protegidos del artículo 9 RGPD, pues hoy por hoy no cubren estos supuestos. Así, este uso se "limite a lo estrictamente necesario" siempre que se den requisitos del artículo 9 RGPD (en concreto artículo 9 (2) (a), b), c), g), h), i) y j)), así como "fines policiales, de gestión de la migración, del asilo o del control de las fronteras, en la medida en que los fines sean proporcionados" (Artículo 5b Otros usos de las técnicas biométricas). En cualquier caso, dejando claro que cualquier otra exigencia normativa debe mantenerse.

V. EL RÉGIMEN DE PROTECCIÓN DE DATOS Y OTRAS NORMAS DE CONCURRENTE APLICACIÓN A LOS SISTEMAS BIOMÉTRICOS

Los sistemas de identificación biométrica, más que probablemente, implican tratamientos de datos personales. Por ello, además de quedar sometidos a las exigencias de los sistemas de alto riesgo del AIA, estarán sujetos al régimen de protección de datos. Esta concurrencia de protección de datos y del AIA no es sencilla. Se trata de normas con lógicas bastante diferentes. Baste señalar que la normativa de AIA no va dirigida a establecer directamente garantías para las personas afectadas, sino obligaciones para los proveedores de sistemas de IA y las empresas o entidades que los utilicen. Como se ha afirmado "las restricciones al uso de técnicas biométricas pueden tener su origen tanto en la "perspectiva de los datos" como en la "perspectiva de la IA", y ambos tipos de restricciones pueden tener el mismo efecto o uno similar, aunque se refieran a conceptos y categorías diferentes". (Comisión de Ética de Datos del Gobierno Federal, 2019). Y esta concurrencia normativa se dificulta más si cabe porque el futuro AIA ignora el régimen de protección de datos.

El tratamiento de datos biométricos y otros datos especialmente protegidos estaría sometido al régimen general de protección de datos y con las singulares garantías de los datos especialmente protegidos (art. 9 RGPD) y las de los tratamientos automatizados (art. 22 RGPD). Ahora bien, el habitual uso de sistemas biométricos en el ámbito policial y penal quedará bajo la regulación especial de la Directiva (UE) 2016/680[57] y, por ende, la transposición española de la Ley Orgánica 7/2021, de 26 de mayo[58].

Pues bien, desde la perspectiva de protección de datos el punto de partida es la prohibición del tratamiento de datos, que sólo se puede levantar si se dan los requisitos excepcionales que se regulan. Los artículos 10 y 11 Directiva (UE) 2016/680 son paralelos a los artículos 9 y 22 RGPD, pero algo menos exigentes y rigurosos.

---

57 Al respecto, cabe seguir los considerandos 11 y 12 Directiva (UE) 2016/680 y considerando 19 del GDPR.

58 De protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

El artículo 10 Directiva (UE) 2016/680 requiere que el tratamiento de datos biométricos sea el "estrictamente necesario", que reúna "garantías adecuadas", que esté específicamente "autorizado por el Derecho de la Unión o del Estado miembros" y vinculado a las finalidades de protección de intereses vitales o relativo a datos que el interesado haya hecho manifiestamente públicos. La transposición española en su artículo 13 prácticamente reitera lo anterior, con alguna referencia a que haya más garantías cuando se trate de menores o discapacitados y añade que las autoridades competentes podrán tratar datos biométricos para las finalidades de la Directiva (UE) 2016/680 y la ley (seguridad pública).

El artículo 11 Directiva (UE) 2016/680 exige especiales garantías para las decisiones automatizadas con datos biométricos (art. 11.2º) y, en particular, la intervención humana. El apartado 3 prohíbe la elaboración de perfiles que conduzcan a la discriminación de personas físicas sobre la base de datos sensibles. La transposición española tampoco aporta nada y en el artículo 14 sólo apunta que la ley habilitante ha de establecer las garantías adecuadas y la intervención humana. La Directiva (UE) 2016/680 (y lo emula la ley española de transposición) también exige medidas de seguridad y confidencialidad, así como control del usuario, el control del almacenamiento, el control del acceso y la integridad (ver art. 29 o considerando 60).

Según se ha dicho, en los casos en los que no aplica el régimen especial policial penal de la Directiva (UE) 2016/680, a los sistemas biométricos hay que aplicarles directamente el RGPD y en principio con las especiales garantías de los artículos 9 y 22.

Son muy numerosas las normas de la UE que permiten recoger, almacenar y compartir datos biométricos. Obviamente se trata de normativa aplicable a tener en cuenta en cada caso concreto. No obstante, es difícil considerar que esta normativa valga como la ley específica que por sí sola habilita, legitima y regula de manera suficiente las particulares garantías de los particulares sistemas biométricos automatizados o de IA.

De modo muy sumario cabe señalar el Paquete de Fronteras Inteligentes de la Comisión Europea, siendo su pieza central el Reglamento del Sistema de

Entradas y Salidas[59]. También, el Sistema de Información de Schengen (SIS) es una base de datos europea centralizada con información sobre personas desaparecidas o buscadas conformada por numerosos Reglamentos[60]. El SIS permite la carga de datos biométricos como huellas dactilares, marcas de manos e imágenes faciales. La Decisión Prüm establece una red descentralizada para el intercambio de datos biométricos[61] y el EURODAC fue la primera base de datos biométricos a escala europea. Entre otra normativa fácilmente proyectable a los sistemas biométricos se encuentra la relativa a documentos de viaje[62]. Así, por ejemplo su artículo 4. 2º limita expresamente el uso de identificadores biométricos para verificar la autenticidad del documento y para comprobar la identidad del titular comparando.

Además del régimen de protección de datos que pueda proceder, en muchos supuestos se aplicará también de forma superpuesta la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Desde la perspectiva de consumo, la explotación de las vulnerabilidades de los consumidores puede calificarse

59 Reglamento (UE) 2017/2226 del Parlamento Europeo y del Consejo, de 30 de noviembre de 2017, por el que se establece un Sistema de Entradas y Salidas (SES).

60 Reglamento (UE) 2018/1860 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, sobre la utilización del Sistema de Información de Schengen para el retorno de los nacionales de terceros países en situación irregular, Reglamento (UE) 2018/1861 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de los controles fronterizos, por el que se modifica el Convenio de aplicación del Acuerdo de Schengen y por el que se modifica y deroga el Reglamento (CE) n.º 1987/2006; Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y por el que se derogan el Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión.

61 Decisión (CE) 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza.

62 Reglamento (CE) 2252/2004 del Consejo, de 13 de diciembre de 2004 sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros.

como una práctica comercial desleal en el sentido de la Directiva sobre Prácticas Comerciales Desleales[63].

VI. LOS MUCHOS REQUISITOS CONSTITUCIONALES Y LEGALES PARA ADMITIR LOS SISTEMAS BIOMÉTRICOS Y DE RECONOCIMIENTO FACIAL

VI.1. Es obligatoria una regulación legal específica de especial calidad que incluya garantías, que no hay

En general, el uso de sistemas de identificación biométricos es una restricción intensa de no pocos derechos fundamentales que para que sea posible requiere de actividad legislativa intensa, de calidad y muy garantista. En particular, estos altos estándares también resultan exigibles como requisitos para evitar la *prohibición* del futuro AIA y la de la normativa de protección de datos.

Tanto el Derecho Europeo como el Derecho Constitucional español son cada vez más exigentes con el principio de calidad normativa de los derechos fundamentales. Y precisamente los hitos se han dado en el ámbito de la protección de datos. Cabe destacar en general la STJUE (Gran Sala) de 8 de abril de 2014, Digital Rights Asuntos C-293/12 y C-594/12 (nº 54). La legislación debe establecer normas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e imponer salvaguardias para que las personas cuyos datos han sido tratados tengan garantías suficientes para proteger eficazmente sus datos personales contra el riesgo de abuso y contra cualquier acceso o uso ilícitos de esos datos[64]. La ley ha de establecer condiciones sustantivas y de procedimiento y criterios objetivos para determinar los límites del acceso de las autoridades competentes a los datos y su uso posterior[65]. El TC español ha sido extraordinariamente exigente con los principios de calidad de la ley también con relación al derecho de protección de datos personales. Además

63 Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior.

64 También STEDH de 1 de julio 2008, Liberty and Others v. the United Kingdom, 1 July 2008, nº 62 y 63. También Rotaru v. Rumanía, § 57 a 59, y S. y Marper contra el Reino Unido, § 99.

