Deusto Journal of Human Rights
Revista Deusto de Derechos Humanos

No. 14/2024

DOI: https://doi.org/10.18543/djhr142024

ARTICLES / ARTÍCULOS

Desafíos ético-jurídicos en el uso de Inteligencia Artificial para el tratamiento masivo de datos biométricos

The ethical-legal challenges in the use of Artificial Intelligence for the massive processing of biometric data

Nuria Cuadrado Gamarra
https://doi.org/10.18543/djhr.3199
Fecha de publicación en línea: diciembre de 2024

Desafíos ético-jurídicos en el uso de Inteligencia Artificial para el tratamiento masivo de datos biométricos

The ethical-legal challenges in the use of Artificial Intelligence for the massive processing of biometric data

Nuria Cuadrado Gamarra
Universidad Complutense de Madrid. España
nuriacua@ucm.es
ORCiD: https://orcid.org/0000-0001-5186-988X

https://doi.org/10.18543/djhr.3199

Fecha de recepción: 31.05.2024
Fecha de aceptación: 04.08.2024
Fecha de publicación en línea: diciembre de 2024

Cómo citar / Citation: Cuadrado, Nuria. 2024. «Desafíos ético-jurídicos en el uso de la Inteligencia Artificial para el tratamiento masivo de datos biométricos». *Deusto Journal of Human Rights*, n. 14: 341-374. https://doi.org/10.18543/djhr.3199

Resumen: El artículo examina la intersección entre la Inteligencia Artificial (IA) y el tratamiento masivo de datos biométricos, resaltando desafíos éticos y jurídicos emergentes. Comienza contextualizando el uso creciente de la IA en sistemas que emplean datos biométricos, como reconocimiento facial, huellas dactilares, escaneo del iris y voz. Se analiza la complejidad en la recopilación, almacenamiento y uso de datos biométricos a gran escala, enfocándose en la privacidad, la seguridad y el consentimiento informado. También aborda los sesgos y sus implicaciones, destacando posibles impactos discriminatorios y los desafíos para salvaguardar los derechos fundamentales en estos sistemas.

Palabras clave: Inteligencia Artificial, datos biométricos, desafíos éticos, privacidad, seguridad, consentimiento, procesamiento masivo.

Abstract: The article examines the intersection between Artificial Intelligence (AI) and the massive processing of biometric data, emphasizing emerging ethical and legal challenges. It begins by contextualizing the increasing use of AI in systems utilizing biometric data such as facial recognition, fingerprints, iris scan and voice. The complexity of collecting, storing, and utilizing biometric data on a large scale is analyzed, focusing on privacy, security, and informed consent. Additionally, it addresses biases and their implications, highlighting potential discriminatory impacts and the challenges in safeguarding fundamental rights within these systems.

Keywords: Artificial Intelligence, biometric data, ethical challenges, privacy, security, consent, massive processing.

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 341-374
https://doi.org/10.18543/djhr.3199 • http://djhr.revistas.deusto.es/

Introducción[1]

En la última década, se detecta un uso en prácticamente todos los sectores de la cotidiana vida individual y colectiva de una tecnología, la Inteligencia Artificial (en adelante, IA)[2], dotada de una potencia excepcional, que ha permitido contribuir a una expansión enorme y un rapidísimo desenvolvimiento de la misma. Hasta el punto de que ha terminado por convertirse en un acontecimiento social y económico, un "boom" mediático y real, una gigantesca tela de araña e instrumento que probablemente terminará siendo accesible, cómodo e imprescindible. Ingenio tecnológico que proyecta una influencia exponencial y que se encuentra en fase de crecimiento, y que, a su vez, terminará por provocar modificaciones de algunas de las nociones más básicas de la existencia.

Uno de los campos en los que la IA ha tenido un impacto significativo es en el tratamiento de datos biométricos. La capacidad de los sistemas de IA para analizar, interpretar y utilizar datos biométricos tales como reconocimiento facial, huellas dactilares, voz, iris, retina, movimientos corporales y otros atributos únicos ha revolucionado tanto la tecnología como los servicios a los que accedemos (Cotino 2022, 68; Bestard 2021, 3). De esta manera, se genera de manera permanente un imparable flujo de ingentes caudales agregados de datos biométricos, de muy diversa procedencia, naturaleza, condición y valor, confirmándose, al mismo tiempo que se multiplica, la explosión de información por sobreabundancia.

