La expansión del uso estatal de las tecnologías biométricas: una mirada crítica

Júlia García-Puig*

RESUMEN

Mientras que los defensores de las tecnologías biométricas alaban sus beneficios para la identificación, la seguridad nacional y la provisión de servicios públicos, las voces más críticas alertan sobre sus riesgos para la privacidad y las libertades civiles. El creciente uso de estas herramientas por parte de los gobiernos e instituciones públicas genera un debate controvertido, anclado especialmente en el carácter altamente sensible de la información biométrica. ¿Qué abarcan exactamente estas tecnologías? ¿Qué datos generan y qué riesgos plantean para nuestras sociedades? Este artículo examina estas cuestiones clave para seguir avanzando el debate acerca de la implementación y el control de los sistemas biométricos.

1. Introducción

Este artículo pone el foco en las cada vez más controvertidas tecnologías biométricas, que se basan en el uso de sistemas automatizados que miden características biológicas o de comportamiento para identificar, monitorear y controlar individuos y poblaciones (Marciano, 2019). Mientras que este tipo de tecnologías se utilizaban hasta hace poco mayormente para fines militares, de seguridad nacional y de investigación criminal, su uso en los últimos años se ha ido extendiendo y adentrando en nuestro día a día. Los gobiernos confían cada vez más en las cámaras de videovigilancia, el reconocimiento facial y los lectores de huellas dactilares, entre otros, para identificar a sus ciudadanos cuando cruzan las fronteras o para darles acceso a servicios públicos.

Sin embargo, al igual que prácticamente cualquier avance tecnológico a lo largo de la historia, las tecnologías biométricas son un arma de doble filo. Si bien pueden ser usadas para prevenir un ataque terrorista, la misma tecnología también puede ser empleada para restringir libertades civilies y ejercer un control opresivo de los ciudadanos. En los últimos años hemos sido testigos de los efectos críticos de tal expansión. Incluso cuando el objetivo es legítimo *a priori,* su uso puede desencadenar consecuencias indirectas no deseadas. Por ejemplo, los sistemas biométricos han demostrado ser útiles para las principales organizaciones humanitarias a la hora de identificar a los individuos desplazados que frecuentemente no llevan consigo documentos identificativos. Sin embargo, en 2021, se acusó a la Agencia de Naciones Unidas para los Refugiados de mala praxis por compartir la información de refugiados rohinyás con

* Universidad de Leiden (j.garcia.puig@fgga.leidenuniv.nl).

el Gobierno de Bangladesh, país que acoge a la mayoría de estos refugiados que escapan de Myanmar perseguidos por motivos étnicos y religiosos. Este hecho suscitó una ola de críticas, tanto por parte de los refugiados como de defensores de los derechos humanos, por temor a que esa información pudiera ser utilizada para forzar el retorno de refugiados si el Gobierno de Bangladesh compartía los datos con el Gobierno de Myanmar. Así pues, aunque esta práctica perseguía el objetivo de mejorar la provisión de ayuda humanitaria entre los refugiados, se derivaron importantes riesgos para su seguridad, tratándose ya de un colectivo en una posición extremadamente vulnerable[1].

En otros casos, el uso indebido de las tecnologías biométricas es deliberado y motivado por el objetivo de reforzar sistemas de control de los ciudadanos inaceptables desde la perspectiva de los Estados de derecho y las democracias. Además, la rápida expansión internacional de este tipo de tecnologías tiene lugar en medio de una insuficiente regulación –incluso inexistente en muchos países– y un desconocimiento extendido acerca de sus riesgos inmediatos y futuros.

La recolección de datos biométricos a gran escala plantea importantes cuestiones políticas, éticas y legales acerca de su tratamiento y su protección. En principio, la recogida sistemática de datos personales por parte de los gobiernos no es nada nuevo ni negativo por sí misma. Es, de hecho, necesaria: la habilidad de un Estado para gobernar eficazmente está estrechamente ligada a su capacidad de "legibilidad", entendiéndose como el conocimiento que tienen de los ciudadanos y sus actividades (Lee y Zhang, 2016). Históricamente, los Estados han recogido una amplia variedad de información sobre sus ciudadanos con múltiples finalidades, a través, por ejemplo, de censos de población, registros de nacimiento, matrimonio, defunción, así como de formularios fiscales y registros de propiedad. Pero las nuevas tecnologías expanden significativamente las habilidades para recopilar cantidades de información detallada de forma automatizada y continua sobre aspectos más cotidianos y rutinarios del día a día de las personas.

La mayor preocupación reside en el carácter particularmente sensible de la información biométrica, que tiende a ser única, inherente e identificativa de cada individuo, y muchas veces invariable. El uso generalizado de estas tecnologías es objeto de gran debate debido a que puede deteriorar derechos fundamentales a nivel individual y colectivo, incluyendo el derecho de no-discriminación, libertad de expresión, información y comunicación, libertad de reunión y asociación, entre otros (Kindt, 2018: 524). Algunas prácticas, como el escaneado facial indiscriminado o la elaboración de perfiles de personas, se consideran contrarias al derecho internacional de los derechos humanos (Bacciarelli, 2023). Los debates sobre el uso y limitación de la biometría tienen una posición central en las agendas políticas nacionales y supranacionales, siendo la Unión Europea (UE) pionera en cuanto a su regulación.