65 De especial interés CEPD, 2022: nº 53 y 55, 15 y 16. Parlamento UE 2021 a): 35-42.

de los importantes precedentes en la STC 290/2000 (en especial, FJ 15º) y en la STC 17/2013 (y su voto particular), cabe destacar la STC 76/2019, de 22 de mayo (en especial FJ 8º): el mandato de calidad "no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares" [66]. Y estas exigencias legales se dan precisamente respecto de datos especialmente protegidos del artículo 9 RGPD y el artículo 10 Directiva (UE) 2016/680, entre los que se incluyen los biométricos. El artículo 9.2 Ley orgánica 3/2018 expresa la reserva de ley[67]. Además, la concurrencia del derecho a no ser sometido a decisiones automatizadas también implica especiales exigencias de regulación legal y garantías (art. 22.2 b) RGPD y artículo 11 Directiva (UE) 2016/680), especialmente cuando se manejan datos especialmente protegidos (art. 22.3º RGPD).

Estas exigencias de calidad normativa en muy buena medida quedan explicitadas y conectadas con las especiales garantías regulatorias del artículo 23 RGPD para las restricciones al derecho de protección de datos. Así pues, se requiere una regulación reforzada, con mayor densidad (Carrasco, 2020: 72), respecto de la que el test de admisibilidad se hace más duro, por lo que la proporcionalidad sólo permitiría en supuestos imperiosos o estrictamente necesarios.

Amén de las garantías de calidad legislativa, como especialmente subraya la STC 76/2019 es la ley la que debe integrar las garantías efectivas que *compensan* el régimen restrictivo de derechos, en nuestro caso por los tratamientos biométricos. Así, la norma legal deberá determinar los fines específicos, la

66 "Según reiterada doctrina constitucional, la reserva de ley no se limita a exigir que una ley habilite la medida restrictiva de derechos fundamentales, sino que también es preciso, conforme tanto a exigencias *denominadas –unas veces– de predeterminación normativa y –otras– de calidad de la ley como al respeto al contenido esencial del derecho, que en esa regulación el legislador, que viene obligado de forma primaria a ponderar los derechos o intereses en pugna, predetermine los supuestos, las condiciones y las garantías en que procede la adopción de medidas restrictivas de derechos fundamentales.* Ese mandato de predeterminación respecto de elementos esenciales, vinculados también en último término al juicio de proporcionalidad de la limitación del derecho fundamental, no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares."

67 "2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad."

fiabilidad y precisión mínimas del algoritmo usado, el periodo de retención de los datos, la posibilidad de auditar estos criterios, la trazabilidad del proceso y otras garantías (Consejo de Europa, 2021).

Pues bien, como se ha expuesto, para los sistemas biométricos la regulación hasta ahora conocida es especialmente la Ley Orgánica 7/2021, de 26 de mayo (o en su caso la LOPD). Esta ley en modo alguno cumple los requisitos de regulación legal y de calidad básicos ni, por supuesto, los requisitos específicos para la implantación de un sistema biométrico concreto. Por cuanto a las normas específicas sectoriales, se trata de un laberíntico conjunto de normas dispersas que tampoco cumplen, ni de lejos estos requisitos de la legalidad. Algunos autores como Carrasco (2020: 71), no obstante, sí que consideran una suficiente base legal[68]. Cabe recordar asimismo, que la posible regulación de la videovigilancia *simple* que pueda haber en modo alguno sirve para las nuevas tecnologías biométricas, siguiendo el mencionado Informe 31/2019 AEPD para el ámbito de la seguridad privada.

Es cierto que en lo relativo al ámbito policial y penal, la UE viene a conceder un margen de regulación amplio a los Estados. Sin embargo, el legislador español no lo ha aprovechado y en este terreno ha sido pretendidamente perezoso y nada cuidadoso. Básicamente ha reiterado el texto de la Directiva (UE) 2016/680. Ha hecho precisamente lo que el CEPD en mayo 2022 acaba de recordar que ni se debe ni puede. Así, una medida legislativa no puede ser invocada como una ley que autoriza el tratamiento de datos biométricos por medio del reconocimiento facial con fines policiales si es una mera transposición de la cláusula general del artículo 10 LED (CEPD, 2022: nº 71, 17). La mera transposición de la cláusula general del artículo 10 Directiva (UE) 2016/680 en el artículo 13 Ley Orgánica 7/2021 no cumple los mínimos estándares exigidos. Lo mismo puede señalarse respecto de las exigencias de regulación legal de calidad de sistemas automatizados que exige el artículo 22 RGPD y el artículo 22 Directiva (UE) 2016/680 al que prácticamente nada añade el artículo 11 Ley Orgánica 7/2021.

68 Así, afirma que "en definitiva, entendemos que hay base legal suficiente para el despliegue de un sistema de reconocimiento facial automático como el analizado, pero sería recomendable una modificación legal que incluyera una mención expresa y un desarrollo que lo dotara de una mayor densidad normativa".

Esta obligatoria e intensa actuación del legislador para la legitimación específica de los sistemas biométricos concurre con la necesaria actuación del legislador en razón del AIA. En este punto cabe recordar que para levantar la teórica prohibición del artículo 5 AIA se exige expresamente la actuación del legislador. Así, el artículo 5. 1 d iii respecto del uso para la detección, localización, identificación o el enjuiciamiento de personas. Y especialmente y en general deben establecerse "normas detalladas" (art. 5.3º) respecto de las autorizaciones concretas del uso de estos sistemas y sobre su supervisión (art. 5.4º). Así pues, el AIA se suma a las obligaciones de regulación legal y de calidad.

Es muy importante subrayar que la regulación del uso de sistemas de identificación biométrica del AIA en modo alguno sirve como la regulación legal que se exige en razón de la normativa de protección de datos. La no prohibición por el AIA de supuestos de reconocimiento facial u otros tratamientos biométricos no supone una habilitación y legalización de los mismos a los efectos de la protección de datos. Esto está claro para instituciones especializadas como el CEPD-SEPD (2020: Nº 31) o Parlamento UE (2021 a). Sin embargo, en el texto del AIA esto solamente puede deducirse del Considerando 24 propuesta del AIA y puede quedar sujeto a interpretaciones. No obstante, por su importancia debería ser más claro y bien merece una regulación específica en el texto del AIA. En este sentido, con acierto se ha propuesto aclararlo expresamente en el texto[69] y que sería preferible que la regulación de sistemas biométricos del AIA converja con los artículos 9 RGPD y 10 de la Directiva (UE) 2016/680 y que el AIA enumere los fines para los que se permite la identificación biométrica a distancia en tiempo real[70].

Las carencias de regulación legal específica de sistemas biométricos no ha pasado en modo alguno desapercibida. En España especialmente es claro el Informe 010308/2019 AEPD sobre reconocimiento facial en servicios de

69 Parlamento UE b): "Los apartados (1) y (2) se entienden sin perjuicio de las prohibiciones que se aplican cuando una práctica de inteligencia artificial viola otras leyes, incluida la ley de protección de datos, la ley de no discriminación, la ley de protección del consumidor y la ley de competencia."

70 Así se propone desde el Parlamento un artículo 5 bis *(Ibídem)*.

videovigilancia privada[71], en el que se afirma que el marco legal actual en modo alguno cuenta con la legislación específica que se requiere, si bien no excluye su posible regulación legal en ámbitos como el de las infraestructuras críticas. Estas carencias de regulación legal se reiteran en igualmente en el caso Mercadona[72] o el de uso de reconocimiento facial para evitar el fraude en exámenes[73].

Y no es una carencia solo española. Así, la Autoridad de Protección de Datos de Hamburgo (DPA Hamburgo, 2018: 19-27) consideró que la videovigilancia indiscriminada y la posterior extracción y almacenamiento biométrico durante la Cumbre del G20 de 2017, carecían de bases legales suficientes. En el caso del "Sistema Automatico di Riconoscimento Immagini S.A.R.I." el Dictamen del Garante de 16 de abril de 2021 señaló la necesidad de una base normativa adecuada que defina claramente las situaciones en las que es posible el uso de tales sistemas, que no deje una amplia discrecionalidad a quienes los utilizan[74]. La autoridad neerlandesa también ha criticado el insuficiente marco legal biométrico (EDRI, 2020).

VI.2. Se necesita un verdadero debate democrático que se refleje en la acción legislativa y control jurisdiccional

El desarrollo de tecnologías de IA con datos biométricos y de reconocimiento facial es un reto esencial al que se enfrentan las sociedades democráticas en el siglo XXI. Posiblemente la sociedad simplemente lo perciba como una más de las tantas amenazas del mundo digital a los derechos en general y a la privacidad en particular. Hay encuestas en 2015 en las que se da una oposición más clara[75],

71 https://www.aepd.es/es/documento/2019-0031.pdf

72 AEPD, Resolución procedimiento sancionador PS 120/2022, https://www.aepd.es/es/documento/ps-00120-2021.pdf

73 AEPD. Informe sobre reconocimiento facial en los exámenes. N/REF: 0036/2020, pág. 16. https://www.aepd.es/es/documento/2020-0036.pdf
Véase también la resolución de advertencia n.º: E/05454/2021 de la AEPD dirigida a la Universidad Internacional de La Rioja (UNIR).