El uso generalizado de sistemas biométricos impulsados por la IA ha brindado beneficios notables en áreas como la seguridad (Barona 2024, 303), la protección de la salud, la identificación personal y la accesibilidad a diferentes servicios. Sin embargo, este progreso

[1] Este trabajo se ha realizado en el marco del Proyecto de I+D+i PID2022-136439OB-I00/ MCIN/AEI/10.13039/501100011033, Derechos y garantías públicas frente a las decisiones automatizadas y el sesgo y discriminación algorítmicas, financiado por el Ministerio de Ciencia y Innovación, Cofinanciado por el Fondo Europeo de Desarrollo Regional "Una manera de hacer Europa".

[2] Como es de sobra conocido, la definición del sintagma Inteligencia Artificial no resulta pacífica. Nos serviremos en este texto del artículo 3.1. del Reglamento Europeo de Inteligencia Artificial, en virtud del cual se considera IA: "un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomías, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entorno físicos o virtuales".

tecnológico conlleva una serie de desafíos éticos y jurídicos que requieren una atención minuciosa y una regulación adecuada (Aliaga y Gutiérrez 2020, 3; Etxeberria et al. 2023, 107-126).

El propósito de este artículo es analizar críticamente la intersección entre la IA y el tratamiento masivo de datos biométricos, examinando los desafíos éticos y legales emergentes en este campo. Se comenzará con una descripción detallada del uso actual de la IA en sistemas biométricos, destacando su evolución y aplicaciones. Posteriormente, se explorarán las complejidades en la recopilación, almacenamiento y uso a gran escala de datos biométricos, enfocándose en las preocupaciones éticas relacionadas con la privacidad, la seguridad o el consentimiento informado. Asimismo, se analizará la relevancia jurídica y regulatoria, evaluando la adecuación de los marcos legales existentes para abordar los desafíos planteados por la combinación de estas tecnologías avanzadas. Además, se discutirá la implementación y efectividad de las políticas actuales en diversos contextos jurídicos y culturales (Álvarez y Sanz 2021)

El análisis culminará con el estudio de un caso específico. En concreto, el controvertido uso del escaneo del iris como método de identificación biométrica que implementó Worldcoin, empresa de criptomonedas dirigida por el CEO de OpenAI Sam Altman, ofreciendo de esta manera una perspectiva práctica de los temas tratados (Andúgar 2023, Barona 2024). Finalmente, se presentarán conclusiones y recomendaciones para futuras investigaciones y políticas públicas en este ámbito.

Las aplicaciones de las tecnologías englobadas dentro del concepto amplio de IA son versátiles, abarcando diversos sectores y contextos. Estas tecnologías se utilizan desde la automatización de tareas mecánicas o rutinarias, como la gestión de comunicaciones, seguimiento de envíos, facturación y remesas, hasta operaciones más complejas, como la toma de decisiones algorítmicas en mercados financieros, clasificación de datos para la selección de personal, filtrado de contenidos, evaluación de solvencia, resolución de disputas y la interacción conversacional con humanos mediante asistentes personales, robots asistenciales y chatbots. Los riesgos asociados son variados, y las cuestiones legales que surgen difieren significativamente según el caso. Las tecnologías de reconocimiento facial y biométricas están revolucionando la forma en que se gestiona la seguridad y la privacidad en diversos contextos, desde el acceso a eventos deportivos hasta el control de la presencia en entornos laborales (Díaz Lima 2023; Espuga 2023)

Resulta necesario, al tiempo que evidente, destacar que los beneficios de la IA son extensos, tanto para el ámbito privado como público. Así, la

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 341-374
https://doi.org/10.18543/djhr.3199 • http://djhr.revistas.deusto.es/