El objetivo del presente artículo es examinar el creciente uso de las tecnologías biométricas en el sector público y los riesgos que plantean a nivel social. En el siguiente apartado expongo las principales funciones de estas tecnologías en el ámbito público, y especifico la tipología de datos biométricos. En el tercer apartado se analizan los crecientes riesgos a los que nos enfrentamos como sociedad. En el cuarto se enfoca la atención en los recientes avances regulatorios de la Unión Europea, cerrando el texto con unas conclusiones y observaciones finales.

2. El auge de las tecnologías biométricas en el sector público

2.1. Usos y aplicaciones

Los ataques del 11 de septiembre de 2001 en Estados Unidos, y la consiguiente guerra al terror, trajeron consigo la intensificación de los sistemas de identificación en virtud de la seguridad nacional (Lyon, 2008). Ese momento de excepción y elevada sensación de inseguridad favoreció que la expansión de tales tecnologías contara con altos niveles de aceptación ciudadana. Pero desde entonces, la creciente aplicación de tecnologías biométricas en tareas

[1] Para más información ver el informe publicado por Human Rights Watch (2021, June 15).

cada vez más cotidianas, como la identificación de civiles, ha ido generando crecientes críticas.

El rápido avance de las tecnologías biométricas permite anticipar el incremento de la cantidad de nuestros datos biométricos en posesión de las instituciones estatales. Actualmente, los Estados utilizan las tecnologías biométricas con tres finalidades principales. La primera es la verificación de la identidad, es decir, la confirmación o la negación de la identidad que la persona en cuestión afirma ostentar (¿es esta persona realmente quién afirma ser?). La segunda funcionalidad, más compleja, consiste en identificar a alguien (¿quién es esta persona?). La tercera finalidad es la de comprobar, sobre la base de una identidad ya establecida, determinadas cualidades o comportamientos, por ejemplo, si una persona tiene antecedentes penales o es sospechosa de terrorismo (Hu, 2017: 171).

El uso de los datos biométricos es especialmente prevalente en tres ámbitos. Uno de ellos es en los sistemas de identificación nacional. Cada vez son más los países que incorporan microchips con imágenes faciales digitalizadas, el iris y/o las huellas dactilares en sus documentos de identidad nacional y pasaportes. En el caso de España, el pasaporte biométrico incluye la fotografía digitalizada y las huellas dactilares de ambos dedos índices. Organizaciones supranacionales como el Banco Mundial han apostado en los últimos años por el desarrollo de sistemas de identificación digitales basados en biometría (Gelb y Clark, 2013). Las tecnologías biométricas también están resultando de mucha utilidad en situaciones de emergencias humanitarias, como conflictos armados y desastres naturales. Médicos Sin Fronteras, el Comité Internacional de la Cruz Roja, y la Agencia de la Organización de las Naciones Unidas para los Refugiados, entre otras, las utilizan para identificar y registrar a personas, proporcionar asistencia y mejorar la distribución de recursos (Açıkyıldız, 2023).

Otro ámbito en el que las tecnologías juegan un rol fundamental es en el control de las fronteras y la inmigración. Los sistemas de reconocimiento facial y lectura del iris facilitan una identificación de pasajeros más rápida, gracias en gran parte a los pasaportes y documentos de identidad biométricos mencionados anteriormente. En muchos aeropuertos ya son habituales los controles de pasaporte completamente automatizados, con máquinas que verifican la identidad de una persona comparando su fisionomía con la lectura del pasaporte digital.

Un tercer sector que hace un uso importante de estos sistemas es la policía y la justicia. La creación de bases de datos con varios tipos de información biométrica, incluyendo el ADN, facilita las investigaciones criminales, y la identificación y vigilancia de sospechosos y delincuentes. El uso de la biometría está especialmente extendido en operaciones de contraterrorismo. De hecho, el Consejo de Seguridad de las Naciones Unidas (2017)[2] solicita a los Estados miembros que "elaboren y apliquen sistemas de recogida de datos biométricos, que podrían incluir la toma de huellas dactilares, la fotografía, el reconocimiento facial y otras formas de recogida de datos biométricos pertinentes que permitan identificar a las personas, a fin de verificar debidamente y de forma responsable la identidad de los terroristas, incluidos los combatientes terroristas extranjeros, de conformidad con el derecho interno y el derecho internacional de los derechos humanos".

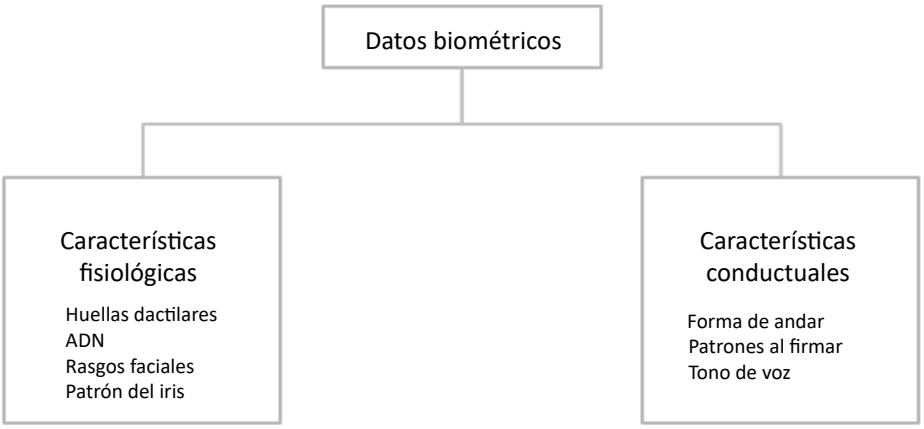
2.2. Tipología y características de los datos biométricos

