Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal*

Lorenzo Cotino Hueso
Catedrático de Derecho Constitucional. Universidad de Valencia.

UNA APROXIMACIÓN A LOS SISTEMAS DE IDENTIFICACIÓN CON TECNOLOGÍAS BIOMÉTRICAS Y RECONOCIMIENTO FACIAL

El reconocimiento facial hay que abordarlo dentro de las tecnologías biométricas. En primer término hay que delimitar los sistemas dedicados a la identificación a través de tecnologías biométricas automatizadas y especialmente las que utilizan inteligencia artificial (IA).

Los datos biométricos son universales por cuanto los tienen todos los humanos, pero son singulares y únicos en cada uno. Los datos biométricos se definen como "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" (art. 3.13 Directiva (UE) 2016/680[1], art. 4.14

* Realizado en el marco de los proyectos MICINN Retos "Derechos y garantías frente a las decisiones automatizadas…" (RTI2018-097172-B-C21), proyecto "Derecho, Cambio Climático y Big Data", Universidad Católica de Colombia, "Algoritmic law" (Prometeo/2021/009, 2021-24) Generalitat Valenciana y estancia de personal investigador en empresa Generalitat Valenciana (AEST/2021/012).

[1] Directiva (UE) 2016/680, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales

Reglamento (UE) 2016/679 de protección de datos, RGPD[2] y art. 3.33 futuro Reglamento IA, en adelante AIA[3]).

Pues bien, estos sistemas de identificación biométrica generan una plantilla de nuestra cara y se compara, por ejemplo, con la de una lista de personas buscadas. Ello puede hacerse además de con los datos faciales con las huellas dactilares el ADN la estructura del Iris o la voz. Con las nuevas tecnologías biométricas se manejan también otros identificadores como las formas de andar las pulsaciones de teclas.

Estos datos personales biométricos solo se consideran bajo el régimen de los datos especialmente protegidos (art. 9 RGPD) cuando son destinados a la identificación. Y en principio, sólo cuando se trata de la identificación uno a varios (p. ej.: contrastar el patrón de mi cara con una lista de personas buscadas).

La identificación uno a uno (p. ej.: contrastar el patrón de mi cara para desbloquear mi teléfono móvil sin compartir esa información con nadie) hasta mayo de 2022 no se consideraba bajo el régimen de datos especialmente protegidos. Sin embargo, el CEPD parece que ha cambiado de opinión y habrá que ver sus consecuencias (CEPD, 2022). Como señalaba Santiesteban (2021: 511), la distinción "no se sostiene".

El uso de sistemas biométricos de identificación en el mundo democrático (EDRI, 2020; Pérez, 2021; Parlamento UE, 2021 a y b) se concentra en muchos casos en los usos vinculados a la seguridad pública. Así son conocidos los supuestos como el de Gales que captaba imágenes de la población que asistía a grandes eventos deportivos o culturales Y si contrastaban con fugados o perseguidos de la justicia. En 2019 los tribunales lo dieron por bueno.

Sistemas similares se han instalado en Alemania, como en Hamburgo en 2017 con motivo de una reunión del G20. La autoridad de protección de datos lo suspendió pero una decisión judicial anuló dicha suspensión y el tema está pendiente en los tribunales. En Berlín en 2019 se utilizado reconocimiento facial policial en una estación de tren y una veintena de ciudades alemanas reconocen el rostro en tiempo real en un proyecto de "Mercado de la ciudad segura". En 2021, un Tri-

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.

[2] 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.

[3] Propuesta de Reglamento del Parlamento Europeo y del Consejoque se establecen normas armonizadas sobre la inteligencia artificial (Ley de Inteligencia Artificial). Una visión general en Cotino 2021.

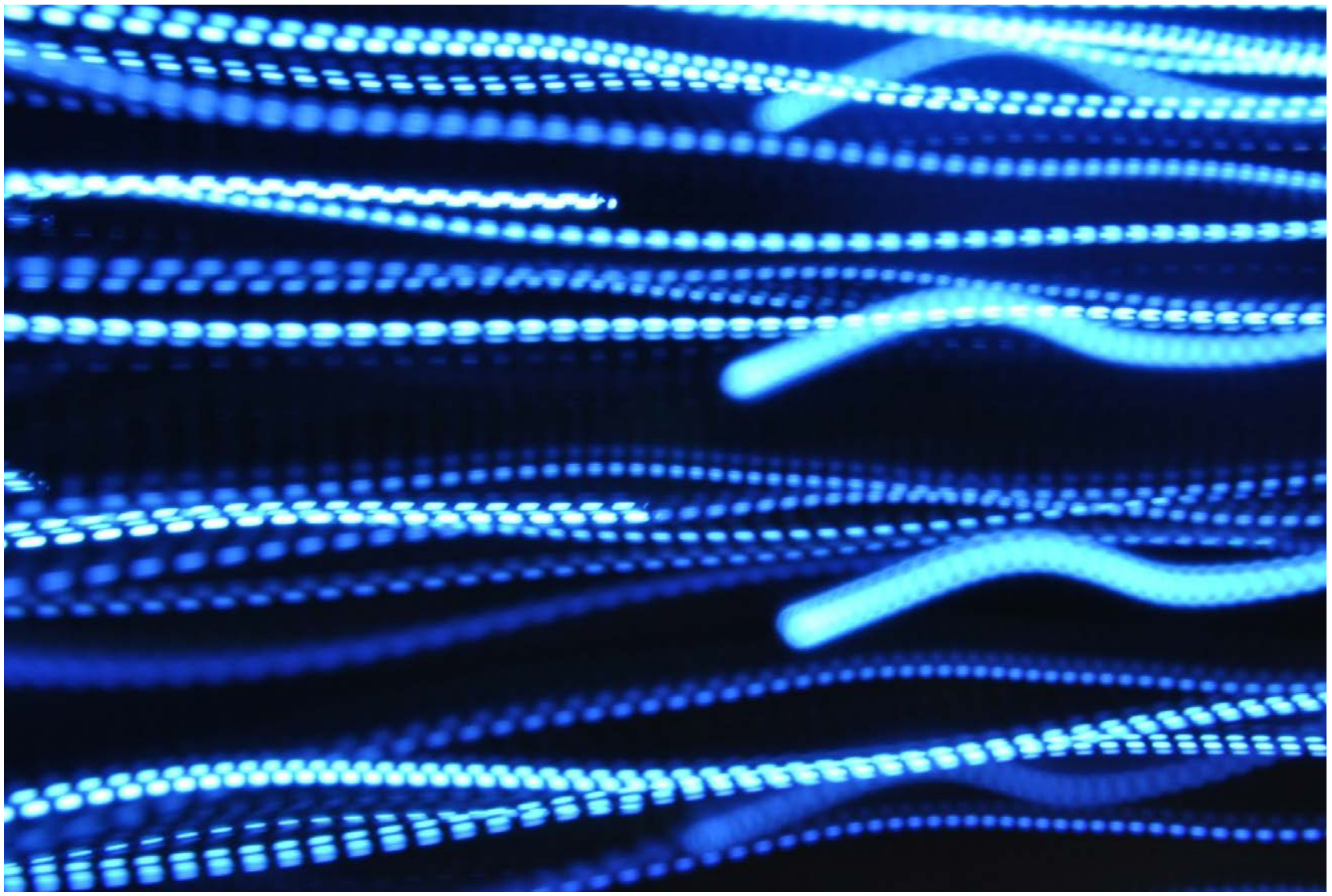


Foto de Daniel Falcão en Unsplash.

bunal detuvo su funcionamiento en Colonia. También en Países Bajos desde 2016 se utilizan estos sistemas con fuertes reticencias de la autoridad de protección de datos. El Garante italiano de la protección de datos considero inadmisible el 16 de abril de 2021 el "Sistema Automatico di Riconoscimento Immagini" SARI, utilizado desde 2019. En Buenos Aires un sistema inteligente se empezó a utilizar en 2019; 300 cámaras para identificar prófugos, que generaron 10 millones de consultas; Guillermo Federico Ibarrola fue erróneamente identificado como prófugo y estuvo detenido 6 días el 12 de abril de 2022 un juez suspendió y una sentencia de 7 de septiembre de 2022 ha anulado. La misma suerte y los mismos días que estuvo detenido Robert Williams en Detroit por otro falso positivo. La concesionaria del metro de São Paulo en Brasil es una buena aficionada al reconocimiento facial. Su sistema con fines de seguridad controlaba 4 millones de usuarios diarios y fue suspendido judicialmente el 22 de marzo de 2022.