IA mejora la eficiencia de las organizaciones y sus procesos internos, dando lugar a nuevos modelos de negocio, productos y servicios. Asimismo, tiene impactos positivos para los Estados, contribuyendo a la predecibilidad en decisiones administrativas (Ponce 2024) y judiciales (Simón 2021), sistemas objetivos de selección de empleados públicos, fortalecimiento de la protección policial, identificación de delincuentes, anticipación de fraudes fiscales (Serrano 2022) o incumplimientos con entidades como la Hacienda Pública o la Seguridad Social. Sin embargo, también se han identificado efectos negativos. Las ventajas mencionadas pueden afectar derechos individuales como la intimidad, la protección de datos, la igualdad o la interdicción de la discriminación. Además, existe una importante preocupación por la posible destrucción de empleo, confusiones entre personas inocentes y delincuentes debido al mal uso de la biométrica, y un aumento de la discriminación basada en diversas circunstancias personales.

Ante estos desafíos, el 21 de abril de 2021, la Comisión Europea presentó la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre Inteligencia Artificial (Reglamento de Inteligencia Artificial o Artificial Intelligence Act), actualmente aprobado[3]. Reglamento a través del que se busca, entre otras cuestiones, establecer normas armonizadas en el ámbito de la IA para abordar los desafíos éticos y legales asociados con su uso en el contexto actual y con proyección de futuro.

1. **Conceptos previos**

Antes de adentrarnos en los detalles del almacenamiento y tratamiento de datos biométricos con sistemas de IA, entendemos que resulta esencial definir algunos conceptos clave que serán recurrentes a lo largo de este análisis. Los datos biométricos son sometidos a un "tratamiento técnico específico" según el artículo 4.14 del Reglamento General Europeo de Protección de Datos[4] (en adelante RGPD), al que en ocasiones se refiere como como tratamiento "automático" y en

[3] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). Véase Simón y Cotino (2024).

[4] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento

otras como "automatizado". Este estudio excluye el simple tratamiento de vídeos y fotografías sin sistemas automatizados para extraer datos biométricos, sin cotejo con una base de datos adicional, como se indica en el Dictamen 3/2012 del G29[5]. Aunque la videovigilancia, ya sea pública o privada, plantea importantes problemas, el enfoque principal aquí se centra en el uso de componentes de IA o aprendizaje automático, que se ha vuelto cada vez más común y representa un avance significativo (Arroyo 2022).

Los sistemas de identificación biométrica automatizados, especialmente aquellos basados en IA o reconocimiento facial, tienden a facilitar la vigilancia masiva o exhaustiva. Resultan difíciles de restringir, manejan datos sensibles, las inferencias y conclusiones derivadas de ellos pueden tener un impacto considerable y la duración del tratamiento puede ser extensa. Además, existe la posibilidad de que se utilicen para fines desconocidos. Es importante señalar que la regulación actual para tratamientos "simples" de videovigilancia no es adecuada legalmente para los tratamientos con sistemas biométricos que incorporan IA y reconocimiento facial, según el Informe 31/2019 de la Agencia Española de Protección de Datos (en adelante, AEPD)[6].

En lo que concierne al uso de los datos biométricos, hay un interés particular en las técnicas de reconocimiento facial basadas en sistemas de IA. El reconocimiento facial es una funcionalidad de software que puede conectarse con diversos sistemas y combinarse con otras funciones. Aunque el reconocimiento facial automático, que implica el tratamiento de datos personales protegidos, ha generado preocupaciones, también se destaca que las técnicas de reconocimiento facial basadas en IA son emblemáticas de esta tecnología y sus riesgos. A pesar del enfoque especial en el reconocimiento facial, el régimen jurídico aplicable es el más general de los sistemas biométricos, no limitándose exclusivamente a patrones faciales.

2. **Uso de la IA en el tratamiento de datos biométricos**

La intersección en constante expansión entre la IA y el tratamiento de datos biométricos ha dejado una marca significativa en el panorama

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).

[5] El llamado Working Party, también conocido como G29 o Grupo de Trabajo del artículo 29, hoy Comité Europeo de Protección de Datos o EDPB por sus siglas en inglés

[6] Véase: https://www.aepd.es/documento/2019-0031.pdf

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 341-374
https://doi.org/10.18543/djhr.3199 • http://djhr.revistas.deusto.es/

tecnológico contemporáneo. Este apartado se centra en una exploración exhaustiva de la aplicación de la IA en el procesamiento de datos biométricos, desglosando diversos aspectos clave que definen este paradigma tecnológico. El avance de la IA ha permitido que los sistemas de reconocimiento facial y otros métodos biométricos sean más precisos y eficientes, lo que ha llevado a su adopción en una variedad de sectores, desde la seguridad pública hasta el comercio minorista (Baz 2021).