Los sistemas biométricos transforman características corporales en datos digitales. En base a las características mensuradas, esos datos biométricos se pueden clasificar en físicos (aspectos relativos al cuerpo) y conductuales (aspectos relativos al comportamiento). Aunque la información biométrica se entiende frecuentemente como única y permanente, no toda lo es necesariamente. Como se observa en el cuadro 1, dentro de las características físicas existen: i) los datos fisiológicos, aquellos que sí suelen ser únicos para cada persona y no se pueden modificar fácilmente, como las huellas dactilares y el patrón del iris; ii) otros datos físicos no fisiológicos, como la estatura, el peso o el color de pelo, que no son únicos a la persona y pueden variar a lo largo de la vida.

[2] Punto 15 de la Resolución S/RES/2396 (2017), aprobada por el Consejo de Seguridad de las Naciones Unidas en su 8148ª sesión el 21 de diciembre de 2017.

Cuadro 1

Tipología de los datos biométricos



Fuente: Elaboración propia.

Los datos biométricos constituyen una categoría especialmente sensible dentro de los datos personales. Su principal peculiaridad radica en que se basan en la "lectura" de cuerpos humanos –algo inherente en todas las personas– por lo que se definen frecuentemente como universales. Esto facilita un amplio alcance de cobertura y la replicación de esos sistemas en diferentes contextos y poblaciones. No obstante, es importante recalcar que, aunque las características biométricas sí que están presentes en la mayoría de la población, este no es el caso para todas las personas, lo que puede agravar la exclusión de ciertos grupos ya vulnerables. Por ejemplo, la medición de ciertos tipos de características biométricas es más difícil, e incluso inviable, en personas con algunas discapacidades físicas y mentales, como la invidencia, la parálisis, y la enfermedad de Parkinson (Martin y Donovan, 2015). Asimismo, algunos estudios apuntan que las profesiones que requieren mucho trabajo manual, como la agricultura, pueden deteriorar las huellas dactilares y dificultar así su uso para la identificación (Woodward *et al.,* 2001).

Otra consideración relevante es que el nivel de sensibilidad y riesgo asociado no es el mismo para todos los tipos de datos, sino que depende de si se basan en características variables o invariables (Kuner y Marelli, 2017). Los datos biométricos estáticos, o primarios, son más sensibles, ya que permiten identificar de forma inequívoca a una persona de forma automatizada (Vacca, 2007). Estos son, en su gran mayoría, los datos de tipo fisiológico, persistentes al paso del tiempo. Por el contrario, los datos dinámicos, o secundarios, también aportan información sobre la identidad de una persona, pero no son suficientes por sí solos para determinar de forma precisa una identidad (Li y Jain, 2009). Estos últimos pueden ser tanto físicos como conductuales, como el tono de voz o la forma de andar.

3. Riesgos sociales derivados de la expansión de las tecnologías biométricas

Como hemos visto, el grado de sensibilidad de cada dato biométrico depende de la unicidad y variabilidad de la información que aportan. De igual manera, el riesgo que presentan viene también determinado, en gran

medida, por la tecnología mediante la cual se generan, almacenan y analizan los datos. Podemos diferenciar, por ejemplo, entre sistemas de verificación biométricos que usan *small data* y *big data* (Hu, 2017). Los riesgos asociados al primer caso son bajos; un ejemplo sería la verificación de identidad mediante la comparación de la foto del pasaporte con la cara de la persona que lo presenta en un control de seguridad o un aeropuerto. En cambio, la identificación biométrica con *big data* requiere la digitalización de todas las fotografías de los pasaportes que, almacenados en grandes bases de datos y con la ayuda de algoritmos y técnicas de reconocimiento facial, pueden facilitar un incremento de la vigilancia a gran escala (Hu, 2017).