74 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877

75 Se sigue de FRA (2020: 19) con remisión a FRA (2015).

mientras que otras sólo reflejan un rechazo de un 3%[76]. En 2019 en Reino Unido tampoco había un nítido rechazo: se acepta el reconocimiento facial para el uso policial y no eran más de un tercio quienes se sienten incómodos por su uso en aeropuertos, transporte, escuelas, supermercados o lugar de trabajo[77].

Ciertamente el futuro AIA ha concentrado el interés desde la sociedad civil. El proyecto de la Comisión Europea *iBorderCtrl* generó protestas públicas, que se unieron a la respuesta a la futura regulación del AIA con la campaña "reclama tu cara" (https://reclaimyourface.eu/). Incluso hay una Iniciativa Ciudadana Europea desde 2021 para la prohibición de las prácticas de vigilancia biométrica masiva[78]. Este movimiento desde la sociedad civil ha sido seguido por el Parlamento UE en su Resolución de 6 de octubre de 2021 sobre inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016(INI))[79]. En la misma se marca una clara línea prohibitiva. Asimismo, el tema atrae la atención de parte importante de las enmiendas al AIA tanto de los ponentes como de los grupos[80]. Por ello, tras su paso por el Parlamento UE es posible que el futuro AIA marque algunas líneas algo más restrictivas. No obstante, considero que la "prohibición" de los sistemas de identificación biométrica es más bien un eslogan, una "excepcionalidad" que queda en manos de los legisladores y, en su caso, de la autorización de jueces o autoridades. Las excepciones en materia de defensa, inteligencia y seguridad y la regulación laberíntica y opaca incluso para especialistas puede permitir que la excepción bien pueda convertirse en la regla.

---

76 Así, respecto del uso de reconocimiento facial en Niza, solo el tres por ciento de los 900 encuestados se opuso directamente (FRA, 2020: 19).

77 Solo el 9 % se siente completamente incómodo cuando se utiliza el reconocimiento facial con fines policiales, y el 10 % cuando se utiliza en los aeropuertos. Sin embargo, el 24 % no se siente cómodo con el uso del reconocimiento facial en el transporte público, el 28 % en las escuelas, el 37 % en los supermercados y el 37 % en el lugar de trabajo. (FRA 2020: 19, Ada Lovelace Institute, 2019).

78 Nº ECI(2021)000001, https://europa.eu/citizens-initiative/initiatives/details/2021/000001_es

79 https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_ES.html

80 https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence
https://www.euractiv.com/section/digital/news/ai-regulation-filled-with-thousands-of-amendments-in-the-european-parliament/

Eso sí, los deberes del legislador no son pocos y, en teoría, la regulación legal es un mecanismo de deliberación pública y democrática. Sin embargo, la Ley Orgánica 7/2021, de 26 de mayo, aprobada sin pena ni gloria –con cinco votos en contra– es buena muestra de la dejadez e incumplimientos del legislador, de la total ignorancia por la sociedad civil y, por qué no decirlo, de los especialistas. No ha habido debate social alguno. Según se ha visto, sigue siendo necesaria una regulación legal particular, pues el marco legal es insuficiente. Hay que desear que este proceso legislativo no sólo se dé y con elevada calidad técnica, sino con la suficiente atención social que permita el imprescindible debate democrático. Y en todo caso, y ante la más que previsible carencia legislativa, esperemos que las autoridades judiciales e independientes responsables efectúen el necesario control tanto de las normas como de su aplicación. Hay que esperar, además, que la futura regulación que habilite estos sistemas no sea consecuencia de un momento crítico como sería un importante atentado.

VI.3. Los límites del consentimiento y la legitimación de sistemas biométricos privados

La legislación de protección de datos abre la puerta a que el consentimiento puede legitimar el tratamiento de datos biométricos especialmente protegidos (artículo 9.2º a RGPD; CEPD, 2020: 20 y ss.; de interés, Santiesteban, 2021: 516 y ss.). Sin embargo, para el sector público hay que partir de que esencialmente el consentimiento sólo excepcionalmente puede legitimar el tratamiento de datos (en especial, Informe 175/2018 AEPD[81]) y, en todo caso, debe contarse con la intensa habilitación legal que se ha señalado. Algo similar sucede en el contexto laboral en el que también hay una clara asimetría de las partes y el tratamiento de datos sólo excepcionalmente puede legitimarse por el consentimiento (CEPD, 2020: 8).

En el sector privado se da la especial dificultad de vincular y justificar el uso de sistemas biométricos respecto del ámbito penal y policial. Para Simó (2022: 7) es "aberrante" afirmar interés público esencial que pueda justificar

81 Puede accederse en https://elconsultor.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbH1czUwMDA0N7M0MTRXK0stKs7Mz7M1MjC0MDQ0MgIJZKZVuuQnh1QWpNqmJeYUpwIAE_FjpzUAAAA=WKE

sistemas biométricos en estos ámbitos. En esta línea, el Informe 0283/2013 AEPD no consideró admisible la instalación de un sistema de control de huella dactilar por una empresa de venta y alquiler de vehículos, previo consentimiento, con la finalidad de identificar a los posibles autores de algunos delitos. Especialmente el caso Mercadona se ratifica en general esta posición. Por su parte, la mencionada Resolución del Parlamento Europeo, de 6 de octubre de 2021, ha pedido que se "prohíba el uso de las bases de datos de reconocimiento facial privadas" (nº 28). No obstante, no hay que excluir radicalmente la posibilidad de intereses públicos que puedan legitimar tratamientos biométricos fundados en la seguridad e incluso intereses públicos fundamentales respecto del artículo 9. 2º RGPD. La misma AEPD señala que una regulación podría por ejemplo habilitar la vigilancia privada con estos sistemas en infraestructuras críticas.

En contextos privados el consentimiento tiene mayores posibilidades para legitimar tratamientos de datos biométricos (art. 9.2 a) RGPD). Pero en todo caso hay especiales restricciones y, sobre todo, exigencias de ley. Así, en muchos supuestos puede haber prohibiciones legales nacionales de tratamientos de datos especialmente protegidos aunque se cuente con el consentimiento. De hecho, sería deseable que haya una regulación expresa que impida tentaciones como las del caso Mercadona y será necesaria una ley en el ámbito laboral o en general el educativo, por ejemplo[82]. La misma AEPD señala que el uso de estas técnicas tendría sentido en el ámbito de infraestructuras críticas, pero acompañado de la oportuna regulación legal.

Además, no hay que olvidar que el consentimiento estará excluido en todas las relaciones asimétricas donde no hay libertad. Así, en principio y en general, para implantar sistemas biométricos y de reconocimiento facial no se puede partir del consentimiento[83].

Aunque se cuente con el consentimiento, el sistema biométrico puede suponer un tratamiento desproporcionado por sujetos privados, que puede hacer nulo

82 En cuanto a los requisitos de consentimiento, ver CEPD (2020) y por cuanto a los obstáculos al consentimiento Selinger y Hartzog (2020).

83 Así por ejemplo en el Informe 0392/2011 AEPD sobre reconocimiento de alumnos de un centro universitario a través de programas de reconocimiento facial.

el consentimiento (con especial aplicación del artículo 7. 4º RGPD). Y, como se insistirá, el cumplimiento de los principios de protección de datos especialmente el de la necesidad, idoneidad y proporcionalidad se hace más complejo con relación a intereses y finalidades en entidades privadas.

En todo caso, en principio en el terreno del marketing e intereses y reconocimiento por ejemplo por plataformas, en principio sí que será posible el consentimiento expreso (art. 9. 2º a) RGPD)[84]. Además, la categorización, el perfilado o el reconocimiento de emociones con biometría excluye que los datos biométricos se consideren datos especialmente protegidos. En cualquier caso, deben tenerse en cuenta los criterios claramente restrictivos del TC sobre el consentimiento dado por los interesados en las redes sociales (STC 27/2020, de 24 de febrero de 2020).