2.1. *Evolución de la aplicación de la IA en datos biométricos*

En lo que sin duda constituye un desvergonzado análisis retrospectivo, procedemos a examinar algunos de los más destacados hitos que han propiciado mejoras sustanciales en la identificación y autenticación biométrica. Este enfoque histórico contextualiza la progresión tecnológica, resaltando cómo la IA ha impulsado avances en la precisión y eficiencia de los sistemas biométricos. Así, a lo largo de la evolución de la aplicación de la IA en el tratamiento de datos biométricos hemos sido testigos de un progreso continuo que ha transformado radicalmente la capacidad de identificación y autenticación. Desde sus primeras implementaciones hasta las más actuales, la IA ha desempeñado un papel esencial en el refinamiento de los sistemas biométricos.

En sus primeras etapas, la recopilación de datos biométricos con sistemas de IA se centraba, principalmente, en algoritmos de comparación simples para la identificación de características biométricas básicas, como huellas dactilares. A medida que la capacidad computacional aumentó, surgieron algoritmos más complejos basados en el aprendizaje automático, permitiendo una adaptación dinámica a patrones biométricos más sofisticados. Con el tiempo, los algoritmos de reconocimiento facial impulsados por la IA han experimentado avances notables. La capacidad de la IA para analizar de manera eficiente las características faciales, considerando aspectos como la variabilidad en expresiones y ángulos de captura, ha mejorado significativamente. Además, el aprendizaje profundo ha permitido modelos más precisos y robustos, contribuyendo a la identificación facial en condiciones diversas. En paralelo, el procesamiento de lenguaje natural ha influido en la interpretación y autenticación de características biométricas como la voz y los patrones de escritura. Los algoritmos basados en esta rama de la IA han logrado una comprensión más profunda de las variaciones en el habla y en la

escritura, mejorando la precisión y la adaptabilidad de los sistemas biométricos relacionados.

La evolución de la aplicación de la IA en datos biométricos no solo se ha traducido en avances tecnológicos, sino que también ha impactado en la accesibilidad y la eficiencia de los sistemas. La capacidad de aprendizaje continuo de la IA ha permitido adaptarse a nuevos patrones biométricos sin intervención humana constante, facilitando la implementación en entornos dinámicos. En conjunto, la evolución en la aplicación de la IA en datos biométricos refleja una trayectoria ascendente, desde métodos iniciales hasta la adopción de técnicas más avanzadas, marcando así una era donde la IA y los datos biométricos convergen para ofrecer soluciones cada vez más precisas y adaptativas en el ámbito de la identificación y autenticación.

2.2. *Aprendizaje automático y procesamiento de lenguaje natural en datos biométricos*

La fusión de la IA con el tratamiento de datos biométricos se ha potenciado significativamente a través del aprendizaje automático y el procesamiento de lenguaje natural (en adelante, PLN). El aprendizaje automático ha revolucionado la interpretación de datos biométricos al permitir que los sistemas se adapten y evolucionen con la experiencia. En el contexto biométrico, algoritmos de aprendizaje automático, como redes neuronales y máquinas de soporte vectorial, han demostrado ser especialmente eficaces en el reconocimiento facial y de voz. Estos algoritmos pueden aprender patrones complejos y variaciones, mejorando la precisión y la capacidad de adaptación de los sistemas biométricos. De la misma manera, el PLN ha ampliado la aplicación de datos biométricos más allá de las tradicionales huellas dactilares y reconocimiento facial. En el ámbito biométrico, el PLN se aplica a la identificación de patrones en la voz y en los patrones de escritura. Los algoritmos de PLN pueden analizar la entonación, el ritmo y otros aspectos lingüísticos, mejorando la precisión en la autenticación biométrica basada en la voz. Además, el PLN permite la interpretación de patrones en la escritura, contribuyendo así a una autenticación más holística.