3.1. Sesgos y discriminación algorítmica

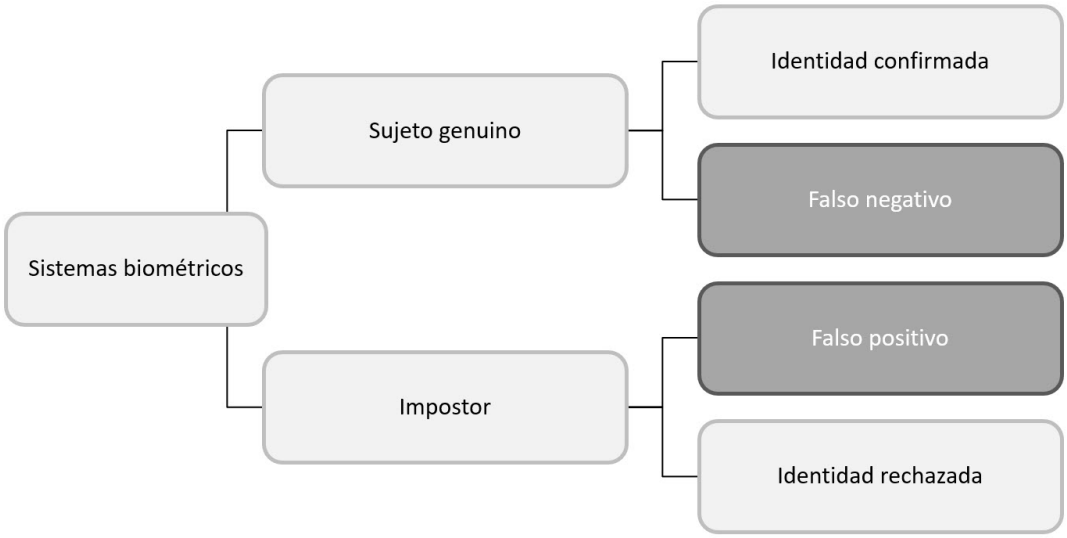
Los sistemas biométricos se alaban frecuentemente por su alta precisión y fiabilidad. Sin embargo, es mucha la evidencia empírica que demuestra su carácter discriminatorio. La discriminación algorítmica se da cuando los algoritmos utilizados para tratar los datos producen resultados que sistemáticamente perjudican a ciertos individuos o grupos por razones de raza, etnicidad o género, entre otras. Algunas de las causas de este sesgo son la falta de diversidad en las bases de datos empleadas y los errores técnicos en el diseño de los algoritmos.

Uno de los ejemplos más estudiados es el desproporcionado número de errores que los sistemas de reconocimiento facial cometen al identificar a personas negras. Esto se debe a que los algoritmos de reconocimiento facial se entrenan frecuentemente con bases de datos en las que predominan rostros de personas blancas occidentales, especialmente hombres. La infrarrepresentación de rostros de personas negras conduce a sesgos en los algoritmos y a una mayor tasa de errores de identificación.

A grandes rasgos, los errores de identificación en los sistemas biométricos pueden ser un falso positivo (el sistema asigna una identidad errónea a la persona) o falso negativo (la identidad es rechazada a pesar de que la persona es quien afirma ser) (cuadro 2). Los dos tipos de

Cuadro 2

Tipos de errores en los sistemas genéricos de identificación biométrica



Fuente: Elaboración propia, versión adaptada a partir del informe *Biometrics at the Frontiers: Assessing the Impact on Society,* publicado por el Joint Research Centre de la Comisión Europea (2005: 34).

errores pueden conllevar graves consecuencias para la persona en cuestión. Un falso negativo puede verse traducido en una denegación de acceso indebida, impidiendo, por ejemplo, cruzar una frontera. Los casos de falsos positivos pueden implicar detenciones injustas por un crimen no cometido.

3.2. La cuestión de privacidad en el centro del debate

Muchas de las críticas a la creciente acumulación de datos por parte de los gobiernos y estados giran en torno al principio de privacidad, o mejor dicho, a su deterioro. La privacidad se entiende comúnmente como la capacidad de una persona para controlar el uso que terceros hacen de sus datos. Ese control se ve comprometido a medida que las nuevas tecnologías digitales recaban cantidades de datos sin precedentes, dificultando nuestra capacidad de saber quién los recolecta y almacena, cómo son analizados y usados, y si son compartidos con terceros. De acuerdo con una visión más restrictiva, el deterioro de nuestra privacidad empieza en el momento en el que nuestros datos son recolectados, independientemente del uso que se haga de ellos[3] (Königs, 2022). Sea cual sea la conceptualización empleada, existe un amplio consenso en la necesidad de salvaguardar la privacidad.

Tal y como se ha mencionado anteriormente, el problema subyacente de los datos biométricos es que la información que contienen es, por naturaleza, especialmente sensible. Se trata, sobre todo, de información única que forma parte de uno mismo, y, por lo tanto, es altamente identificativa (Joint Research Centre, 2005). Mucha de nuestra información biométrica está ligada a nuestro cuerpo y no puede ser modificada. Esto no sería un problema en sí mismo en condiciones perfectas, si pudiésemos asegurar completa e inequívocamente que nuestros datos estarán siempre seguros y que nunca van a ser utilizados para fines que puedan afectarnos negativamente. Pero estas condiciones ideales, desafortunadamente, no se dan en el mundo real. Los ciberataques se han convertido en un arma muy poderosa, afectando a hospitales, aeropuertos, y gobiernos. Las filtraciones indebidas de datos biométricos pueden ser usadas para suplantar identidades. A diferencia del uso de otros sistemas de identificación –como las contraseñas– la forma de nuestro iris o de nuestras huellas dactilares no se pueden modificar fácilmente. Además, nuestros datos biométricos pueden contener otros tipos de información. Por ejemplo, la falta de huellas dactilares puede ser un indicio de enfermedades genéticas como la adermatoglifia (Nousbeck *et al.,* 2011) o de tratamiento por cáncer (Chavarri-Guerra y Soto-Perez-de-Celis, 2015).