Una vía paralela de legitimación para el tratamiento de datos biométricos incluso para el ámbito policial y penal es que los datos se hayan hecho manifiestamente públicos (art. 9.2º e) RGPD). Ahora bien, como ha señalado el CEPD "difundir y hacer públicas fotos o vídeos no sería en modo alguno suficiente, sería necesario haber hecho deliberadamente que la plantilla biométrica (y no simplemente una imagen facial) sea libremente accesible y pública a través de una fuente abierta" (CEPD, 2022, nº 75: 19). No es suficiente que el interesado no haya activado o establecido características específicas de privacidad. La configuración por defecto de un servicio, por ejemplo, hacer que las plantillas estén disponibles públicamente, o la ausencia de elección, por ejemplo, que las plantillas se hagan públicas sin que el usuario pueda cambiar esta configuración, no debe interpretarse en modo alguno como datos manifiestamente hechos públicos (*Ibídem*, nº 76).

El Parlamento UE (2021 a: 87) presta esencialmente su atención a la gestión automatizada del consentimiento para el uso de técnicas biométricas proponiendo un artículo específico (Artículo 5 *sexies*). Posiblemente, la más completa

84 Parlamento UE, 2021: 11. Véase CEPD 2019 y 2020. En 2019 afirma que La Junta Europea de Protección de Datos (JEPD) considera que "el uso de la videovigilancia, incluida la funcionalidad de reconocimiento biométrico, instalada por entidades privadas para sus propios fines (por ejemplo, de marketing, estadísticos o incluso de seguridad) requerirá, en la mayoría de los casos, el consentimiento explícito de todos los interesados" (artículo 9, apartado 2, letra a), del RGPD)".

resolución en la materia es la española del caso Mercadona que considera que no se dan los presupuestos para levantar la prohibición de tratamientos de datos biométricos especialmente protegidos. Asimismo, en ámbito privado el 12 de agosto de 2019 un Tribunal de Ámsterdam, 7728204 CV VERZ 19-9686 consideró inadmisible utilizar escáneres de huellas dactilares en las cajas registradoras de una cadena de zapaterías en aquella ciudad. Se entendió que era una medida desproporcionada para el nivel de seguridad requerido en las zapaterías.

La sentencia de 7 de mayo 2021 del Tribunal de Justicia do Estado de São Paulo[85] prohibió el reconocimiento biométrico para la personalización de publicidad a la concesionaria de la línea 4 del Metro de Sao Paulo (Via Quatro). Se trataba de un sistema de clasificación y categorización para marketing nada transparente, sin información ni por supuesto consentimiento de los afectados.

VI.4. Sólo los sistemas "estrictamente necesarios": un escrutinio muy estricto de la necesidad y proporcionalidad

Aunque sea difícil, el sistema biométrico puede contar con legitimación particular y específica por la vía legal o en su caso el consentimiento u otras. Pero aun contando con legitimación y una regulación legal de calidad, estos sistemas tan impactantes en la sociedad y los derechos de las personas han de ser sometidos a un escrutinio muy estricto especialmente por cuanto a su necesidad, proporcionalidad, adecuación o minimización. Como sucedió en el caso SYRI (sentencia de 5 de febrero de 2020 del Tribunal de Distrito de la Haya)[86], como punto de partida cabe seguir la STEDH de 4.12.2008, S. Y Marper C. Reino Unido: "cualquier Estado que reclame un papel pionero en el desarrollo de nuevas tecnologías tiene una responsabilidad especial por golpear el recto equilibrio a este respecto" (n.o 112). Así pues, se parte de un canon de control más estricto por el deber de "responsabilidad especial cuando aplican nuevas tecnologías" de los Estados (nº 6.6 y 6.84 sentencia SYRI de 5 de febrero) y en concreto el legislador (6.85). El SEPD (2019 a)

85 https://www.accessnow.org/cms/assets/uploads/2021/05/Sentenc%CC%A7a-Maio-7-2021-Sao-Paulo-metro.pdf

86 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878

ha prestado especial atención al análisis de proporcionalidad respecto de la privacidad y protección de datos y alertado de los problemas al respecto específicamente respecto del reconocimiento facial (2019 b).

La Directiva (UE) 2016/680 en su artículo 10 y el artículo 5 AIA afirman el canon de que el sistema biométrico sea "estrictamente necesario". Y el CEPD analiza específicamente este canon en el ámbito biométrico[87]. Y obviamente "el listón de la necesidad y la proporcionalidad es más alto cuanto más profunda es la injerencia" (CEPD, 2022: 46). Se recuerda que para el TJUE la discrecionalidad del legislador ha de ser limitada y no vale cualquier objetivo de interés general[88]. De igual modo, si hay decisiones automatizadas el canon es más estricto y, por consiguiente mayores las garantías necesarias (art. 11 Directiva (UE) 2016/680, art. 22.3º RGPD).

Para el análisis concreto procedente habrá que atender la finalidad o finalidades perseguidas. Bajo el régimen general de protección de datos, en muchos casos se necesitará un "interés público esencial" (artículo 9. 2º g) que pueda justificar el tratamiento biométrico, como mínimo en todos los supuestos de uso por el sector público. Gutiérrez ha analizado especialmente el –mero– interés público (no esencial) que puede ser suficiente en muchos supuestos de videovigilancia (Gutiérrez, 2020: ap. 2°). Sin embargo, la exigencia de interés público cualificado para el legislador será la regla general y ello va en la línea de una mayor intensidad de necesidad y justificación del concreto sistema que el legislador quiera legitimar. Y de nuevo hay que remitir a la muy exigente STC 76/2019, de 22 de mayo precisamente respecto de la cualificación del interés público esencial. Será muy importante poder justificar que entre las alternativas eficaces posibles no hay otra similar que no suponga un tratamiento tan intromisivo. Y para la ponderación con anterioridad se han señalado los elementos más relevantes para ponderar la intensidad de la afección a los derechos en juego: finalidades reales y ocultas, identificación, rastreo, seguimiento, categorización, perfilado de emociones o predicción de

87 CEPD, 2022: apartados 3.2.1.2 y 3.1.3.4, nº 73 y ss., 19 y ss. y nº 50 y ss., 15 y ss.

88 STJUE (Gran Sala) de 8 de abril de 2014, Digital Rights Asuntos C-293/12 y C-594/12, párr. 51.

comportamientos, contextos penales, laborales, políticos, religiosos, educativos, lugares de acceso público y otros sensibles, duración del tratamiento y mantenimiento de datos, realización por sujetos públicos o privados, menor transparencia y explicabilidad, garantías de conservación de los datos, etc.

En Alemania, el Tribunal Constitucional Federal alemán, 11 de marzo de 2008, 1 BvR - 1 BVR 2074/05 --1254/07[89] deja claro que cuanto más grave sea la injerencia, más restrictivas deben ser las condiciones de uso de los datos y la proporcionalidad de la recogida de datos depende en gran medida de las disposiciones que limitan el almacenamiento y el uso de los datos y, como se ha adelantado al inicio y he tenido ocasión de estudiar en profundidad en otro estudio, después del presente trabajo, la importante sentencia de 16 de febrero de 2023 del TC alemán es muy exigente con el legislador para poder utilizar sistemas automatizados, y excluye la inteligencia artificial en ámbitos policiales y de seguridad. El Consejo Constitucional francés en 2012[90] consideró que la creación de una base de datos biométricos, que permite identificar a la práctica totalidad de la población francesa por sus huellas dactilares, era una injerencia inconstitucional en el derecho al respeto de la vida privada.

Y ya de modo concreto para el ámbito que nos ocupa, cabe mencionar que sobre la base de la proporcionalidad la autoridad de Hamburgo fue contraria a la base de datos policial en el contexto de la cumbre del G20 de 2017, aunque, un juez luego lo aceptó[91]. El Garante, autoridad italiana de protección de datos, el 16 de abril de 2021 consideró que el *Sistema Automatico di Riconoscimento Immagini* (SARI) utilizado desde 2019 era una forma de vigilancia indiscriminada y masiva si se utilizaba tal y como estaba diseñado. En Francia, la CNIL fue contraria a un sistema de control de acceso basado en el reconocimiento facial en las escuelas, Consejo regional de Provenza-Alpes-Costa Azul, decisión que fue ratificada por el Tribunal Administrativo de Marsella de 27 de

89 http://www.bverfg.de/e/rs20080311_1bvr207405.html

90 https://www.conseil-constitutionnel.fr/decision/2012/2012652DC.htm

91 Como se ha detallado al inicio, la autoridad de datos de Hamburgo ordenó eliminar la base de datos policial de plantillas biométricas, pero un tribunal de primera instancia anuló la orden y el proceso sigue judicializado.

febrero de 2020[92]. Por el contrario, la sentencia de 4 de septiembre de 2019 del caso de Gales sí consideró admisible el sistema de identificación biométrica[93].