La integración de aprendizaje automático y PLN en sistemas biométricos ha impulsado la capacidad de interpretar datos complejos y variados. En el reconocimiento facial, por ejemplo, los algoritmos pueden aprender a reconocer expresiones faciales específicas y adaptarse a diferentes condiciones de iluminación. En el

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 341-374
https://doi.org/10.18543/djhr.3199 • http://djhr.revistas.deusto.es/

reconocimiento de voz, la combinación de PLN con aprendizaje automático permite una interpretación más precisa y contextual de los patrones vocales, mejorando la autenticación biométrica.

2.3. *Aplicaciones prácticas en seguridad, salud y otros sectores*

Si analizamos las aplicaciones prácticas que han surgido de la convergencia entre la IA y los datos biométricos, debemos detenernos en examinar casos de implementaciones exitosas en sectores clave, como la seguridad, la salud y el ámbito empresarial, identificando beneficios tangibles y potenciales riesgos asociados con la adopción masiva de estas tecnologías. La confluencia de la IA y el tratamiento de datos biométricos ha desencadenado una proliferación de aplicaciones prácticas, marcando un impacto significativo en diversos sectores. A continuación, trataremos de, brevemente, destacar algunos casos específicos de implementaciones exitosas en áreas clave, resaltando tanto los beneficios tangibles como los riesgos asociados.

Uno de los sectores más prominentes que ha experimentado la influencia de la IA en datos biométricos es el de la seguridad. La aplicación de reconocimiento facial y huellas dactilares ha mejorado la autenticación en sistemas de acceso, desde desbloqueo de dispositivos hasta control de acceso a instalaciones críticas. La IA permite una identificación más precisa y eficiente, fortaleciendo la seguridad en entornos sensibles.

En el ámbito de la salud, la IA ha encontrado aplicación en la identificación biométrica para garantizar la integridad del historial médico y la autenticación de pacientes. Sistemas biométricos basados en el reconocimiento de iris, huellas dactilares o incluso patrones de voz han mejorado la precisión y seguridad en el acceso a información médica sensible, contribuyendo a una atención médica más personalizada y segura.

La implementación de la IA en la gestión de identidad empresarial ha facilitado el control de accesos y la autenticación de empleados. El reconocimiento facial y otras formas de autenticación biométrica han simplificado los procesos de registro y asegurado la integridad de los sistemas de seguridad corporativos. Esto no solo optimiza la eficiencia, sino que también mitiga riesgos asociados con el acceso no autorizado.

Aunque las aplicaciones prácticas de la IA en datos biométricos ofrecen beneficios notables, también plantean desafíos y riesgos. La vulnerabilidad a ataques de manipulación de datos, la posibilidad de discriminación inherente a ciertos algoritmos, y la preocupación por la

privacidad son aspectos críticos que deben abordarse para garantizar un despliegue ético y seguro de estas tecnologías.

2.4. *Desafíos éticos y de privacidad en el uso y diseño de la IA con datos biométricos*

El análisis crítico de los desafíos éticos y de privacidad que emergen con la integración más profunda de la IA en el ámbito biométrico aborda casos específicos de controversias éticas, centrándose particularmente en el reconocimiento facial y otros métodos biométricos. Este análisis proporciona una visión matizada de las preocupaciones éticas y de privacidad que requieren una atención cuidadosa en el desarrollo y aplicación de sistemas biométricos impulsados por la IA. La convergencia entre la IA y los datos biométricos, si bien ha brindado avances significativos, plantea desafíos éticos y de privacidad que requieren una consideración cuidadosa y un enfoque equilibrado.

Uno de los desafíos éticos más prominentes radica en la presencia de sesgos y discriminación en los sistemas biométricos impulsados por la IA. Estos sistemas pueden exhibir sesgos inherentes a los conjuntos de datos utilizados para su entrenamiento, lo que puede resultar en identificaciones incorrectas y discriminación, especialmente hacia grupos étnicos minoritarios. La necesidad de abordar estos sesgos para garantizar la equidad y evitar consecuencias discriminatorias se presenta como un imperativo ético (Cotino 2023a; Díaz Lima 2023).