La privacidad está intrínsecamente relacionada con la noción de agencia, entendida en este contexto como la percepción de propiedad y control que uno tiene sobre sus datos digitales, así como la capacidad de decidir acerca de su creación, acceso y uso (Kaurin, 2019). En otras palabras, un individuo tiene agencia cuando tiene autonomía para ejercer la propiedad y el control sobre la creación y el uso de sus datos. Desde un punto de vista ético y ontológico, existe un interesante debate en torno a cómo la digitalización de los cuerpos afecta a la autorrepresentación de uno mismo en la esfera digital y cómo disminuye la capacidad individual de limitar la información que puede ser extraída de nuestro cuerpo.

El principio de agencia se ve comprometido cuando la recolección de datos corporales se hace sin autorización ni conocimiento por parte del individuo en cuestión. Esto sucede porque la captura de ciertos indicadores biométricos no requiere la colaboración activa del individuo, e incluso puede pasar desapercibida. Es el caso de las cámaras de circuito cerrado de televisión (CCTV) y las tecnologías de reconocimiento facial, las cuales pueden recolectar información mientras paseamos dentro de su área de cobertura sin que seamos conscientes de ello. Esto genera inquietud por la creciente capacidad que tienen los gobiernos de extraer datos sin autorización explícita ni el consentimiento de los ciudadanos (Marciano, 2019). Incluso cuando el sistema requiere nuestra participación activa, cada vez tenemos menos poder para decidir si queremos ser sujetos de estas tecnologías o no (Hu, 2017). Un ejemplo son los pasaportes biométricos. Si bien un ciudadano puede negarse a proveer tal información a las autoridades renunciando a la tramitación de su pasaporte, esta

[3] Véase Königs (2022) para una discusión más extensa sobre las diversas formas de conceptualizar la privacidad.

decisión conlleva importantes limitaciones en cuanto a su movilidad internacional.

3.3. Vigilancia y control social

Las tecnologías biométricas incrementan sustancialmente las capacidades de vigilancia y control de los Estados. No es casualidad, entonces, que la idea del panóptico[4] de Jeremy Bentham siga viva a día de hoy, más de doscientos años después de su publicación, en los debates acerca de cómo la digitalización afecta a nuestras sociedades. El carácter ubicuo de las tecnologías digitales resuena con la estructura semicircular del panóptico, donde el guardián puede observar todas las celdas de la prisión desde una torre central de vigilancia sin que los prisioneros sean conscientes de si están siendo observados o no. Las cámaras de reconocimiento facial, por ejemplo, dibujan claros paralelismos con la idea de una vigilancia continua y centralizada, y muchas veces imperceptible.

La creciente presencia de cámaras en espacios públicos genera un efecto desincentivador[5], por el cual los ciudadanos cambian su comportamiento o se autocensuran tratando de evitar las posibles represalias por parte del Gobierno. Este fenómeno tiende a disuadir la participación en manifestaciones y protestas cuando se teme que las autoridades públicas puedan perseguir posteriormente a los participantes o tacharlos de enemigos. El efecto desincentivador va mucho más allá del individuo; conlleva un enorme deterioro de los principios democráticos y los derechos fundamentales, como la libertad de expresión y de asamblea.

Las tecnologías biométricas están siendo sujetas a abusos de poder con el fin de reforzar el control político, especialmente en manos de regímenes autoritarios. Numerosos informes vienen denunciando en los últimos años un incremento del uso de herramientas digitales para identificar, monitorear y arrestar a manifestantes y miembros de la oposición política. A modo de ejemplo, el Gobierno ruso acumula un largo historial de denuncias por usar el reconocimiento facial para detener a activistas y críticos del régimen[6].

Las tecnologías biométricas pueden asimismo reforzar un nivel ilícito de control social. Un uso semejante se ha llevado particularmente lejos en el caso de China, cuyo modelo de control y vigilancia se basa en la vinculación de múltiples bases de datos y sistemas de monitorización. Estas prácticas resultan especialmente invasivas en las regiones autónomas de Sinkiang y del Tíbet, donde se concentran minorías étnicas. El sistema principal de vigilancia masiva en Sinkiang –*Integrated Joint Operations Platform (IJOP)*–, usado por la policía para identificar actividades o comportamientos considerados sospechosos, recoge una gran variedad de información de todos sus ciudadanos, incluyendo su grupo sanguíneo. El sistema *IJOP* ha sido objeto de duras críticas por marcar especialmente a la población musulmana uyghur y otros grupos minoritarios de origen turco (Wang, 2019). En Irán, la ola de protestas por el asesinato de Mahsa Amini en 2022 provocó el despliegue de sistemas de reconocimiento facial, usados para identificar y castigar a las mujeres que no cumplan con el requisito obligatorio de llevar *hiyab*. Las cámaras fueron instaladas en las calles y el transporte público, pero también en establecimientos comerciales y oficinas (González, 2023).

4. La Unión Europea: pionera en la regulación de sistemas y datos biométricos

En los últimos años, la UE se ha consolidado como la pionera en la regulación de las tecnologías digitales y la más garantista en cuanto a los derechos de los ciudadanos en relación con estas tecnologías. No existe una ley específica de biometría, regulándose este tipo de tecnologías y datos biométricos a través de múltiples instrumentos legales. A continuación se

[4] Cabe recordar que la idea del panóptico fue inspirada por el hermano de Jeremy Bentham, quién diseñó un sistema similar para coordinar el trabajo y mejorar la eficiencia en las fábricas en un momento de expansión del sector industrial. Bentham trasladó esa idea y la contextualizó en su trabajo sobre la reforma del sistema penitenciario en Inglaterra.