El sector privado también parece que quiere implementar sistemas de identificación biométrica por motivos de seguridad. El uso de sistemas de reconocimiento facial por servicios de seguridad privada no fue admitido por la AEPD en 2019 (Informe 10308/2019 AEPD). El mismo año, una sentencia del Juzgado de lo Penal número 2 de San Sebastián en 2019 dio por bueno implantar estos sistemas biométricos en tiendas. En cualquier caso, el supuesto más relevante ha sido el de la mayor distribuidora en España, Mercadona, que recibió una fuerte sanción por implantar un sistema inteligente biométrico que controlaba si quienes accedían a algunos establecimientos estaban en sus listas de "personas con una orden de alejamiento o medida judicial análoga en vigor" (Resolución procedimiento sancionador PS 120/2022). El 12 de agosto de 2019 un Tribunal de Ámsterdam tampoco permitió utilizar escáneres de huellas dactilares en las cajas registradoras de una cadena de zapaterías en aquella ciudad. En el ámbito educativo se vienen utilizando polémicos sistemas biométricos para el control de asistencia de estudiantes, que han generado problemas en España, Francia o Suecia.

Es importante señalar que las nuevas tecnologías especialmente con la IA suponen un salto cualitativo, que nada tiene que ver el uso de estos sistemas con la *simple* videovigilancia pública o privada (por todos, Gutiérrez, 2020). Ahora se compara en milisegundos a las personas cuya imagen se capta con las listas de personas buscadas, o se pueden generar automatizadamente grandes cantidades de datos procesados que pueden ser utilizados para múltiples finalidades. Baste ahora indicar que la por lo general insuficiente regulación de la videovigilancia no sirve para dar cobertura legal a estos nuevos fenómenos.

Y LOS SISTEMAS BIOMÉTRICOS DE CATEGORIZACIÓN, RECONOCIMIENTO DE EMOCIONES Y EVALUACIÓN DE LA PERSONALIDAD, TANTO O MÁS PELIGROSOS

Con la nueva generación de tecnologías biométricas e IA cada vez cobran más protagonismo el uso de la lectura de datos del rostro, indicadores sanguíneos, pulsación de teclas, forma de andar, etc. Aunque también se trate de datos universales y que singularizan a la persona, cada vez más se utilizan para finalidades que no son la identificación. El futuro reglamento AIA propuesto en abril 2021 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. 3.33.º). Se ha apuntado que en la definición deben incluirse los "pensamientos", dado que ello parece posible a través de las interfaces cerebro-ordenador. Y un "sistema de categorización biométrica" se define en el futuro AIA 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 (art. 3. 35.º, Parlamento UE 2021 a).

Estos sistemas suponen contar a gran escala con la evaluación del mejor psicólogo para leer emociones, detectar la verdad de las manifestaciones, predecir futuros comportamientos (Parlamento UE, 2021 b: 12 y ss. 53 y ss.). Asimismo, permiten para categorizar y agrupar rápida, masivamente y con un grado de granularidad muy alto a conjuntos de personas con afinidades. Desde hace años se utilizan estos sistemas para el control de fronteras, como en EEUU el Agente Virtual Automatizado para la Evaluación de la Verdad en Tiempo Real (AVATAR), que analiza el comportamiento no verbal y verbal de los viajeros. Al parecer, el sistema también se ha probado en el aeropuerto de Bucarest. La Comisión Europea financió el proyecto *Intelligent Portable Control System* (*iBorderCtrl*), con herramientas de detección del engaño y de evaluación basada en el riesgo. El mismo ha generado una relativa reacción desde la sociedad civil, una iniciativa ciudadana europea y la campaña *reclaimyourface.eu*. En 2020 la AEPD rechazó el uso reconocimiento facial con tecnologías avanzadas para evitar el fraude en exámenes por universidades *online* (*e-proctoring*, Informe 0036/2020, AEPD; resolución de advertencia E/05454/2021 AEPD). 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.

Grandes empresas y plataformas disponen de sistemas de reconocimiento biométrico y facial. En junio de 2022, Microsoft ha anunciado que retira sus sistemas *Azure Face*; previamente había dejado de vender este tipo de tecnología a la policía de EEUU. Meta-Facebook dispone desde 2017 de patentes de reconocimiento de emociones. En noviembre de 2021 eliminó el polémico uso del reconocimiento facial.

Pese a que estos sistemas biométricos inteligentes ciertamente generen escalofríos, lo cierto es que el Derecho actual los regula con menos cautelas y garantías. Cuando no tienen la finalidad de identificación, los datos biométricos no son especialmente protegidos bajo el artículo 9 RGPD. Así lo ha ratificado en mayo de 2022 el CEPD (2022). Asimismo, el futuro AIA no los considera sistemas prohibidos y sólo en algunos supuestos se consideran de alto riesgo. En general el AIA sólo les impone escasas obligaciones de que los afectados estén informados de su uso (artículo 52 AIA). Las instituciones

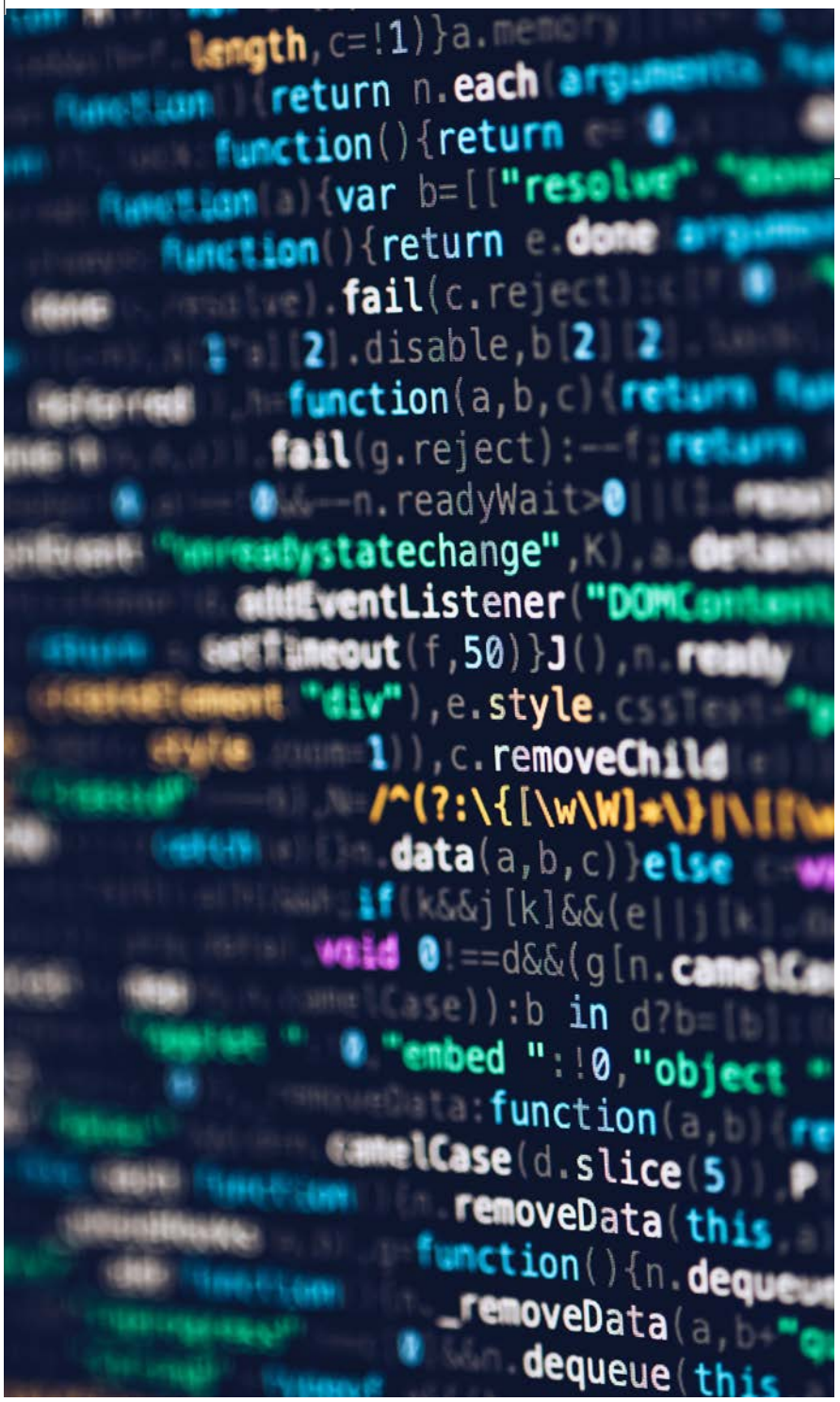


Foto de Markus Spiske en Unsplash.

y autoridades más importantes señalan el peligro que suponen sistemas biométricos inteligentes y piden su prohibición (FRA, 2000; CEPD-SEPD, 2021 n.º 35) o una regulación más estricta, similar a la de los sistemas de identificación biométrica (Parlamento UE, 2021 a: 81-82).