La recopilación masiva de datos biométricos plantea interrogantes éticos en relación con el consentimiento informado y la autonomía del individuo. La falta de comprensión completa sobre cómo se utilizarán y compartirán estos datos, así como la posibilidad de usos no autorizados, plantea preocupaciones sobre la transparencia y el control del individuo sobre su información biométrica. De este modo, garantizar un proceso de consentimiento claro y transparente se erige como un principio ético fundamental.

La seguridad de los datos biométricos frente a amenazas y ataques cibernéticos constituye otro desafío ético crucial. La posibilidad de manipulación o robo de datos biométricos plantea riesgos significativos para la privacidad y la seguridad de los individuos. Se requieren medidas rigurosas para salvaguardar la integridad de estos datos y mitigar las amenazas potenciales.

Asimismo, la ausencia de un marco regulatorio robusto y la asignación clara de responsabilidades éticas en el uso de la IA con

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 341-374
https://doi.org/10.18543/djhr.3199 • http://djhr.revistas.deusto.es/

datos biométricos son desafíos adicionales. La falta de normativas claras puede dar lugar a prácticas no éticas o incluso ilegales en la recopilación y tratamiento de datos biométricos. Establecer un marco regulatorio sólido y fomentar la responsabilidad ética en todas las fases de desarrollo y aplicación de estas tecnologías se presenta como una necesidad imperante.

El uso de datos biométricos en el ámbito jurídico y penal plantea importantes retos y consideraciones éticas, como se discute en diversas investigaciones recientes (Etxeberria Guridi et al. 2023; Flórez y Camelo 2023). Estas tecnologías no solo afectan la privacidad de los individuos, sino que también tienen implicaciones legales significativas (Garriga et al. 2023; Garrós 2021). La discriminación algorítmica y su impacto en la dignidad de la persona y los derechos humanos es otro aspecto crucial (Iturmendi 2023).

3. **Recopilación y almacenamiento de datos biométricos a gran escala**

La recopilación masiva de datos biométricos plantea desafíos significativos en términos de privacidad y seguridad. Las organizaciones deben asegurar que los datos se almacenen de manera segura y se utilicen de manera ética (Bestard 2021) La recopilación de datos biométricos a gran escala involucra la captura y análisis de un volumen masivo de información única para cada individuo. Esto incluye, entre otros, el reconocimiento facial, huellas dactilares y patrones de voz. La complejidad radica en la variedad de fuentes y métodos de recopilación, desde sistemas de videovigilancia hasta dispositivos móviles, lo que exige una atención meticulosa a la precisión y la integridad de los datos.

La escala masiva de la recopilación de datos biométricos plantea cuestiones éticas fundamentales. La obtención de datos sin el conocimiento o el consentimiento informado de los individuos puede comprometer la privacidad o la autonomía. La transparencia en los procesos de recopilación y el respeto por los derechos individuales se tornan imperativos éticos en este contexto. El uso de IA en el reconocimiento facial y otros sistemas biométricos ha generado preocupaciones sobre la invasión de la privacidad, la vigilancia masiva y la posibilidad de errores y sesgos en los algoritmos (Castellanos 2023)

El almacenamiento seguro de datos biométricos es esencial para mitigar riesgos asociados con la seguridad y la privacidad. La vulnerabilidad de estos datos ante amenazas cibernéticas exige

medidas robustas de seguridad, como cifrado avanzado y protocolos de acceso controlado. Además, se debe garantizar la anonimización efectiva para proteger la identidad de los individuos, minimizando así el riesgo de uso indebido. Asimismo, la retención y eliminación de datos biométricos plantea desafíos éticos sobre la duración justificada y necesaria de la retención. Establecer políticas claras que rijan la retención y el período de conservación es esencial para evitar la acumulación innecesaria de información y garantizar la gestión ética de los datos biométricos a lo largo del tiempo (Flórez y Camelo 2023; Sempere 2020).

La ausencia de un marco regulatorio sólido y la falta de principios éticos claros en la recopilación y almacenamiento de datos biométricos pueden generar prácticas inconsistentes y riesgos para los individuos. Establecer directrices éticas y reglamentaciones que guíen la gestión de datos biométricos a gran escala es esencial para garantizar una práctica ética y legal en este ámbito. A este respecto, debemos destacar el cambio significativo que introduce el nuevo Reglamento de IA (RIA) y que posteriormente desarrollaremos. Asimismo, se analizará la relevancia jurídica y regulatoria, evaluando la adecuación de los marcos legales existentes para abordar los desafíos planteados por la combinación de IA y datos biométricos (Razquin 2022; Romano 2023).