[5] Conocido comúnmente como *chilling effects*.

[6] Para más información, véase el artículo publicado por Human Rights Watch (2015, 15 de septiembre), https://www.hrw.org/news/2021/09/15/russia-broad-facial-recognition-use-undermines-rights

exponen los dos principales: la Ley de Inteligencia Artificial y el Reglamento General de Protección de Datos (RGPD).

4.1. La Ley de Inteligencia Artificial

Como ya se ha mencionado, los riesgos derivados de las tecnologías y datos biométricos emergen, en particular, cuando se combinan con algoritmos. Sobre esta base, la nueva regulación en materia de inteligencia artificial (IA) de la UE ha supuesto importantes avances en la limitación del uso y desarrollo de sistemas biométricos en los Estados miembros. Aunque hayan transcurrido casi tres años desde que la primera propuesta de ley europea de IA fue presentada por la Comisión Europea, esta fue finalmente aprobada por el Parlamento Europeo el pasado 13 de marzo de 2024. Su entrada en vigor es paulatina y puede extenderse hasta 36 meses desde su publicación en el *Diario Oficial de la Unión Europea* (European Parliament, 2024). La cronología indica que la regulación va siempre un paso por detrás de la innovación tecnológica, no sólo debido al dinamismo y velocidad a la que avanzan las tecnologías, sino también dada la complejidad para analizar todas sus posibles aplicaciones y potenciales riesgos, y llegar a acuerdos que satisfagan los intereses del gran número de actores involucrados. La Ley de IA traza un marco jurídico armonizado que busca proteger a los ciudadanos de peligros emergentes, al mismo tiempo que fomentar la innovación en el sector de la IA.

La ley establece un enfoque basado en el nivel de riesgo planteado por el sistema o la tecnología en cuestión, sobre la base del cual se establecen unos requisitos y unas obligaciones concretas. Como se observa en el cuadro 3, los riesgos se clasifican en cuatro grupos. En el nivel más alto de riesgo se sitúan las prácticas consideradas inaceptables, quedando prohibidas en su totalidad. Es el caso de los sistemas de identificación biométrica a distancia en tiempo real. También se prohíbe la creación de bases de datos de reconocimiento facial usando la extracción no selectiva de imágenes faciales de Internet o de CCTV, así como los sistemas de IA basados en información biométrica para inferir características personales, incluyendo creencias

Cuadro 3

Niveles de riesgo estipulados en el marco regulatorio de la Ley de IA de la UE

Fuente: Elaboración propia, basada en la publicación de la Comisión Europea (European Commission, 2024).

religiosas, convicciones políticas, orientación sexual o raza. Igualmente, no están permitidos los sistemas de reconocimiento de emociones en lugares de trabajo o centros educativos.

Aun cuando los sistemas de identificación biométrica presentan un riesgo inaceptable, existen ciertas excepciones en las que se permite su uso. Así, en ciertas situaciones, los cuerpos policiales y de seguridad pueden ser autorizados a utilizar los sistemas de identificación biométrica a distancia en tiempo real en espacios públicos, por ejemplo, para la búsqueda de una persona desaparecida o la prevención de un ataque terrorista. También se reconocen excepciones en el uso de técnicas para el reconocimiento de emociones por determinadas razones de seguridad o médicas. Con todo, el listado de excepciones acerca de los sistemas y datos biométricos previstas en la Ley de IA de la UE ha suscitado críticas y malestar entre las principales organizaciones internacionales en materia de derechos digitales[7].

4.2. El Reglamento General de Protección de Datos (RGPD)

Dado que los datos biométricos constituyen un subtipo de datos personales, su regulación está contemplada en el Reglamento General de Protección de Datos (RGPD)[8]. Este es el marco legislativo en materia de privacidad de la información personal en la UE, que, desde su entrada en vigor en 2018, es de obligado cumplimiento en todos los Estados miembros. El RGPD se considera el reglamento más completo y protector a nivel mundial, y un ejemplo para el desarrollo de leyes de privacidad en otros países (Sullivan, 2019; Yakovleva, 2022). Reconoce a los individuos el derecho de conocer quiénes recolectan sus datos, con qué fines, y cómo son usados. Con ese objetivo, los recolectores de datos personales están obligados a informar a los sujetos de los datos sobre ciertos aspectos. Además, el RGPD incorpora nuevos derechos que los individuos pueden ejercer, como solicitar más información sobre el tratamiento de sus datos por parte de terceros y requerir la supresión de información personal de las bases de datos. Los principales derechos generales de los individuos (como sujetos de los datos personales) estipulados por el RGPD aparecen resumidos en la tabla 1.

Los datos biométricos figuran en el RGPD como una de las categorías especiales dentro de los datos personales que requieren especial protección, debido a que "por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales" (Punto 51, RGPD, 2016). Salvo ciertas excepciones, su tratamiento para la identificación de manera unívoca a una persona física queda prohibido bajo la regulación europea (Art.9, RGPD, 2016).