El lector habrá apreciado que no se ha hecho referencia a China, donde el uso actual de las tecnologías biométricas supera con mucho los sueños más húmedos de cualquier dictador. Ahí se combinan las tecnologías de identificación, categorización y reconocimiento de emociones para su famoso sistema de crédito social[4], control policial, de la lealtad al partido[5] o de seguimiento de atención y evaluación y control mental en el ámbito educativo[6]. Hay que señalar que en los Estados democráticos, los sistemas más vinculados a la defensa, inteligencia y seguridad nacional que posiblemente sean los más impactantes, por lo general nos resultan desconocidos.

[4] <https://nhglobalpartners.com/china-social-credit-system-explained/>.
[5] <https://www.telegraph.co.uk/world-news/2022/07/04/china-uses-mind-reading-ai-test-loyalty-communist-party-members/>.
[6] <https://globalvoices.org/2022/08/05/china-surveillance-tech-is-extending-from-the-classroom-to-kids-summer-holidays/>.

"SOLAMENTE" ESTÁN EN JUEGO LOS PRINCIPIOS ESENCIALES DEL ESTADO DEMOCRÁTICO, LA DIGNIDAD Y TODOS LOS DERECHOS FUNDAMENTALES

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, la Agencia de la Unión Europea para los Derechos Fundamentales (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 (entre otros, Consejo de Europa, 2021)".

No hacen falta excesivas explicaciones de por qué queda amedrentada la sociedad democrática y lo difícil que es vivir una vida digna si por el mero hecho de ir a comprar el pan es posible que controlen nuestros movimientos, identifiquen si somos una persona buscada por cualquier motivo, y capten datos para evaluar nuestro comportamiento o lo predigan. Y ello puede ser más intromisivo si lo aderezamos con el uso de estos sistemas en una manifestación, actividades políticas o sindicales, un lugar religioso, un centro de salud, de asistencia social, educativo, de menores, etc. 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 n.º 18), como también recuerda Carrasco para el caso de Gales (Carrasco, 2020).

El uso de estos sistemas pone en entredicho la presunción de inocencia al tratarnos a todos como sospechosos, al tiempo de dificultar la defensa de quienes resulten positivos por estos sistemas. Las posibilidades de generar errores, sesgos y discriminaciones son muchas, aunque sean involuntarias. Estos sistemas son probabilísticos y aplicados a miles o millones de personas los errores pueden salir muy caros a los afectados.

En cualquier caso, los derechos vinculados a la privacidad, intimidad y protección de datos quedan especialmente atraídos y afectados cuando se utilizan los sistemas biométricos. La sola captación de nuestros datos aunque se eliminen inmediatamente después de que se cotejen con una lista de búsqueda ya que es impactante. Y por supuesto la posible utilización y conservación posterior de estos datos procesados puede hacer más intensa la afectación a estos derechos. Y el riesgo de que se utilicen para finalidades inadmisibles.

El reconocimiento facial y las tecnologías suponen disparar y con fuego racheado a los derechos fundamentales. Me gustaría insistir ahora como lo he hecho con mayor profundidad en otros lugares (Cotino, 2022) en que no se trata sólo de concretas afectaciones a determinados derechos fundamentales como derechos subjetivos, que lo son. El uso de estas tecnologías impacta severamente en el ser humano y la sociedad democrática y afecta a los derechos lo es también con carácter

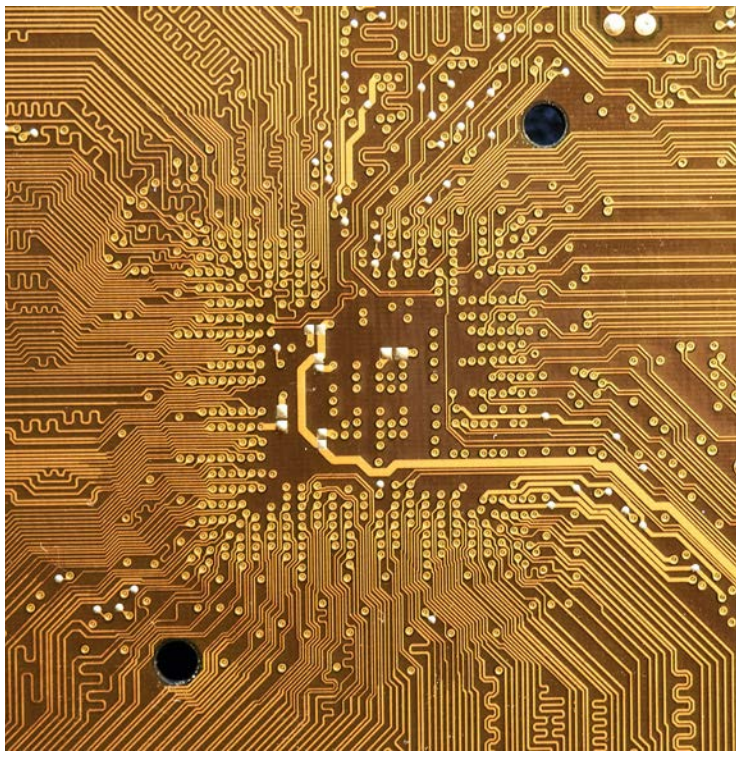


Foto de Manuel en Unsplash.

colectivo. La respuesta jurídica no puede ser –sólo– aplicar las técnicas específicas para afectaciones concretas de derechos subjetivos de individuos. Ello puede ser tan insuficiente como mirar el mundo a través de una pajita. De ahí que, entre otras cosas, se necesitan especialmente nuevas técnicas de cumplimiento normativo en el diseño y por defecto, de responsabilidad reactiva, de análisis multirriesgos no ceñidos a un derecho fundamental (como la protección de datos) o de protección colectiva de derechos.

UNA COMPLEJA RESPUESTA JURÍDICA, DE GEOMETRÍA VARIABLE Y CON UNA SUPERPOSICIÓN DE REGÍMENES NORMATIVOS

La geometría de los sistemas biométricos puede ser muy variable. Por tanto, la respuesta jurídica también ha de serlo y de poco o nada vale abordar jurídicamente el tema en términos binarios. El uso de estas técnicas puede ir desde el escaso impacto de que accedamos a nuestro móvil con nuestra huella o rostro, 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.

Las variables de quién, cómo, dónde y para qué se realiza el tratamiento son muchas y deben tenerse muy en cuenta en su tratamiento jurídico, regulación y ponderación de su admisibilidad (CEPD, 2022, n.º 16; Parlamento UE a y b, Anexo; SEPD, 2019). Así, hay que valorar en cada caso concreto la intensidad de la afección a los derechos en juego; las finalidades reales del sistema: identificación, rastreo, seguimiento, categorización, perfilado de emociones o predicción de comportamientos; el uso en contextos penales, laborales, políticos, religiosos, educativos, lugares de acceso público y otros sensibles; la duración del tratamiento y el mantenimiento de datos; la realización por sujetos públicos o privados, la menor transparencia y explicabilidad, garantías de conservación de los datos, etc.

Respecto del uso de sistemas biométricos hay una importante y compleja concurrencia y superposición de regímenes jurídicos. Como punto de partida, no hay que perder de vista el efecto directo de variados derechos fundamentales en juego a la que hay que acudir especialmente. No en vano, la regulación legal, además de que deba controlarse desde los derechos fundamentales, tiene importantes lagunas. Asimismo, hay exclusiones de aplicación de algunas normas para el ámbito de la defensa, inteligencia y seguridad nacional (como por ejemplo la del artículo 2.3.º del futuro RAI). 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) para el ámbito de rastreos masivos en el extranjero, exigiendo especialmente garantías de regulación legal en estos ámbitos.