VII. LA BATERÍA DE GARANTÍAS EN EL DISEÑO, DE EVITACIÓN DEL SESGO Y LA DISCRIMINACIÓN Y DE OBLIGACIONES DE TRANSPARENCIA

VII.1. Garantías y exigencias de responsabilidad activa y en el diseño que impone a los sistemas biométricos el RGPD y el futuro AIA

En el caso de que existan sistemas de identificación biométricos, además de la regulación legal y la necesaria legitimación de los mismos, teniendo en cuenta su necesidad y proporcionalidad, habrá que cumplir toda una batería de garantías y exigencias de estudios de impacto, responsabilidad activa y en el diseño.

Como en otros lugares he señalado (Cotino, 2022 a) las nuevas tecnologías exigen adoptar de raíz los sistemas de responsabilidad activa, demostrada, en el diseño bajo el modelo jurídico del "más vale prevenir que curar" y el cumplimiento normativo. Y como lo que está en juego no es solo el derecho de protección de datos, sino prácticamente todos los derechos y los principios democráticos, los sistemas preventivos deben extenderse al impacto multirriesgo ético y social, como especialmente subraya Mantelero (2022 a). En esta línea, es del todo acertada la Carta de Derechos Digitales (2022 b) cuando su apartado I. 4 "declara que el principio de cumplimiento normativo desde el diseño es de aplicación íntegramente al desarrollo de los entornos digitales, y por ello los desarrollos científicos, tecnológicos y su despliegue contemplarán en la determinación de sus requerimientos un análisis sobre el cumplimiento de tal principio". Y, también para todos los derechos su XVIII. 4º afirma

92 La autoridad francesa consideraba que el sistema violaba los principios de proporcionalidad y minimización de datos (CNIL, 2020), ver decisión en el asunto nº 1901249 de 27 de febrero de 2020, http://marseille.tribunal-administratif.fr/content/download/178764/1756210/version/1/file/1901249.pdf . El Tribunal Administrativo de Marsella anuló la decisión del consejo regional de Provenza-Alpes-Costa Azul de la puesta en marcha en Marsella y Niza por falta de base legal, ver párrafo 13.

93 Ya referida al inicio, ver párrafos 122 y ss., sobre necesidad, 135 y ss.; conclusión, en párrafo 159.

que "será necesaria una evaluación de impacto en los derechos digitales en el diseño de los algoritmos en el caso de adopción de decisiones automatizadas o semiautomatizadas".

En todo caso, siguiendo la regulación actual, los usos de IA para reconocimiento facial como tratamientos de datos han de seguir todos los estándares de la responsabilidad proactiva, de ahí que la marca IA de la UE se defina como "ética en el diseño" (Cotino, 2019; Martínez, 2019). De especial importancia es la realización de estudio de impacto del que ya el Grupo del Artículo 29 (2012) asentó los elementos básicos para el caso de biometría y más recientemente el Consejo de Europa (2021: 13-15). El mismo resultará obligatorio (art. 27 Directiva (UE) 2016/680, art. 35 RGPD). Además, el CEPD recomienda que se hagan públicos los resultados de dichas evaluaciones, o al menos los principales resultados y conclusiones para aumentar la confianza y la transparencia (CEPD, 2022: nº 57). La normativa de datos impone también que se lleve a cabo el registro de actividades (art. 25 Directiva (UE) 2016/680), análisis de riesgos, obligaciones de seudonimización, anonimización, gestión de la calidad de los datos, documentación de violaciones, medidas de seguridad adecuadas. A este respecto destaca la necesidad de compartimentar datos, separar datos, plantillas y datos brutos, cifrar los datos y plantillas biométricas, definir una política de cifrado y gestión de claves, asociar una firma o un *hash* a la integridad a los datos y prohibir cualquier acceso externo a los datos biométricos. El CEPD (2022: nº 98, ap. 3.2.5.3), recuerda que la seguridad será aún más relevante si la autoridad policial utiliza un proveedor de servicios externo y recuerda la ISO/IEC 24745, Seguridad de la información, ciberseguridad y protección de la privacidad – Protección de la información biométrica.

Estas garantías son generalmente aplicables y en el caso de sistemas biométricos deben exigirse con especial intensidad. Además, como garantías "compensatorias" deben incluirse algunas como auditorías con confidencialidad, intervención de las autoridades de datos, intervención y participación de autoridades judiciales, independientes o incluso legislativas. Las autoridades de datos también consideran que antes de desplegar los sistemas biométricos también habrá de darse la consulta previa a la autoridad de control (art. 28 Directiva (UE) 2016/680, CEPD, 2022: nº 97). Cabe también señalar que las autoridades de protección de datos ya han interpretado y "extraído" a partir de la actual normativa y principios de la protección de datos no pocas

obligaciones sobre gobernanza de los datos, calidad y robustez de los sistemas, evitación de sesgos y discriminación, obligación de auditorías, así como importantes obligaciones de transparencia. Y todo ello sin esperar a la aprobación de la normativa de IA. Baste seguir las Guías sobre IA de la AEPD (2020 y 2021) o del Grupo del artículo 29 (2018), ahora CEPD.

Lo anterior desde la perspectiva de protección de datos. Pero es que los sistemas de identificación biométricos son sistemas de alto riesgo de IA (Anexo I. 1º) y habrán de cumplir las muchas obligaciones del futuro AIA[94]. Es más, el reconocimiento facial en diversos casos implica un régimen específico, al que se añaden más obligaciones y garantías. Como es sabido, un sistema de alto riesgo supone aplicar medidas adecuadas de evaluación y mitigación de riesgos (art. 9 AIA), a utilizar conjuntos de datos de alta calidad con buena gobernanza (art. 10 y 16 AIA), obligaciones de los desarrolladores de generar documentación técnica para los clientes o usuarios del sistema (art. 11). También es esencial el diseño de la IA para que genere registros y *logs* de funcionamiento (art. 12) y para el reconocimiento facial las exigencias son exhaustivas (art. 12. 2). También los desarrolladores han de garantizar la transparencia a los usuarios de estos sistemas (art. 13). Las obligaciones de supervisión humana (art. 14) incluyen el *plus* de que la identificación resultante ha de ser verificada y confirmada por al menos dos personas físicas (art. 14.º) antes de que se tomen decisiones por el usuario del sistema. Bien es cierto que como señala Pérez y García (2021: 85) esta supervisión puede resultar especialmente difícil e imprecisa, incluso apunta que una aparente supervisión humana puede servir para difuminar la responsabilidad sobre el sistema y desviarla a los operadores de primera línea que no tienen control efectivo sobre el sistema. Además, me permito apuntar que estas garantías de verificación pueden ser cuestionables, máxime si de ello puede derivar la no aplicabilidad de las garantías del artículo 22 RGPD. Téngase en cuenta que si se considera que el sistema está supervisado, puede no considerarse que es sólo automatizado por lo que quedaría fuera de las especiales garantías del artículo 22. También los sistemas de reconocimiento han de estar diseñados con un nivel adecuado de precisión, solidez y ciberseguridad (art. 15 AIA). Asimismo, hay que tener en cuenta que para los sistemas IA de identificación

94 Sobre la aplicación del principio de responsabilidad proactiva y el diseño para el ámbito de la IA destaca recientemente, Hernández, 2022. También, Alberto, 2017; Navas, 2017; Martínez, 2019.

biométrica se siguen estrictos procedimientos de evaluación de la conformidad ex ante y no a través de la autoevaluación como regla general (artículo 43. 1º; art. 19. 2º). Después se someten al sistema de vigilancia del mercado y de supervisión, y los sistemas biométricos cuentan también con reglas especiales en el ámbito policial con respecto a las autoridades competentes (art. 63. 1º). Todas estas exigencias del futuro AIA serán desarrolladas además por todo un armazón de normas técnicas y de armonización, que serán acompañadas de la normalización técnica de la IA que está en fase de desarrollo a través de organismos como el CEN-CENLEC.

Y todo este arsenal de medidas preventivas, tecnológicas y de garantías a adoptar, habrá de ser concretado por la legislación específica que legitime el sistema biométrico del que se trate. La STC 76/2019, de 22 de mayo ha sido muy clara en este sentido. Ahora bien, lo cierto es que si "por defecto" todas estas garantías ya las establece la normativa, puede cuestionarse la necesidad y utilidad de reiterar o adaptar las mismas –y con rango de ley– para cada sistema de identificación biométrico del que se trate. Cierto es que el legislador podrá no sólo adaptar este tipo de medidas, sino, además, podrá añadir las que consideren específicamente necesarias en razón del uso y circunstancias concretas. Se da así una especial oportunidad de añadir la perspectiva señalada por cuanto a los análisis multirriesgo de los diferentes derechos en juego, así como las posibilidades de participación y de vinculación a la sociedad civil por cuanto al uso de estos sistemas.