Es importante, sin embargo, remarcar que no toda la información biométrica está considerada como dato biométrico bajo el RGPD. En concreto, esta disposición define los datos biométricos 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" (RGPD, 2016). La mención de "un tratamiento técnico específico" es clave para entender la interpretación del RGPD. La información corporal se reconoce y, por lo tanto, se regula como dato biométrico únicamente cuando es tratada con unas tecnologías concretas. Por ejemplo, conforme al artículo 51 de dicha normativa, "el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física" (RGPD, 2016).

[7] Véase, por ejemplo, la nota de prensa de AccessNow titulada "The EU AI Act: a failure for human rights, a victory for industry and law enforcement", publicada el 13 de marzo de 2024 (https://www.accessnow.org/press-release/ai-act-failure-for-human-rights-victory-for-industry-and-law-enforcement/).

[8] Su nombre en inglés es General Data Protection Regulation (GDPR).

Tabla 1

Reglamento General de Protección de Datos (RGPD) de la Unión Europea: derechos de los interesados, referentes a la privacidad de datos personales

Art.13 Art.14	*Derecho a ser informado* de los datos personales recolectados y su finalidad, tanto si la información se ha obtenido directamente de los interesados como de otra fuente.
Art.15	*Derecho de acceso* al responsable del tratamiento de los datos personales para obtener confirmación acerca de si los datos han sido tratados, y, en caso afirmativo, obtener detalles del proceso.
Art.16 Art.19	*Derecho de rectificación,* eso es, a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan.
Art.17	*Derecho de supresión,* conocido como "el derecho a ser olvidado", esto es, a obtener sin dilación indebida del responsable del tratamiento la supresión de datos personales.
Art.18	*Derecho a la limitación del tratamiento* de los datos en esos casos estipulados por la ley.
Art.20	*Derecho a la portabilidad,* o a recibir los datos personales que se hayan facilitado previamente, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos sin obstáculos a otros responsables.
Art.21	*Derecho de oposición* a ciertos tratamientos de los datos personales.
Art.22	*Derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado,* incluida la elaboración de perfiles, que produzca efectos jurídicos para la persona o le afecte significativamente de modo similar.

Nota: Para una descripción más extensa y detallada de los casos, consúltese el capítulo III del RGPD.

Fuente: Elaboración propia a partir del capítulo II del RGPD (Parlamento Europeo y Consejo Europeo, 2016).

5. Conclusiones y consideraciones finales

El uso de sistemas biométricos por parte de los gobiernos es una práctica en auge en todo el mundo, y que previsiblemente va a generar una creciente cantidad de información biométrica sobre los ciudadanos. En este artículo se ha argumentado que, sin descuidar el gran potencial aportado por las tecnologías biométricas, es fundamental conocer los riesgos que pueden derivarse de su empleo, entre ellos, la discriminación algorítmica, la erosión de la privacidad y la agencia individual, así como los abusos de poder para discriminar a ciertos grupos y ejercer un control social invasivo.

Sin duda, todas las tecnologías están sujetas a posibles desviaciones de uso, es decir, a que sean empleadas en un futuro para fines diferentes de aquellos para los que fueron diseñadas. Asimismo, los intereses de los que controlan la tecnología y los datos pueden variar con el tiempo, lo que resulta especialmente preocupante tratándose de información biométrica altamente identificativa e inalterable. Estas fueron las críticas que recibió el Gobierno francés recientemente cuando anunció un incremento de cámaras de vigilancia en espacios públicos como medida para reforzar la seguridad en los Juegos Olímpicos de 2024. El riesgo de que las imágenes de vídeo almacenadas se pudieran utilizar para fines ilegítimos en un futuro alentó un fuerte debate.

Finalmente, las consecuencias de las tecnologías vienen determinadas en gran medida por quién las usa y cómo. Aun cuando en las democracias consolidadas el riesgo de un uso indebido es menor que en países con deficiencias democráticas, sería ingenuo pensar que las democracias están libres de tales abusos. Solo hace falta recordar el escándalo de la Agencia de Seguridad Nacional de los Estados Unidos destapado por Edward Snowden en 2013, que sacó a la luz el uso invasivo que el Gobierno hacía de las tecnologías para vigilar a millones de civiles. Como argumenta Schneier (2016), no cabe dar por supuesto que absolutamente todas las personas que puedan tener algún

poder o alguna influencia sobre la tecnología o los datos vayan a actuar siempre con total integridad. Por este motivo, es fundamental seguir promoviendo los debates en la esfera social y política sobre qué tecnologías queremos en nuestra sociedad y cómo las implementamos, al igual que cómo podemos mejorar los sistemas de control y rendición de cuentas sobre quienes disponen de la capacidad de recoger y usar nuestros datos personales más sensibles.