En el mundo democrático, el uso de sistemas biométricos de identificación ha generado numerosos conflictos jurisdiccionales, destacando experiencias en el Reino Unido, Alemania, Países Bajos, Italia, Suecia, Buenos Aires, Brasil y España. Se han implementado proyectos polémicos, como el *AFR Locate* en el Reino Unido[7] y sistemas biométricos en eventos en Países Bajos. Asimismo, han surgido controversias legales y éticas en Alemania, donde el Bundesverfassunggericht declaró la inconstitucionalidad de dos normas que permitían el uso de sistemas automatizados en el ámbito policial (Cotino 2023b).

En Buenos Aires un sistema de cámaras establecido con el objetivo de garantizar la seguridad, identificó erróneamente a personas por lo que un tribunal suspendió su uso[8], mientras que, en Brasil, un juzgado ordenó la suspensión del uso de un sistema de control biométrico

[7] El once de agosto de 2020 una *High Court* del Reino Unido declaró la ilegalidad, por ausencia de transparencia y eficacia, de un sistema de reconocimiento facial empleado por la Policía de Gales del Sur. Véase: extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.judiciary.uk/wpcontent/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

[8] Véase: https://www.accessnow.org/buenos-aires-y-sao-paulo-suspenden-reconocimiento-facial.

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 341-374
https://doi.org/10.18543/djhr.3199 • http://djhr.revistas.deusto.es/

implementado por la empresa ViaQuatro, concesionaria del metro de Sao Paulo[9]. En España, el uso de sistemas biométricos en el ámbito privado ha generado conflictos legales, con sanciones a empresas como Mercadona[10]. Además, se menciona la aplicación de sistemas biométricos en el ámbito educativo y privado. Por último, sirva como ejemplo, y probablemente como advertencia de los desafíos a los que nos enfrentamos, el uso de sistemas de reconocimiento facial establecido recientemente por el Gobierno iraní en orden a controlar el uso del velo incluso cuando las mujeres se encuentran dentro de su vehículo (Harari 2024, 296) o los sistemas de reconocimiento facial que incorporan IA en China (Han 2020).

Se destaca que, más allá de la identificación, los sistemas biométricos inteligentes permiten el reconocimiento de emociones y la evaluación de personalidades. La Comisión Europea financió un proyecto, *Intelligent Portable Control System* (iBorderCtrlla)[11], con el objeto de aplicar la IA a los ámbitos de la migración y el asilo que generó encontradas reacciones en la sociedad civil y en la doctrina más autorizada, dado el alto grado de afectación a un buen número de derechos fundamentales. Grandes colosos empresariales, como Microsoft y Meta-Facebook, han retirado o modificado sus sistemas de reconocimiento facial y biométrico en respuesta a preocupaciones éticas. Aunque estos casos son significativos en el mundo democrático, se plantea la incertidumbre sobre el uso de sistemas biométricos en contextos más vinculados a la defensa y seguridad nacional, especialmente en China.

4. **Desafíos éticos en la aplicación de la IA**

La presencia de sesgos en los algoritmos de IA, especialmente aquellos entrenados en conjuntos de datos sesgados, puede generar discriminación. Esto se traduce en decisiones y recomendaciones que pueden tener consecuencias perjudiciales para ciertos grupos étnicos, de género o socioeconómicos. Abordar estos sesgos y garantizar la equidad en la aplicación de la IA son imperativos éticos.

Por otro lado, la opacidad en el funcionamiento interno de algunos modelos de IA plantea desafíos éticos relacionados con la falta de

[9] Véase: https://www.accessnow.org/press-release/sao-paulo-tribunal-prohibe-camaras-de-reconocimiento-facial-en-el-metro/.

[10] Procedimiento PS/00120/2021 de la AEPD, de 27 de julio de 2021.