Si descendemos a la legislación aplicable, especialmente hay que superponer la futura normativa de IA con la(s) normativa(s) de protección de datos y sus especialidades para el ámbito policial y penal, que es el habitual de los sistemas de identificación biométricos. Asimismo, concurre diversa normativa sectorial. Así pues, 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 sistemas 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 "PROHIBICIÓN" DEL FUTURO REGLAMENTO DE INTELIGENCIA ARTIFICIAL. DE UN "NO ES NO" A UN "SÍ SE PUEDE"

Teóricamente el AIA supone un sistema de semáforo. Rojo: prohíbe algunos usos de IA (art. 5). Amarillo: fija algunos usos como de "alto riesgo" (art. 6 y Anexos II y III) y éstos deben cumplir numerosas obligaciones que ocupan el grueso del reglamento. Verde: no es obligatorio cumplir la regulación del AIA. Como excepción, algunos sistemas IA, como los sistemas biométricos de reconocimiento de emociones o de categorización tienen algunas obligaciones especialmente de informar a los afectados (art. 52).

La idea de una prohibición de estos sistemas tiene pleno sentido si pensamos en los excesos en China. Y posiblemente también desplegaría sus efectos respecto del uso de estos sistemas el ámbito de la defensa y seguridad nacional, respecto de lo que el AIA no aplica. Respecto de estos casos tan aberrantes no puede haber otra respuesta que el "no es no". En algunos estados de Estados Unidos se ha acudido a la técnica de la moratoria (California) o una prohibición (San Francisco, Boston, Portland y Oregón; Pérez, 2021: 78 y ss.), al igual que se ha propuesto en Italia en 2021. Las instituciones y autoridades como el Comité europeo de protección de datos un supervisor europeo de protección de datos, así como desde la

sociedad civil europea se apuesta por una prohibición fuerte y real de muchos usos de sistemas biométricos. Y en buena medida esta sería la posición del Parlamento de la UE. Tras la propuesta del AIA en abril de 2021 y el movimiento *reclaim-yourface.eu* se marca una clara línea prohibitiva 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)).

Sin embargo, el artículo AIA regula ampliamente una "prohibición" que no lo es tal. Vamos a verlo. 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 AIA de la Presidencia de Francia y Chequia, también se incluye "en nombre" de autoridades policiales. Visto del reverso, no estarían prohibidos los reconocimientos faciales que no funcionen a partir de imágenes en tiempo real, algo que ha sido especialmente criticado (CEPD-SEPD, 2021, n.º 31; Parlamento UE, 2021). Tampoco estarían prohibidos en los lugares que no sean de acceso al público, como locales de empresas y fábricas, oficinas y lugares de trabajo, las prisiones, zonas de control fronterizo y espacios en línea (Considerando 9 AIA). Cabe recordar que, por exclusión, también quedan fuera de la prohibición las finalidades de defensa e inteligencia. Asimismo, los usos de estos sistemas en el ámbito de "migración o de asilo" parecen admitirse (art. 5.4 AIA, versión Presidencia checa 2022). Y en el contexto privado, no hay que excluir las finalidades de seguridad privada en establecimientos de acceso público (supermercados, transporte, estadios, escuelas, etc.), siempre que no se hagan "en nombre" de autoridades policiales, así como no estarían prohibidas las finalidades privadas de marketing, comercio u otras.

Todos estos sistemas de identificación biométricos quedarían fuera de la prohibición del artículo 5.

Pero, además, se trata de una falsa prohibición por cuanto los sistemas que sí que están prohibidos por el artículo 5 se pueden admitir si se cumplen particulares presupuestos y garantías que ahí se regulan. Como punto de partida, se pueden utilizar estos sistemas *prohibidos* si se da una autorización previa obligatoria y motivada por autoridad judicial o administrativa independiente. Cada Estado debe regular "normas detalladas" sobre la autorización, si bien el AIA establece requisitos y presupuestos para esta autorización. La autorización ha de ser "estrictamente necesaria" bajo presupuestos de necesidad y proporcionalidad y se regulan los fines que pueden justificar las autorizaciones, y la verdad son bastante amplios[7].

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 pasan a considerarse sistemas de alto riesgo en razón del apartado 1 del Anexo III y, como consecuencia les será aplicable nada despreciable régimen del AIA.

Por último, hay que recordar que los tan preocupantes sistemas biométricos de emociones y categorización, ni están prohibidos, ni en general son de alto riesgo, sino solo sometidos al artículo 52. Como se ha adelantado y siguiendo las autoridades más sensibles a esta materia es desear que o bien se regulen como sistemas de alto riesgo o en algunos casos directamente se prohíban. Todo ello sin perjuicio de una mejora regulatoria de estos sistemas desde la protección de datos (CEPD-SEPD, 2021; Parlamento UE, 2021)

SISTEMAS DE IDENTIFICACIÓN BIOMÉTRICA BAJO LA NORMATIVA DE PROTECCIÓN DE DATOS Y OTRAS

Procede abordar ahora cuál es el régimen jurídico de los sistemas de identificación biométrica desde la normativa de protección de datos que, como se ha dicho, se ha de superponer a la futura normativa de IA.

El tratamiento para la identificación de datos biométricos queda sometido al régimen general de protección de datos y con las singulares garantías de los datos especialmente protegidos (art. 9 RGPD), así como en su caso también las garantías de los tratamientos automatizados (art. 22 RGPD) y las concreciones de la Ley Orgánica 3/2018.

Ahora bien, el habitual uso de sistemas biométricos en el ámbito policial y penal quedará bajo la regulación especial de la Directiva 2016/680 (Considerandos 11 y 12, y Cons. 19 RGPD) y, por ende, la transposición española de la Ley Orgánica 7/2021, de 26 de mayo[8]. Los artículos 10 y 11 Directiva 2016/680 son paralelos a los artículos 9 y 22 RGPD, aunque algo menos exigentes y rigurosos.

Pues bien, desde la perspectiva de protección de datos el punto de partida del artículo 9. 1.º RGPD también es la "prohibición" del tratamiento de datos biométricos que, no obstante, "no será de aplicación" (art. 9.2.º RGPD) si se dan los requisitos excepcionales que se regulan que entre otras cosas y por lo general pasan por una regulación legal particular (Santiesteban: 513 y ss.). El artículo 10 Directiva 2016/680 exige 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 sea relativo a datos que el interesado haya hecho manifiestamente públicos. El artículo 13 Ley Orgánica 7/2021 no aporta prácticamente nada.

Respecto de los tratamientos biométricos que sean decisiones únicamente automatizadas, el artículo 11 Directiva 2016/680 exige especiales garantías en el apartado 2.º y, en particular, la intervención humana. El apartado 3.º prohíbe la elaboración

[7] 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.

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

de perfiles que conduzcan a la discriminación de personas físicas sobre la base de datos sensibles. El artículo 14 Ley Orgánica 7/2021 tampoco aporta nada al respecto. El artículo 29 y el considerando 60 Directiva 2016/680 (que, de nuevo simplemente emula la ley española) también exige en estos casos, medidas de seguridad y confidencialidad, así como control del usuario, el control del almacenamiento, el control del acceso y la integridad.

Son muy numerosas las normas de la UE que permiten recoger, almacenar y compartir datos biométricos. Sin espacio ahora para su descripción y análisis, cabe recordar ahora el Reglamento del Sistema de Entradas y Salidas, el Sistema de Información de Schengen (SIS), la Decisión Prüm o EURODAC. Ahora bien, de esta laberíntica normativa hay que subrayar que es muy difícil considerar que valga como la ley específica que por sí sola habilita, legitima y regula de manera suficiente las particulares garantías de concretos sistemas biométricos automatizados o de IA. Asimismo, además del régimen de protección de datos que pueda proceder, en muchos supuestos se aplicará también de forma superpuesta la Directiva 2002/58/CE de intimidad en el sector de las comunicaciones. También puede concurrir otra normativa sectorial en caso de plataformas, consumo, prácticas desleales, etc. En estas normas podrán sumar algunas exigencias para los sistemas biométricos, pero estas normas no se pueden considerar como normas reguladoras habilitantes.