En todo caso, como a continuación se señala las medidas a adoptar para evitar los sesgos y la discriminación son especialmente importantes. Asimismo, la legislación puede reforzar uno de los mayores riesgos de las tecnologías de reconocimiento como es la "desviación de la finalidad" (Parlamento UE 2021 b: 16). Y que se utilicen datos para apoyar el sistema, desviando su finalidad y sin una ley que lo permita con garantías (CEPD, 2020 a: 15-16). Es por ello que es especialmente necesaria la garantía de una arquitectura compartimentada, para evitar su uso con fines no autorizados.

El cumplimento de todas estas obligaciones de responsabilidad proactiva acaba secuenciándose en toda una serie de medidas a adoptar en las diversas etapas de interés (en especial CEPD, Anexo II: 29-35): al momento de concebir y diseñar el sistema de identificación biométrica, o al momento de preparar

los pliegos y mecanismos de contratación del mismo. También durante el desarrollo o la adquisición del sistema y antes de su despliegue, momento en el que el entrenamiento del sistema, la comprobación de errores y sesgos o la seguridad del mismo es especialmente relevante. Tras el despliegue del sistema cobra especial protagonismo garantizar la intervención humana y la supervisión de los resultados y la reevaluación de su funcionamiento, así como la garantía de los derechos de los interesados afectados de acceso de información y frente a posibles vulneraciones de derechos.

VII.2. Medidas para la evitación de sesgos y errores de los sistemas biométricos

Los sistemas biométricos son siempre probabilísticos, por lo que el riesgo de errores de los sistemas de reconocimiento facial parece ser muy alto[95]. Como recuerda el FRA, un riesgo de un 0,01% –aparentemente muy bajo para la IA– respecto de un sistema aplicado a millones de personas puede afectar y mucho a cientos de personas. Los riesgos de error siguen siendo bastante altos, tanto de falsos negativos (el *software* de reconocimiento facial no encuentra una cara que está presente en una imagen); así como de falsos positivos en los que el sistema identifica una estructura no facial como un rostro real. Una causa habitual es la insuficiencia de datos de entrenamiento, así como la falta de calidad o veracidad de las bases de datos (Consejo de Europa, 2021: 9, también 12-13). Frente a ello es necesario adoptar importantes medidas, especialmente de calidad de los datos (FRA, 2018: 81-97). Especialmente el futuro AIA implica importantes obligaciones durante el ciclo de vida del sistema biométrico (diseño, adquisición, despliegue y funcionamiento). Si el sistema IA es de alto riesgo hay importantes obligaciones de gestión de calidad y gobernanza de datos, así como las de supervisión humana y evaluación del sistema. De este modo se impone la percepción de errores, minimización de sesgos y de posibles discriminaciones. Desde la perspectiva de la protección de datos, también rige el principio de calidad de los datos de entrada del sistema (art. 5 RGPD, artículo 7 Directiva (UE) 2016/680) y las autoridades de protección de datos ya derivan importantes exigencias de exactitud y calidad

95 Así lo recuerdan entre otros el Consejo de Europa (2021) y el CEPD (2020: nº 27 y 29, 10 y ss. Asimismo, Parlamento UE (2021 a), ap. 2. 1º sobre falsos positivos y negativos. En cualquier caso, respecto de la perspectiva de discriminación destacan especialmente los trabajos de la FRA (2019 y 2020).

de los datos de entrenamiento y de entrada, de verificación del funcionamiento de los algoritmos, auditorías, etc. (AEPD, 2020 y 2021). Asimismo, las obligaciones de transparencia y explicabilidad del sistema permiten a los usuarios y a los interesados y afectados la detección de posibles errores, sesgos o discriminaciones.

Así pues, los responsables del sistema biométrico han de comprobar la calidad de las imágenes y plantillas biométricas insertadas en las listas de vigilancia para evitar posibles falsas coincidencias. El responsable del sistema debe ser capaz de establecer los requisitos de rendimiento y expresarlos en la métrica más adecuada. Hay diversas alternativas. Es útil distinguir entre falsos positivos (ej.: se reconoce a una imagen como que sí que está en lista de vigilancia) y los falsos negativos (persona buscada que no es reconocida). Según el sistema y su concreta finalidad y configuración hay que valorar la importancia de unos y otros, conocer las métricas de rendimiento y los umbrales aceptables. A mayor umbral habrá menos personas erróneamente localizadas, pero también más personas que escapan al sistema. En Detroit Robert Williams fue detenido porque un algoritmo le confundió con otro y el tema está judicializado[96]. Los mismos días de cárcel que sufrió en Buenos Aires Guillermo Federico Ibarrola por un falso positivo[97].

Y a los errores posibles hay que añadir los problemas de sesgos y posible discriminación de los sistemas biométricos y de reconocimiento facial Así, por ejemplo, la sensibilidad a la luz afecta a personas de piel muy clara o muy oscura y ciertos colectivos están más expuestos a los falsos positivos y más personas sean detenidas por error por su color de piel. También los menores de 13 años parecen ser especial objeto de errores (FRA, 2020: 27-28: FRA 2018: 17).

VII.3. Obligaciones de información y transparencia de los sistemas biométricos

El principio de transparencia de protección de datos exige toda una serie de información sobre la existencia del sistema de reconocimiento, elementos

96 https://elpais.com/tecnologia/2021-05-01/el-hombre-que-puede-acabar-con-la-tecnologia-de-reconocimiento-facial-en-estados-unidos.htmlb

97 https://www.accessnow.org/buenos-aires-y-sao-paulo-suspenden-reconocimiento-facial/

básicos de funcionamiento y recepción de datos y destino de los mismos. No obstante, lo normal en el ámbito policial y criminal será la excepción de estos principios por cuestiones de seguridad (Considerando 26 Directiva (UE) 2016/680). Y es la ley la que debe regular estas excepciones de las obligaciones de informar. Dicha ley ha de cumplir con los requisitos de los artículos 13. 3º y 15 Directiva (UE) 2016/680 o, en general, los requisitos de los límites a los derechos del artículo 23 RGPD. A este respecto, la FRA (2020: 24) insiste en la necesaria justificación de las restricciones.

Pero aunque se regulen excepciones y restricciones legales, el CEPD (2022: nº 85, 22-23) recuerda que, en cualquier caso, el responsable del tratamiento deberá garantizar que se facilite efectivamente la información en relación con, al menos, los siguientes elementos:

— identidad y datos de contacto del responsable del tratamiento, incluido el responsable de la protección de datos,

— la finalidad del tratamiento y que se trata de un tratamiento a través de sistemas de reconocimiento facial,

— el derecho a presentar una reclamación ante una autoridad de control y los datos de contacto de dicha autoridad,

— el derecho a solicitar el acceso, la rectificación o la supresión de los datos personales y la limitación del tratamiento de los mismos.

Es más, en la medida en la que el sistema biométrico implicara un tratamiento sólo automatizado del artículo 13 Directiva (UE) 2016/680 o 22 RGPD, la transparencia tendría una especial dimensión, incluyendo la lógica del algoritmo y sus parámetros básicos, explicabilidad, derecho al recurso e intervención humana. En principio, no habrá nunca casos de decisiones sólo automatizadas, en tanto en cuanto que será obligatoria la supervisión humana del AIA.

En cualquier caso, el CEPD (2022: nº 87) para sistemas automatizados de identificación biométrica afirma que si los datos personales se recogen sin el conocimiento del interesado, como objeto de un procedimiento de cooperación penal o en la situación de que los datos personales se traten en el marco de

operaciones encubiertas, si la toma de decisiones se realiza únicamente sobre la base del sistema de reconocimiento, los interesados deben ser informados de las características de la toma de decisiones automatizadas. Además el artículo 13.2º Directiva (UE) 2016/680 obliga a informar sobre la base jurídica del tratamiento, información sobre el lugar donde se recogieron los datos personales sin el conocimiento del interesado, el período durante el cual se almacenarán los datos personales o, cuando esto no sea posible, los criterios utilizados para determinar dicho período y las categorías de destinatarios de los datos personales (incluidos terceros países u organizaciones internacionales).