Bibliografía

Açlkylldlz, Ç. (2023). 'I know you like the back of my hand': biometric practices of humanitarian organisations in international aid. *Disasters, 48*(2). https://doi.org/10.1111/disa.12612

Article 19. (2023, 22 de agosto). Iran: *Tech-enabled "Hijab and chastity" law will further punish women.* https://www.article19.org/resources/iran-tech-enabled-hijab-and-chastity-law-will-further-punish-women/

Bacciarelli, A. (2023). *Time to ban facial recognition from public spaces and borders.* Human Rights Watch. https://www.hrw.org/news/2023/09/29/time-ban-facial-recognition-public-spaces-and-borders

Chavarri-Guerra, Y., y Soto-Perez-de-Celis, E. (2015). Loss of finger- prints. *New England Journal of Medicine, 372*(16). https://doi.org/10.1056/NEJMicm1409635

Consejo de Seguridad de las Naciones Unidas. (2017). Resolución 2396 de 21 de diciembre de 2017. https://documents.un.org/doc/undoc/gen/n17/460/28/pdf/n1746028.pdf?token=QtLiRM7ZBR7pyywJfe&fe=true

European Commission. (2024). AI Act. Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

European Parliament. (2024). Artificial Intelligence Act: MEPs adopt landmark law (13 de marzo). https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law

Gelb, A., y Clark, J. (2013). *Identification for development: the biometrics revolution*. Center for Global Development, 315. www.cgdev.org

Gonzalez, B. (2023, diciembre). *Facial recognition in Iranian metro being used as scare tactic to enforce hijab.* Biometric Update | Biometrics news, companies and explainers. https://www.biometricupdate.com/202312/facial-recognition-in-iranian-metro-being-used-as-scare-tactic-to-enforce-hijab

Hu, M. (2017). From the national surveillance state to the cybersurveillance state. *Annual Review of Law and Social Science,* 13, 161-180. https://doi.org/10.1146/ANNUREV-LAWSOCSCI-110316-113701

Human Rights Watch. (2015, 15 de septiembre). *Russia: Broad facial recognition use undermines rights.* https://www.hrw.org/news/2021/09/15/russia-broad-facial-recognition-use-undermines-rights

Human Rights Watch. (2021, 15 de junio). *UN shared Rohingya data without informed consent.* https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent

Joint Research Centre. (2005). Biometrics at the frontiers: assessing the impact on society. Technical report series. Institute for Prospective Technological Studies, European Commission. https://op.europa.eu/en/publication-detail/-/publication/cd472dc6-4298-441c-92ec-7307811bb479/language-en

Kaurin, D. (2019). Data protection and digital agency for refugees. *World Refugee Council Research Paper Series,* 12. https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees/

Kindt, E. J. (2018). Having yes, using no? About the new legal regime for biometric data. *Computer Law and Security Review, 34*(3), 523–538. https://doi.org/10.1016/J.CLSR.2017.11.004

Königs, P. (2022). Government surveillance, privacy, and legitimacy. *Philosophy & Technology, 35*(8). https://doi.org/10.1007/s13347-022-00503-9

Kuner, C., y Marelli, M. (2017). *Handbook on data protection in humanitarian action.* International Committee of the Red Cross. https://www.icrc.org/en/data-protection-humanitarian-action-handbook

Lee, M. M., y Zhang, N. (2016). Legibility and the informational foundations of state capacity. *Journal of Politics, 79*(1), 118–132. https://doi.org/10.1086/688053

Li, S. Z., y Jain, A. (2009). *Encyclopedia of biometrics.* Springer. https://link.springer.com/referencework/10.1007/978-0-387-73003-5

Lyon, D. (2008). Biometrics, identification and surveillance. *Bioethics, 22*(9), 499–508. https://doi.org/10.1111/J.1467-8519.2008.00697.X

Marciano, A. (2019). Reframing biometric surveillance: from a means of inspection to a form of control. *Ethics and Information Technology, 21*(2), 127–136. https://doi.org/10.1007/s10676-018-9493-1

Martin, A. K., y Donovan, K. P. (2015). New surveillance technologies and their publics: a case of biometrics. *Public Understanding of Science, 24*(7), 842–857. https://doi.org/10.1177/0963662513514173

Nousbeck, J., Burger, B., Fuchs-Telem, D., Pavlovsky, M., Fenig, S., Sarig, O., *et al.* (2011). A mutation in a skin-specific isoform of SMARCAD1 causes autosomal-dominant adermatoglyphia. *The American Journal of Human Genetics, 89*(2), 302–307. https://doi.org/10.1016/j.ajhg.2011.07.004.

Parlamento Europeo y Consejo Europeo. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (*Diario Oficial de la Unión Europea,* de 4 de mayo de 2016). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L:2016:119:FULL

Schneier, B. (2016). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* W. W. Norton & Company.

Sullivan, C. (2019). EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era. *Computer Law & Security Review: The International Journal of Technology Law and Practice,* 35, 380–397. https://doi.org/10.1016/j.clsr.2019.05.004

Vacca, J. R. (2007). *Biometric technologies and verification systems.* Elsevier Butterworth-Heinemann.

Wang, M. (2019, 1 de mayo). *Interview: China's "big brother" app.* Human Rights Watch. https://www.hrw.org/news/2019/05/01/interview-chinas-big-brother-app

Woodward, J. D., Webb, K., Newton, E., Bradley, M., y Rubenson, D. (2001). *Army biometric applications: Identifying and addressing sociocultural concerns.* Arroyo Center RAND. https://www.rand.org/pubs/monograph_reports/MR1237.html

Yakovleva, S. (2022). Three data realms: convergence or competition. Amsterdam Law School Research Paper, No. 2022-58. *Institute for Information Law Research Paper* No. 2022-13. https://ssrn.com/abstract=4028668 or http://dx.doi.org/10.2139/ssrn.4028668