Una vez expuesta la regulación básica de IA y de protección de datos es posible derivar resultados de esta compleja superposición y concurrencia. Ahora bien, hay que llamar la atención de que se trata de normas con lógicas muy diferentes. El futuro AIA regula obligaciones para los proveedores de servicios de IA de alto riesgo y para las empresas y administraciones que los contraten ("usuarios"). Además, el AIA ignora totalmente tanto a los interesados a quienes afecta el sistema de IA, cuanto a la normativa de protección de datos.

LA NECESIDAD DE MEJOR REGULACIÓN LEGAL Y DEBATE DEMOCRÁTICO DE CALIDAD EN ESPAÑA, QUE NO SE DA

Del análisis superpuesto de las exigencias constitucionales y legales lo primero que se deriva es la obligatoria actuación del legislador para habilitar de manera expresa cada sistema de identificación biométrica concreto. En modo alguno puede aducirse que la decisión sobre el uso de sistemas biométricos ha quedado fuera de la arena política y legislativa española.

Y además en dicha regulación se deben recoger los requisitos y garantías concretos que se consideren adecuados. Especialmente hay que cumplir con el mandato de calidad legislativa. Y hay que recordar que justo en materia de privacidad y protección de datos el TJUE y el TC han sido especialmente exigentes. Así, cabe destacar en general la STJUE (Gran Sala) de 8 de abril de 2014, Digital Rights Asuntos C-293/12 y C-594/12 (y en especial las Conclusiones de Pedro Cruz, n.º 108 y ss.) tan estrictas sobre la calidad normativa precisamente de la Directiva 2006/24 de retención de datos de comunicaciones electrónicas, siendo además que era relativa a una Directiva –siempre más genérica que el Derecho nacional que la transpone–. En el ámbito constitucional español, también el ámbito de protección de datos es el que ha suscitado las sentencias más rigurosas sobre calidad normativa. Cabe recordar inicialmente las SSTC 290/2000 (en especial, FJ 15.º) y en la STC 17/2013 (y su voto particular), pero sobre todo hay que tener en cuenta la STC 76/2019, de 22 de mayo (en especial FJ 8.º). Quien suscribe precisamente participó en el la petición al Defensor del Pueblo del recurso de inconstitucionalidad respecto de la Ley Orgánica 3/2018, que dio lugar a la sentencia más exigente en materia de calidad de la ley. La misma ha sido muy rigurosa respecto de la necesidad de que la ley limitativa del derecho de protección de datos integre en su contenido no sólo el detalle de la restricción y sus presupuestos, sino que también se han de regular las garantías concretas *compensatorias* de la restricción. Estas exigencias europeas y constitucionales se replican en la normativa y en particular con relación a los datos especialmente protegidos como los biométricos y, de ser aplicable, para los tratamientos automatizados. Así, cabe acudir a los artículos 9 RGPD y 10 Directiva 2016/680, artículo 9.2.º Ley Orgánica 3/2018, artículo 22. 2b RGPD y 11 Directiva 2016/680 para decisiones automatizadas y, en general, las fuertes exigencias para los límites a los derechos

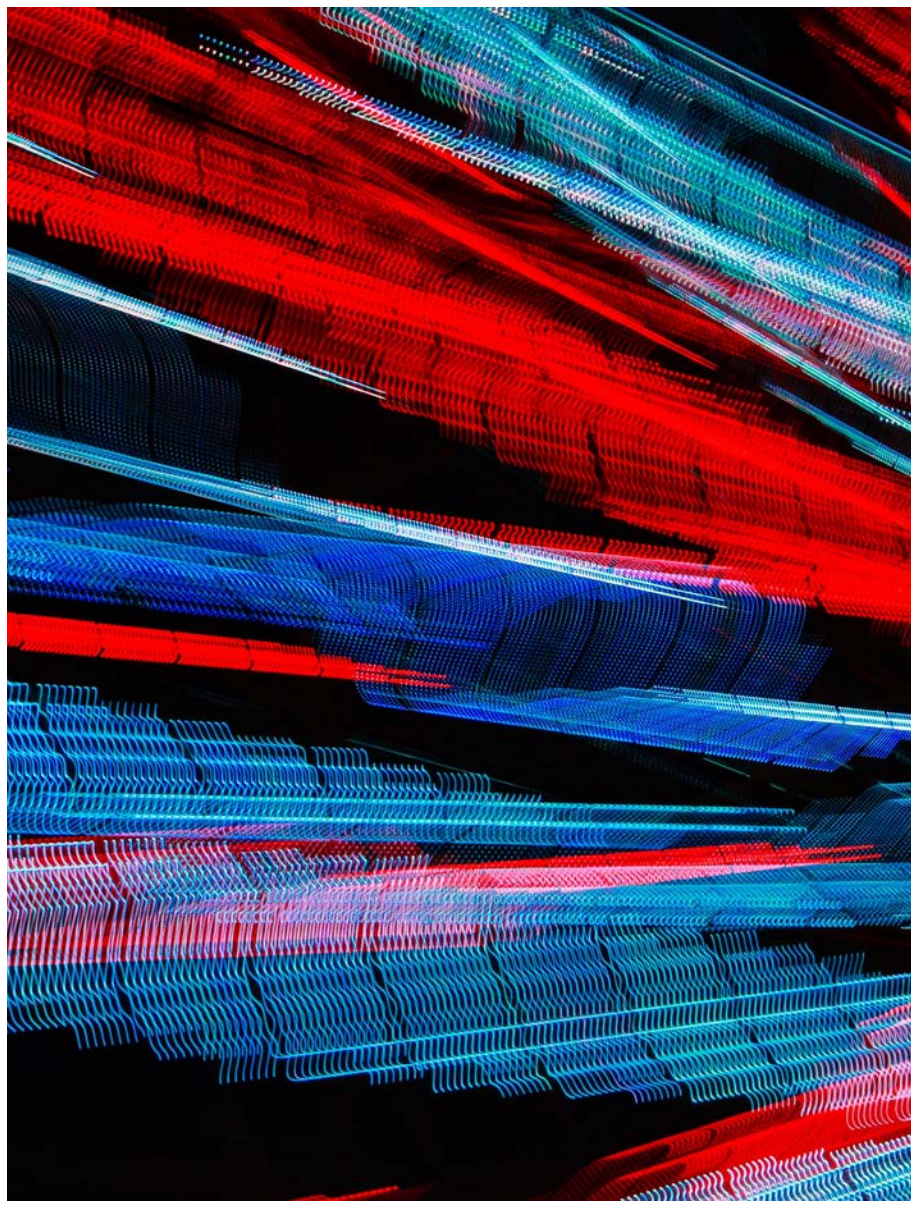
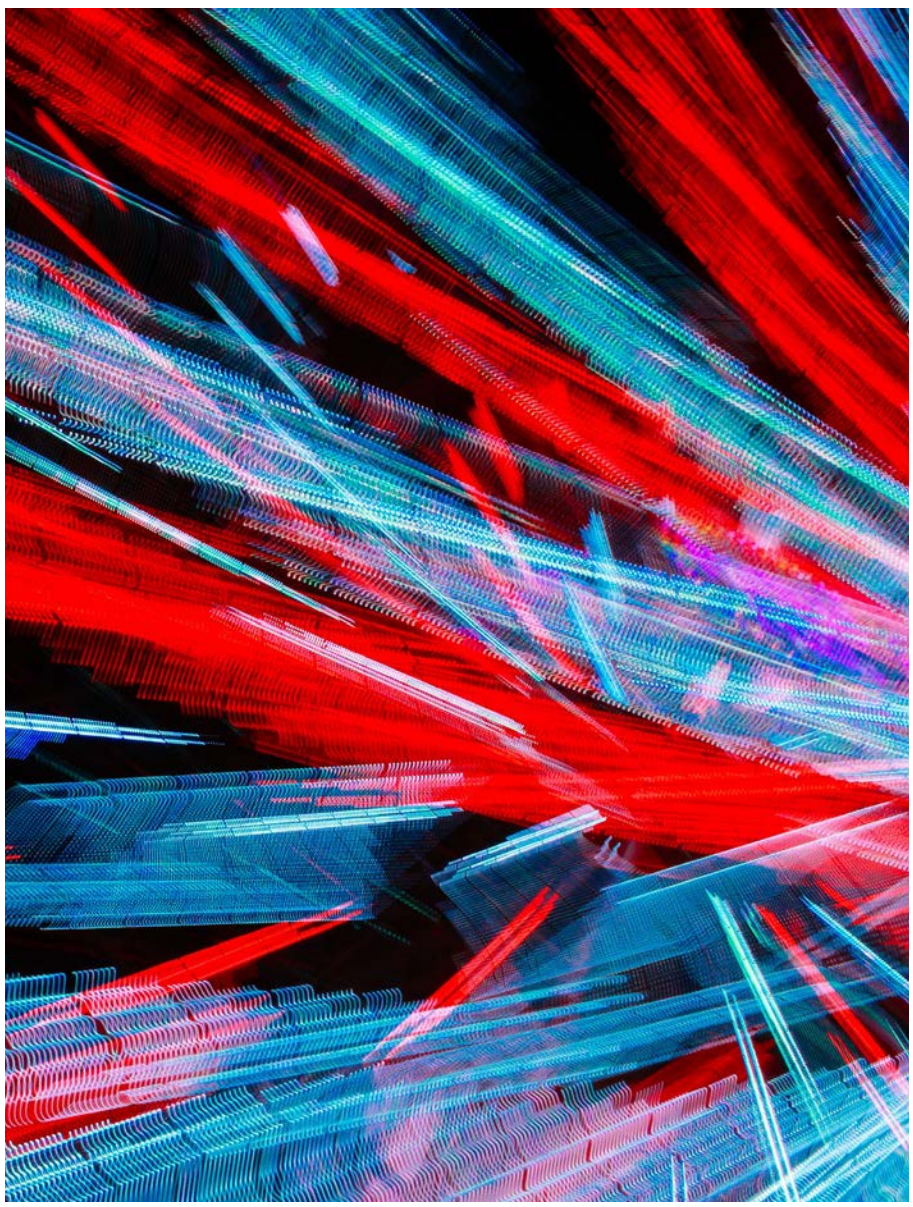