Pues bien, lo cierto es que parece que, en la realidad, todas estas prevenciones y garantías mínimas de transparencia que claramente se afirman desde la UE parecen evanescerse en la realidad en España. Por lo que he podido conocer, cuando se ha ejercido el derecho de acceso a la información pública al respecto a autoridades policiales, las respuestas han sido por lo general muy insatisfactorias en tanto en cuanto se acude a que se trata de materias clasificadas por lo que ni siquiera estarían en el ámbito de aplicación de la Ley Orgánica 7/2021 (art. 2. 3º d) o por cuestiones de seguridad (art. 14 Ley 19/2013)[98].

VIII. A MODO DE CONCLUSIÓN: SISTEMAS DE IDENTIFICACIÓN BIOMÉTRICA SÍ, PERO CON GARANTÍAS QUE HOY NO PARECEN DARSE

Según uno conoce más sobre los sistemas biométricos y de reconocimiento facial ya existentes encuentra muchos más motivos para alarmarse y preocuparse por su uso en nuestras sociedades democráticas. Aunque también hay que aprovechar las oportunidades que ofrece para, entre otros terrenos, el

98 Me remito a la investigación coordinada por el equipo liderado por Lucía Martínez Garay, Universidad de Valencia-Amnistía Internacional, sobre sistemas IA públicos del ámbito policial y penitenciario. En concreto, derechos de acceso ejercidos por uno de los miembros del equipo frente a la Guardia Civil (Exp. Transp. nº 062893) y los Mossos d'Esquadra (19 de noviembre de 2021, respuesta 18 de enero de 2022). En el caso de la Guardia Civil, se afirma que estos sistemas de identificación biométrica quedan afectados por Acuerdo del Consejo de Ministros de 28 de noviembre de 1986, ampliado por Acuerdos de 17 de marzo y 29 de julio de 1994, otorga el carácter de "Reservado" a aquella información relativa a "las plantillas de personal y medios y de equipo de las Unidades". En el caso de solicitud de información sobre Sistema Automático de Identificación Biométrica (ABIS) (nº expediente: 001-062892, la denegación es en razón del artículo 14 Ley 19/2013.

ámbito de la seguridad pública y nacional. Pero con garantías. Después de remitir este estudio Rivero (2023) realiza una interesante aproximación a esta materia. Advierte de los excesivo recelos naturales al cambio tecnológico que suscitan estas tecnologías. Y de especial interés es su posición especialmente abierta a las mismas, pero siempre con garantías y, como señala, "hacia mejores algoritmos". Por mi parte sostengo, que los mejores algoritmos vendrán en buena medida predeterminados por el cumplimiento de una mejor regulación que obligue a que estos algoritmos sean admisibles. Más temor producen los sistemas biométricos de categorización, reconocimiento de emociones y evaluación de personalidad. Y, lamentablemente, éstos quedan bajo un régimen jurídico de casi total desprotección.

Hay que tener claro que estamos ante un auténtico salto cualitativo, los sistemas biométricos con IA no son un peaje más del mundo digital. De hecho, el complejo Derecho de la videovigilancia queda totalmente superado.

Hay un complejo régimen jurídico superpuesto, que parte de la miríada de derechos fundamentales en juego. No hay que olvidar que despliegan su efecto directo, que no es nada desdeñable en este tema. Téngase en cuenta, por ejemplo, la prohibición de discriminación. En todo caso, se da especialmente una vis atractiva del futuro AIA y la regulación de protección de datos, con la especialidad del régimen jurídico del ámbito policial y penal. La superposición de estos Derechos no es en modo alguno sencilla. Y peor con todas las exclusiones que se pretenden para el ámbito de seguridad y defensa nacional, y también de seguridad pública. Hoy por hoy por la vía de materias clasificadas parece que no se apliquen ni las leyes ni, lo que es peor, los derechos fundamentales con efecto directo.

Pues bien, según se ha analizado, el punto de partida de protección de datos y de IA es una teórica prohibición. Pero ésta se queda jurídicamente en que los sistemas de identificación biométrica son posibles bajo el punto de partida de la excepcionalidad. Ello se traduce –o debería– esencialmente en un canon de control más estricto tanto de la calidad de la ley reguladora, cuanto del control de su necesidad y proporcionalidad. También se ha seguido cómo la regulación superpuesta de protección de datos y el futuro AIA conlleva toda una auténtica batería de garantías, de medidas técnicas y organizativas y de transparencia antes durante y después del desarrollo de

estos sistemas y de su uso. Más allá de la normativa europea que establece las reglas del juego, según se ha expuesto queda un ámbito muy importante para el legislador nacional, que ha de actuar para legitimar y garantizar de forma concreta cada sistema de identificación biométrica. La Ley Orgánica 7/2021, de 26 de mayo es prácticamente una oportunidad perdida por cuanto no aporta casi nada respecto de la Directiva que transpone. De ahí que en principio, no vale como ley habilitante, ni como ley de calidad que regule con garantías la materia, según claramente exige el TC. Amén de las garantías desde el punto de vista de la ciudadanía, no hay que olvidar que la inacción o mala regulación del legislador está privando del uso de estas tecnologías tanto en ámbitos de seguridad en las que podrían ser muy útiles, así como en otros ámbitos públicos y privados: salud, educación, laboral, personalización de servicios públicos, marketing y un largo etcétera.

Es necesario que la actividad legislativa se acompañe de un verdadero debate social y político que acabe de definir hasta dónde estemos dispuestos a llegar en el uso de las tecnologías biométricas y de reconocimiento facial con IA. Y claro está, además de la regulación, será esencial que la normativa se cumpla y se controle efectivamente.

IX. BIBLIOGRAFÍA

Los numerosos documentos de resoluciones o informes relativos a casos particulares de instituciones, así como enlaces a recursos no propiamente bibliográficos están en las notas a pie y sus enlaces.

– AEPD, (2020): *Adecuación al RGPD de tratamientos que incorporan Inteligencia artificial. Una introducción*, https://www.aepd.es/es/media/guias/adecuacion-rgpd-ia.pdf

  - (2021): *Requisitos para Auditorías de Tratamientos que incluyan Inteligencia artificial*, https://www.aepd.es/es/media/guias/requisitos-auditorias-tratamientos-incluyan-ia.pdf

– ALBERTO GONZÁLEZ, P. (2017): "Responsabilidad proactiva en los tratamientos masivos de datos", *Dilemata*, nº 24, pp. 115-129.

– BEGAULT, L. (2019): "Automated Technologies and the Future of Fortress Europe", Amnistía Internacional, , https://www.amnesty.org/en/latest/news/2019/03/automated-technologies-and-the-future-of-fortress-europe/

– CONGRESSIONAL RESEARCH SERVICE (2020): Fe*deral Law Enforcement Use of Facial Recognition Technology*, 27 de octubre, https://crsreports.congress.gov/product/details?prodcode=R46586

– CEPD-SEPD, (2021): *Dictamen conjunto 5/2021 sobre 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).* https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_es.pdf

– CEPD (2019): *Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo*, Versión 2.0, 29 de enero, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en

- (2020): *Directrices 05/2020 sobre el consentimiento en virtud del Reglamento 2016/679,* https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf

- (2022): *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, Version 1.0, 12 mayo, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en

- (2019): *Directrices 4/2019 sobre el artículo 25 Protección de datos por diseño y por defecto*

– Consejo de Europa; ZUIDERVEEN BORGESIUS, F. (2018): *Discrimination, artificial intelligence, and algorithmic decision-making.* Directorate General of Democracy, Consejo de Europa. https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73

– Consejo de Europa (2023): "Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público", en Gamero Casado, Eduardo, (Dir.), *Inteligencia artificial y sector público: retos, límites y medios*, Tirant lo Blanch, Valencia.

- (2019): *Guidelines on Artificial intelligence and data protection*, https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b7

- (2021): *Guidelines on Facial Recognition*, https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

– COTINO HUESO, L. (2019): "Ética en el diseño para el desarrollo de una inteligencia artificial, robótica y big data confiables y su utilidad desde el derecho", *Revista Catalana de Derecho Público* nº 58 (junio 2019). http://dx.doi.org/10.2436/rcdp.i58.2019.3303

- (2020): "El alcance e interactuación del régimen jurídico de los datos personales y big data relacionado con salud y la investigación biomédica", *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada*, nº 52, pp. 57-96, nº52 enero-junio 2020.

- (2021): "Un análisis crítico constructivo de la Propuesta de Reglamento de la Unión Europea por el que se establecen normas armonizadas sobre la Inteligencia Artificial (Artificial Intelligence Act)", *Diario La Ley*, 2 de julio de 2021, Wolters Kluwer. Acceso completo en https://links.uv.es/2FK3xc4

- (2022 a): "Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal", *El Cronista del Estado Social*, IUSTEL, monográfico Inteligencia artificial, nº 100, septiembre-octubre 2022, pp. 68-79.

- (2022 b): "Nuevo paradigma en la garantías de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial", en COTINO HUESO, L. (editor), *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*,

Thompson-Reuters Aranzadi, FIADI (Federación Iberoamericana de Asociaciones de Derecho e Informática), Cizur, 2022, https://www.uv.es/cotino/publicaciones/fiadimiovfinalmaquet.pdf

- (2023 a): "Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial. Los altos estándares del Tribunal Constitucional alemán y otros tribunales, que no se cumplen ni de lejos en España", *Revista General de Derecho Administrativo*, RGDA Iustel, RGDA Iustel, nº 63.

- (2023 b): "Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público", en Gamero Casado, Eduardo, (Dir.), *Inteligencia artificial y sector público: retos, límites y medios*, Tirant lo Blanch, Valencia.

– DAVIES, B., INNES, M. y DAWSON, A. (2018): *An evaluation of South Wales Police's use of Automated Facial Recognition*, Police Science Institute Crime and Security Research Institute, Cardiff University Institute, septiembre, https://static1.squarespace.com/static/51b06364e4b02de2f57fd72e/t/5bfd4fbc21c67c2cdd692fa8/1543327693640/AFR+Report+%5BDigital%5D.pdf

– DPA (2019): *Vervolgevaluatie van de Wet biometrie vreemdelingenketen*, https://zoek.officielebekendmakingen.nl/blg-913828.pdf

– EDRI (MONTAG L. y otros), (2021): *The Rise and rise of biometrics mass surveillance in the EU, A legal analysis of biometrics mass surveillance practices in Germany, the Netherlands, and Poland*, EDRi - European Digital Rights, https://edri.org/wp-content/uploads/2021/07/EDRI_RISE_REPORT.pdf

– EIREINER, V. (2020): 'Imminent dystopia_ Media coverage of algorithmic surveillance at Berlin-Südkreuz'. https://www.researchgate.net/publication/340413439_Imminent_dystopia_Media_coverage_of_algorithmic_surveillance_at_Berlin-Sudkreuz

– ETXEBERRIA GURIDI, J. F., (2021): Inteligencia Artificial aplicada a la videovigilancia: tecnologías de reconocimiento facial, en BARONA

VILAR, S. (ed.), *Justicia algorítmica y neuroderecho: una mirada multidisciplinar*, Tirant lo Blanch, Valencia, pp. 443-467.

– FRA- Agencia de la Unión Europea para los Derechos Fundamentales, (2019): *Data quality and artificial intelligence- mitigating bias and error to protect fundamental rights*, Luxembourg, Publications Office, junio, https://fra.europa.eu/en/publication/2019/artificial-intelligence-data-quality

– FRA- Agencia de la Unión Europea para los Derechos Fundamentales, (2020): *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, Luxembourg, Publications Office https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

– GALLEGO RODRÍGUEZ, P. (2022): "Los registros biométricos y su aplicación al proceso penal desde una perspectiva constitucional", en CALAZA LÓPEZ, Sonia y LLORENTE SÁNCHEZ-ARJONA, Mercedes (dirs.), *Inteligencia artificial legal y administración de justicia*, Aranzadi, Cízur, pp. 211-255.

– GRUPO DE TRABAJO DEL ARTÍCULO 29, (2012): *Dictamen 3/2012 sobre la evolución de las tecnologías biométricas*, WP193, 27 de abril, https://www.aepd.es/sites/default/files/2019-12/wp193_es.pdf

- (2018): *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*. 3 de octubre de 2017 y revisadas el 6 de febrero de 2018, https://ec.europa.eu/newsroom/article29/items/612053

– GUTIÉRREZ DAVID, M. E. (2020): "Legitimación y principios en el tratamiento de datos personales con fines de videovigilancia privada. Especial referencia al uso de técnicas biométricas de reconocimiento facial", en BERMÚDEZ, Javier y DE MARCOS, Ana (ed.), *Transparencia, lobbies y protección de datos*, Aranzadi Thomson Reuters, Cizur Menor, págs. 411-461.

– HERNÁNDEZ PEÑA, J. C. (2022): *El marco jurídico de la inteligencia artificial. Principios, procedimientos y estructuras de gobernanza*, Aranzadi, Cízur Menor.

– IZQUIERDO CARRASCO, M., (2020): "La utilización policial de los sistemas de reconocimiento facial automático. Comentario a la sentencia del Alto Tribunal de Justicia de Inglaterra y Gales de 4 de septiembre de 2019". *Revista Ius et Veritas,* núm. 60, mayo (2020), pp. 86-103. https://doi.org/10.18800/iusetveritas.202001.004

– JOH, E. E. (2014): Policing by Numbers: Big Data and the Fourth Amendment (February 1, 2014). *89 Wash. L. Rev. 35*, https://ssrn.com/abstract=2403028

– KIND, C. (2021): *Containing the canary in the AI coalmine - the EU's efforts to regulate biometrics*, Ada Lovelace Institute. https://www.adalovelaceinstitute.org/blog/canary-ai-coalmine-eu-regulate-biometrics/

– MANTELERO, A. (2022): *Beyond Data. Human Rights, Ethical and Social Impact Assessment*, Springer, Information Technology and Law Series IT&LAW 36, 2022, https://link.springer.com/book/10.1007/978-94-6265-531-7

– MARTÍNEZ MARTÍNEZ, R. (2019): "Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo", *Revista catalana de dret públic*, nº 58, pp. 64-81.

– NAVAS NAVARRO, S. (2017): "Derecho e inteligencia artificial desde el diseño. Aproximaciones", en NAVAS NAVARRO, S. (coord.). *Inteligencia artificial: tecnología, derecho*, Tirant lo Blanch, Valencia, pp. 23-72.

– PARLAMENTO UNIÓN EUROPEA (GONZÁLEZ FUSTER, G.), (2020): *Artificial Intelligence and Law Enforcement: Impact on Fundamental Rights*, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies julio, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf

– PARLAMENTO UNIÓN EUROPEA (MADIEGA T. y MILDEBRATH, H.), (2021): *Regulating facial recognition in the EU (Deep análisis)*, EPRS- Servicio de Investigación del Parlamento Europeo, septiembre,

https://www.europarl.europa.eu/thinktank/es/document EPRS_IDA (2021)698021

– PARLAMENTO UNIÓN EUROPEA (WENDEHORST, C. y DULLER, Y.), (2021): *Biometric Recognition and Behavioural Detection*, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, agosto 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf

– PÉREZ Y MADRID, A. (2021): *El reconocimiento facial es un superpoder. Cómo te afectar y por qué deberías conocerlo*, Tecnos, https://e-archivo.uc3m.es/handle/10016/33010

– RIVERO ORTEGA, R. (2023): "Algoritmos, inteligencia artificial y policía predictiva del estado vigilante". *Revista General de Derecho Administrativo*, nº 62.

– SÁNCHEZ-MONEDERO, J. y DENCIK L. (2020): 'The Politics of Deceptive Borders: "Biomarkers of Deceit" and the Case of iBorderCtrl', *Information, Communication & Society 1*. https://doi.org/10.1080/1369118X.2020.1792530

– SANTISTEBAN GALARZA, M. (2022): "Reconocimiento facial y protección de datos: una respuesta provisional a un problema pendiente". *Revista de Derecho de la UNED* (RDUNED), (28), pp. 499–526. https://doi.org/10.5944/rduned.28.2021.32887

– SELINGER, E. y HARTZOG, W. (2020): "The Inconsentability of Facial Surveillance", *Loyola Law Review*, Vol. 66(1), https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4053&context=faculty_scholarship

– SIMÓN CASTELLANO, P. y DORADO FERRER, X. (2022): "Límites y garantías constitucionales frente a la identificación biométrica", *IDP. Revista de Internet, Derecho y Política*, 2022, n.º 35, pp. 1-13, https://doi.org/10.7238/idp.v0i35.392324.

– SEPD-Supervisor europeo de protección de datos (2019): *Directrices del SEPD para la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales,* 19 de diciembre 2019, https://edps.europa.eu/system/files/2021-12/19_12_19_edps_proportionality_guidelines_es.pdf

– SORIANO ARNANZ, A. (2021): "Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos", *Revista de Derecho Público: Teoría y Método, Vol. 3, pp. 85-127, DOI:10.37417/RPD/vol_1_2021_535*

  - (2022): "Discriminación algorítmica: garantías y protección jurídica", en COTINO HUESO, L. (coord.), Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas, Aranzadi, Cizur Menor, pp. 139-169.

– U.S. GOVERNMENT ACCOUNTABILITY OFFICE (2021): *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, https://www.gao.gov/assets/gao-21-518.pdf