Foto de Fabio Ballasina en Unsplash.

del artículo 23 RGPD. El futuro AIA aún añade más garantías de "normas detalladas" (art. 5.3.º y 4.º; también, artículo 5.1.d.iii AIA).

Pues bien, la Ley Orgánica 7/2021, de 26 de mayo como se ha señalado, prácticamente es un *corta y pega* de la Directiva. Y esto es lo que precisamente el CEPD ha recordado en mayo de 2022 que es lo que no se debe hacer y añade que si la ley nacional es una mera reiteración del artículo 10 Directiva 2016/680, no puede ser invocada como una ley que autoriza el tratamiento de datos biométricos (CEPD, 2022, n.º 71). Ello es así pese a las dudas de algunos autores sobre si la esta ley orgánica ya da cobertura a los tratamientos biométricos específicos (Carrasco, 2020). Yo no lo considero y es exigible y no sólo "deseable" (Santiesteban, 2021: 526; 515).

Cualquiera podría pensar que, precisamente, el futuro AIA que regula los sistemas de identificación biométricos que no están prohibidos, o en su caso los requisitos para que sean autorizados es precisamente la regulación legal que reúne los requisitos. Pues no. Precisamente las autoridades europeas han expresado claramente que el AIA en modo alguno es la base legal que se requiere por normativa de la protección de datos (CEPD-SEPD, 2021, n.º 31; Parlamento UE, 2021). El futuro AIA regula algunos sistemas de IA como de alto riesgo, sin que ello signifique que pasen a considerarse legales. En este sentido no pocos de los sistemas de alto riesgo del anexo III hoy por hoy son contrarios a las leyes vigentes. Ello debería quedar aún más claro en el futuro AIA, aunque puede deducirse del Considerando 24. Como he adelantado, el futuro AIA y el RGPD se ignoran. De igual modo, cabe apuntar que la regulación de la *antigua* videovigilancia no sirve para dar cobertura legal a las nuevas tecnologías biométricas. Son fenómenos distintos.



Así las cosas, hoy por hoy existe un marco legal combinado esencialmente europeo que da cierta cobertura general a la posibilidad de los sistemas biométricos. Pero este marco legal impone y remite a la existencia de leyes (nacionales o europeas) que en su caso los regulen y con garantías de forma concreta. Y hoy por hoy no existen tales leyes concretas para desarrollar e implantar sistemas biométricos con IA. Esta carencia la ha con claridad la AEPD respecto del reconocimiento facial de seguridad privada (Informe 010308/2019 AEPD), los sistemas biométricos de control de exámenes (Informe 0036/2020 AEPD) o en el caso Mercadona (procedimiento sancionador PS 120/2022 AEPD). En otros países no parecen estar mejor. La carencia de base legal también ha sido acusada por la autoridad de protección de datos de Hamburgo en el caso del G20 de 2017; por el Garante italiano respecto del "Sistema Automatico di Riconoscimento Immagini S.A.R.I." o la autoridad neerlandesa respecto de los sistemas biométricos ahí desplegados.

Así pues, para en su caso admitir estas tecnologías tan impactantes en los derechos es necesario que el legislador haga bien sus deberes. Las exigencias de calidad normativa no son un mero requisito formal. Como se ha señalado, los sistemas biométricos pueden ser muy variables y requieren de una fina labor del legislador para cada supuesto y uso concreto.

Y, obviamente, no se necesita sólo una regulación técnicamente buena, sino que previamente debe darse una ponderación de la necesidad, justificación objetiva y razonable de la proporcionalidad del uso del sistema de identificación biométrico y que se *compense* con todas las garantías que sean precisas. Toda la regulación ha de partir bajo la clara premisa de que sólo se pueden admitir estos sistemas cuando sean "estrictamente necesarios" (art. 5 AIA), bajo un canon de control muy estricto y de que "el listón de la necesidad y la proporcionalidad es más alto cuanto más profunda es la injerencia" (CEPD, 2022: 15, 19, 46; SEPD, 2019). Bajo el RGPD en muchos casos se necesitará un "interés público *esencial*" (artículo 9. 2.º g) que pueda justificar el tratamiento biométrico. Como ha recordado la STC 76/2019 en modo alguno vale cualquier finalidad ni interés público. La falta de justificación y proporcionalidad ha sido también el motivo para considerar inadmisibles casos comentados en el párrafo anterior, así como en Francia respecto del sistema biométrico de control de acceso de escuelas en Marsella. Así lo han considerado tanto la autoridad francesa (la CNIL, el 29 de octubre de 2019) o un tribunal el de 27 de febrero de 2020.

Pero además de las exigencias propiamente jurídico constitucionales, la tarea legislativa debe venir acompañada de un debate social y político democrático real, dada la importancia

capital del tema. Vamos, todo lo contrario del mal ejemplo de la Ley Orgánica 7/2021. En vez de reiterar la Directiva, esta ley bien podría haber establecido un marco de requisitos y garantías más concretos según categorías o usos al cual remitirse la habilitación legal concreta. Este marco satisfaría las exigencias constitucionales y europeas y al mismo tiempo evitaría la necesidad de una labor legislativa concreta para la implantación de un sistema de identificación biométrica. De este modo, la ley concreta que deba habilitar el sistema a implantar en buena medida sólo habría de remitirse al concreto régimen correspondiente con menores adecuaciones.

LOS LÍMITES DEL CONSENTIMIENTO PARA LEGITIMAR LOS SISTEMAS DE BIOMÉTRICOS Y SU USO POR EL SECTOR PRIVADO

La legislación de protección de datos abre la puerta a que el consentimiento puede legitimar el tratamiento de datos biométricos especialmente protegidos (artículo 9.2.º a RGPD; CEPD, 2020: 20 y ss.; de interés, Santiesteban, 2021: 516 y ss.). El consentimiento ha sido el gran enemigo de la protección de datos puesto que todos hemos *vendido el alma al diablo* con tal de vivir en esta sociedad tecnológica. Es por ello que sus limitaciones son muchas. Para el uso de sistemas biométricos por el sector público el consentimiento solo es admisible excepcionalmente (175/2018 AEPD) y, en todo caso, debe partirse del principio de legalidad. 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).

Señala Simó (2022: 7) que es "aberrante" afirmar que las empresas privadas pueden justificar uso de sistemas de identificación biométricos con fines de la seguridad y por motivos de interés público. No obstante, si bien, como señala la AEPD estos tratamientos biométricos pueden estar justificados –y con regulación legal– en sectores muy particulares, como las infraestructuras críticas. Aunque sea bien difícil, no hay que excluir radicalmente que el legislador considere que sí que hay un interés público esencial que pueda legitimar específicamente estos tratamientos de datos, incluso en manos de la seguridad privada (Gutiérrez, 2020, apartado 2). El Parlamento UE en 2021 ha pedido que se "prohíba el uso de las bases de datos de reconocimiento facial privadas" (n.º 28)[9]. Los tribunales y las autoridades han sido reacios a los sistemas de identificación biométricos privados por motivos de seguridad, como por ejemplo respecto de una casa de alquiler de coches (Informe 0283/2013 AEPD) y especialmente en el ya referido caso Mercadona. En Países Bajos tampoco se admitió que una zapatería los utilizase y, por doble partida, en el caso del Metro de Sao Paolo no se ha admitido ni para seguridad ni para finalidades de marketing personalizado.

En todo caso, la ley también debería aclarar algunos supuestos en los que no cabe el uso de sistemas biométricos en contextos privados, incluso aunque se cuente con el consentimiento, como especialmente determinados usos del reconocimiento de emociones, categorización y comportamientos.

Incluso en los supuestos en los que el consentimiento sí que legitima el tratamiento de datos biométricos, no puede olvidarse que pasa a ser nulo si hay un tratamiento desproporcionado (art. 7. 4.º RGPD). En este sentido fácilmente puede considerarse desproporcionado que una plataforma o red social adivine en nuestros pensamientos y emociones por el mero hecho de haber clicado la política de privacidad. La STC 27/2020, de 24 de febrero de 2020 ha sido bastante restrictiva sobre el valor del consentimiento en las redes sociales. En un sentido similar, el CEPD (2022, n.º 75: 19) ha sido bien restrictivo para admitir un tratamiento de identificación biométrica por tratarse de datos manifiestamente públicos. Subraya el CEPD que en ningún caso se legitima por esta vía por el hecho de que las imágenes que alimentan el sistema biométrico estén disponibles en fuentes abiertas.

Debe señalarse que las grandes tecnológicas y plataformas parece que están dando un paso atrás, al menos públicamente. En junio de 2022, Microsoft ha anunciado que retira sus sistemas de reconocimiento facial *Azure Face*; previamente había dejado de vender este tipo de tecnología a la policía de EEUU. Meta-Facebook dispone desde 2017 de patentes de reconocimiento de emociones. En noviembre de 2021 eliminó su polémico uso del reconocimiento facial.

DE PERMITIRSE UN SISTEMA BIOMÉTRICO, HABRÍA DE CUMPLIR CON TODO UN ARSENAL DE MEDIDAS, GARANTÍAS Y TRANSPARENCIA BAJO EL PARADIGMA DEL "MÁS VALE PREVENIR QUE CURAR"

En el caso de que se opte por adoptar concretos sistemas de identificación biométricos, además de la obligatoria regulación legal y legitimación de los mismos, de su necesidad y proporcionalidad, habrá que cumplirse toda una batería de garantías y exigencias de estudios de impacto, responsabilidad activa y en el diseño.

Una viga maestra de la regulación europea de datos es la privacidad en el diseño y por defecto. Precisamente el lema de la marca europea de la IA es la "ética en el diseño" y el futuro AIA es su paradigma (Cotino, 2019). Como he tenido ocasión de explicar (Cotino, 2022) 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). Una buena expresión de ello es la reciente Carta de Derechos Digitales, XVIII. 4.º cuando afirma 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". Es más, estas técnicas de garantía deben involucrar a la sociedad civil e incluir fórmulas participativas.

[9] Resolución del Parlamento Europeo, de 6 de octubre de 2021, n.º 28.

La superposición del futuro AIA y la actual normativa de protección de datos implica una larga retahíla de medidas técnicas organizativas y de garantía a aplicar respecto de estos sistemas biométricos tan impactantes. Por cuanto al futuro AIA, en tanto en cuanto el sistema de identificación biométrico será de alto riesgo (Anexo I.1.º), pasa a tener que cumplir todo el grueso de la regulación: evaluación y mitigación de riesgos (art. 9 AIA), 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), el diseño de la IA para que genere registros y logs de funcionamiento (art. 12), siendo las exigencias exhaustivas para el reconocimiento facial (art. 12.2). Las obligaciones de supervisión humana (art. 14.5.º) incluyen también el "plus" de la identificación resultante ha de ser verificada y confirmada por al menos dos personas físicas antes de que se tomen decisiones por el usuario del sistema. Los sistemas de reconocimiento han de estar diseñados con un nivel adecuado de precisión, solidez y ciberseguridad (art. 15). Asimismo, se siguen estrictos procedimientos de evaluación de la conformidad ex ante y no a través de la autoevaluación como regla general (art. 43.1.º; art. 19). Después los sistemas de IA se someten al sistema de vigilancia del mercado y de supervisión, también con reglas especiales en el ámbito policial (art. 63.1). Todas estas exigencias 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.

Y todas estas garantías que impondrá el AIA a los sistemas de identificación biométricos se superponen a las muchas exigidas por la normativa de protección de datos. No es posible entrar en detalle ahora, cabe recordar la obligatoriedad del estudio de impacto (art. 27 Directiva 2016/680, art. 35 RGPD), que en la medida de lo posible habrá de ser público CEPD (2022); el registro de actividades (art. 25 Directiva 2016/680), análisis de riesgos, obligaciones de seudonimización, anonimización, gestión de la calidad de los datos, documentación de violaciones, medidas de seguridad adecuadas, la necesidad de compartimentar y cifrar datos y plantillas biométricas, etc. Estas garantías son generalmente aplicables y en el caso de sistemas biométricos deben exigirse con especial intensidad. Las autoridades de datos también consideran que antes de desplegar los sistemas biométricos habrá de darse la consulta previa a la autoridad de control (art. 28 Directiva 2016/680; CEPD, 2022, n.º 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) y ahora del CEPD.

Esta batería de medidas exigidas por la normativa actual de datos y el futuro AIA incluye también fuertes obligaciones de transparencia e información sobre el sistema de identificación biométrico empleado (arts. 13 y 14 Directiva 2016/680, arts. 12 y ss. RGPD). Entre otras cosas se ha de informar de la base legal del tratamiento, origen de los datos, conservación de los datos, cesiones y posibilidad de ejercicio de derechos. En el ámbito policial y criminal lo normal será establecer excepciones y restricciones de la transparencia del sistema biométrico, pero habrán de concretarse y justificarse por ley y con los requisitos que marca el artículo 13.3.º y 15 Directiva 2016/680 o el 23 RGPD. Además, el CEPD (2022, n.º 85 y ss.: 22-23) ha fijado que aunque se regulen excepciones en todo caso debe informarse de que hay un sistema biométrico, su finalidad, contacto del responsable, derecho a presentar una reclamación, si se toman de decisiones únicamente sobre la base del sistema, etc.

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. El TC ha sido muy claro en este sentido. No obstante, 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.

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: 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 (en especial CEPD, Anexo II: 29-35).

PARA CONCLUIR

Conforme uno conoce más sobre los sistemas biométricos y de reconocimiento facial encuentra muchos más motivos para alarmarse y preocuparse por su uso en nuestras sociedades democráticas. Prácticamente no queda ni un solo principio o derecho constitucional que no esté en peligro por los sistemas biométricos. Y no se trata del temor a que se adopten estos sistemas en su versión más peligrosa y totalitaria como la que ya hoy día se da en China. Tampoco es un temor conspiranoico a que los sistemas más intromisivos ya se estén utilizando en el ámbito de la defensa, seguridad nacional e inteligencia. Basta saber de los sistemas que ya existen y ya se han puesto en funcionamiento en el ámbito de la identificación biométrica en los países democráticos. De hecho, más temor producen

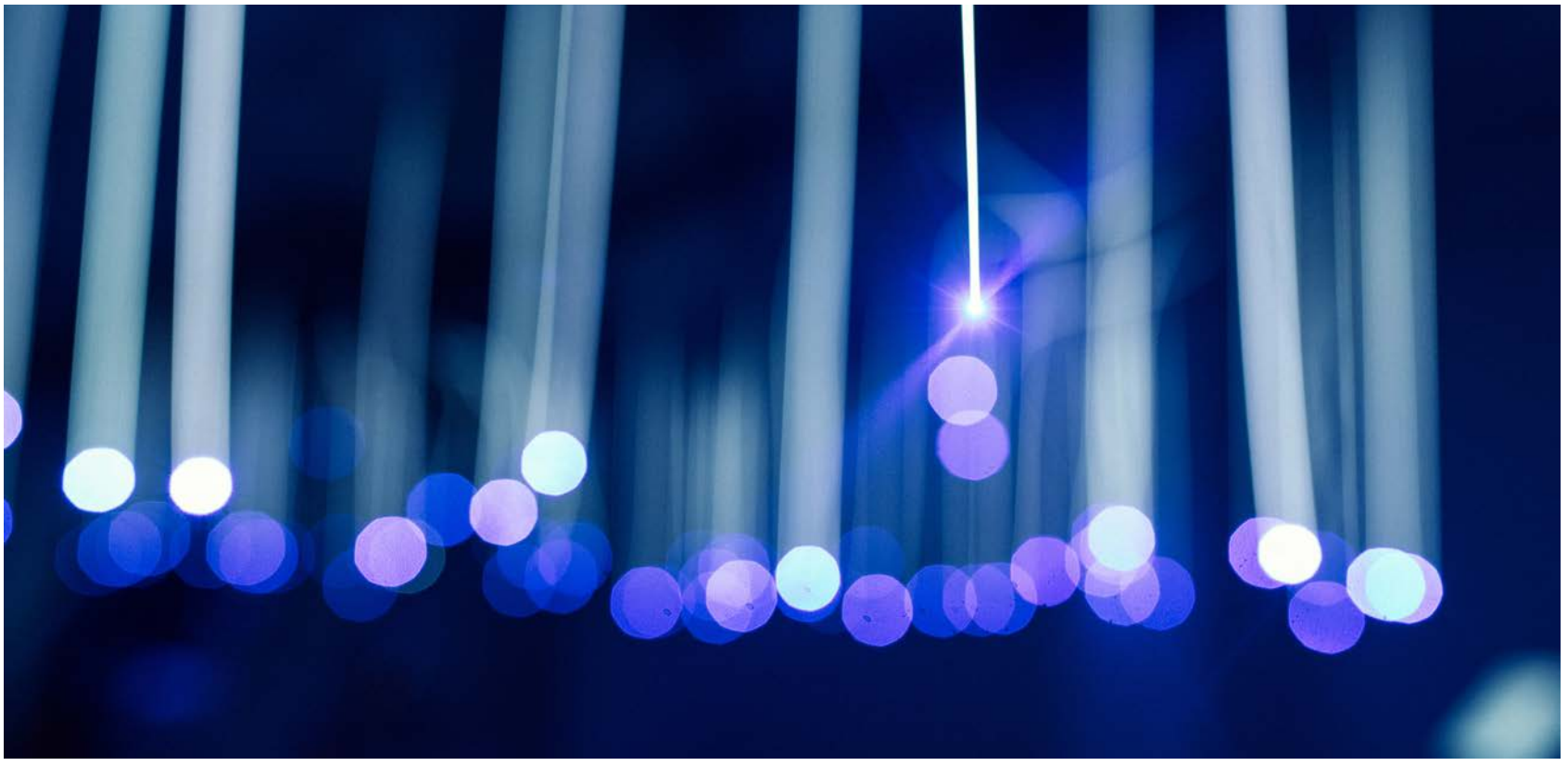


Foto de McDobbie Hu en Unsplash.

los sistemas biométricos de categorización, reconocimiento de emociones y evaluación de personalidad que ya desarrollan las tecnológicas y plataformas y que, literalmente ya leen y predicen nuestros pensamientos y nos clasifican a partir de los datos que gentil les facilitamos. Curiosamente estos sistemas que no son de identificación quedan bajo un régimen jurídico de casi total desprotección.

La sociedad no parece consciente de que éste no es un *peaje más* del mundo digital, a pagar para disfrutar y seguir *zombificados* o abducidos con las dichosas redes y plataformas. Tampoco se trata una cesión más de nuestra libertad a favor de la seguridad. Se trata de un auténtico salto cualitativo.

Ahora bien, de poco o nada sirve hablar en términos maximalistas o binarios de la prohibición o no de estos sistemas. Es tanta la variedad que puede darse respecto de quiénes, cómo, dónde, cuándo o para qué utilicen estos sistemas biométricos o de reconocimiento facial que es necesario utilizar todos los instrumentos y herramientas que nos brinda el Derecho para dar un tratamiento fino y adecuado a esta materia. Y el tratamiento jurídico en modo alguno es sencillo. La miríada de derechos fundamentales en juego despliega su efecto directo, que no es nada desdeñable en este tema. En todo caso, se da especialmente una *vis atractiva* de dos regímenes jurídicos. El 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 especialmente en estas páginas se ha intentado su análisis conjunto.

Como se ha visto, la prohibición es el punto de partida de estas normativas. Pero está muy lejos de ser una regla. Es muy difícil hoy día afirmar que un sistema biométrico está prohibido totalmente. La prohibición es bastante limitada y admite expresamente excepciones. Así, la teórica prohibición se queda jurídicamente en que los sistemas de identificación biométrica son posibles bajo el punto de partida de la excepcionalidad. Ello se traduce esencialmente en un canon de control más estricto tanto de la calidad de la ley reguladora, cuanto del control de su necesidad y proporcionalidad. Dejando al margen esta prohibición que no lo es, 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. Y es en el cumplimiento de todas estas exigencias donde hay que poner el foco.

La legislación europea establece el marco y las bases de la regulación, el campo de juego. De hecho habrá que ver cómo queda finalmente la regulación del futuro AIA con los miles de enmiendas y con el papel más garantista que ha de jugar finalmente el Parlamento UE. Y precisamente el reconocimiento facial se ha convertido en un estandarte y centro de atención. Pero más allá de la normativa europea, según se ha expuesto, queda un ámbito muy importante al legislador que ha de actuar para legitimar y garantizar de forma concreta cada sistema de identificación biométrica. Y esencialmente este legislador es el nacional. Hasta la fecha el legislador español no ha aportado prácticamente nada al respecto con la Ley Orgánica 7/2021, de 26 de mayo. Ni otras leyes. No contamos con una ley habilitante y con las garantías respecto de un sistema de identificación biométrico concreto, ni para el sector público ni para el sector privado. En el sector privado, las posibilidades del consentimiento se han analizado, pero en muchos casos no son suficientes. Esta situación no solo es negativa para las garantías de los ciudadanos para el caso de que estén funcionando sistemas de identificación biométricos inteligentes. 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.

Necesitamos que la labor legislativa no sólo sea de la calidad *técnica* obligatoria, sino también de calidad *política y democrática*. 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. Se debe hacer una labor pedagógica de los peligros, pero también de las ventajas que los sistemas biométricos pueden suponer y las garantías con las que se pueden configurar. Hay que evitar en lo posible que los pasos legislativos especialmente en el terreno de seguridad se den al calor de atentados islamistas o de otro tipo. Si no, más que pasos se tratará de cesiones que muy posiblemente no cumplirán con todos los estándares y exigencias constitucionales y del Derecho europeo para la implantación de los temidos sistemas biométricos y de reconocimiento facial. Y claro está, además de regular más y mejor, será esencial que la normativa se cumpla y se controle efectivamente. ❖

BIBLIOGRAFÍA CITADA Y DE REFERENCIA EN LA MATERIA

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

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

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>.

CEPD (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>.

CEPD,(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>.

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

Consejo de Europa (2021): *Guidelines on Facial Recognition*, 2021, <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", en *Revista Catalana de Derecho Público* n.º 58 (junio 2019). <http://dx.doi.org/10.2436/rcdp.i58.2019.3303>.

— Y otros, (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)", en *Diario La Ley*, 2 de julio de 2021, Wolters Kluwer. Acceso completo en <https://links.uv.es/2FK3xc4>.

— (2022): "Nuevo paradigma en las garantías de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial", en COTINO HUESO, Lorenzo (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>.

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>

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, 2021, 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>.

— (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>.

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.ª 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, J. y De Marcos, A. (ed.), *Transparencia, lobbies y protección de datos*, Aranzadi Thomson Reuters, Cizur Menor, 2020, pp. 411-461.

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>.

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>.

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, Ch. 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>.

Santistéban 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>.

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>.