[11] Véase: https://www.iborderctrl.eu/.

transparencia y explicabilidad. La dificultad para comprender cómo toma decisiones un sistema de IA puede socavar la confianza de los usuarios y dificultar la rendición de cuentas. Establecer prácticas transparentes y asegurar la explicabilidad de los modelos son aspectos clave para abordar este desafío.

Asimismo, la recopilación masiva de datos para entrenar modelos de IA presenta preocupaciones éticas significativas en términos de privacidad y seguridad. La posibilidad de identificar patrones sensibles en datos personales y la amenaza de brechas de seguridad plantean riesgos para la privacidad individual. Garantizar prácticas de manejo de datos éticas y protocolos de seguridad robustos es esencial para proteger la información personal.

La automatización impulsada por la IA tiene el potencial de alterar significativamente el panorama laboral, lo que genera desafíos éticos relacionados con el desempleo y los cambios socioeconómicos. La necesidad de reentrenamiento y adaptación de las habilidades laborales se convierte en un imperativo ético para mitigar los impactos negativos en los trabajadores afectados.

Definir la responsabilidad y establecer mecanismos efectivos de rendición de cuentas en el desarrollo y aplicación de sistemas de IA es un desafío ético clave. En situaciones donde los sistemas de IA toman decisiones críticas, la asignación clara de responsabilidades se vuelve esencial para abordar posibles consecuencias adversas y garantizar una toma de decisiones ética.

Por último, el uso de IA en contextos militares plantea preocupaciones éticas sobre la potencial falta de control humano, la escalada de conflictos y el impacto desigual en regiones y poblaciones. Abordar estos desafíos implica establecer límites éticos claros en el desarrollo y aplicación de tecnologías de IA en el ámbito militar.

5. **Consideraciones jurídicas y marco regulatorio**

La legislación en torno a la IA y los datos biométricos está en constante evolución. Es crucial que las leyes sean actualizadas para proteger adecuadamente los derechos de los individuos sin sofocar la innovación tecnológica (Castellanos 2023). La recopilación y procesamiento de grandes cantidades de datos en la aplicación de la IA requieren un estricto cumplimiento de las leyes de protección de datos y privacidad. El marco regulatorio debe establecer principios claros sobre cómo se pueden recopilar, almacenar y utilizar los datos para garantizar que se respeten los derechos fundamentales de privacidad de los individuos.

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 341-374
https://doi.org/10.18543/djhr.3199 • http://djhr.revistas.deusto.es/

Las leyes y regulaciones deben abordar la necesidad de transparencia y explicabilidad en los sistemas de IA. Esto implica la obligación de que las organizaciones proporcionen información clara sobre cómo funcionan sus algoritmos, especialmente en casos donde las decisiones afectan a los individuos. La capacidad de entender y cuestionar las decisiones de la IA es fundamental para la rendición de cuentas.

Establecer la responsabilidad legal en casos de decisiones erróneas o consecuencias adversas causadas por sistemas de IA es asimismo esencial. El marco regulatorio debe definir claramente quién es responsable en diferentes fases del ciclo de vida de la IA, ya sea en el diseño, entrenamiento o implementación. Además, se deben establecer mecanismos para la rendición de cuentas en situaciones donde los sistemas de IA toman decisiones cruciales.

Las leyes y regulaciones deben abordar los aspectos de seguridad cibernética en el contexto de la IA. Esto implica establecer estándares de seguridad para proteger los sistemas de IA contra amenazas y ataques cibernéticos. La integridad y la confidencialidad de los datos procesados por sistemas de IA deben ser una prioridad legal. Las normas deben también abordar la discriminación y los sesgos en los algoritmos de IA. Esto implica la implementación de medidas para garantizar que los sistemas de IA no perpetúen o amplifiquen sesgos existentes en la sociedad. La prohibición de discriminación injusta basada en raza, género u otras características protegidas debe ser una consideración central.

El marco legal debe abordar cuestiones relacionadas con la propiedad intelectual y los derechos de autor en el desarrollo de la IA. Esto incluye la definición de la propiedad de los modelos de IA, algoritmos y resultados generados por sistemas de IA, así como la protección de los derechos de los desarrolladores y creadores involucrados en proyectos de IA. Por otro lado, las leyes y regulaciones deben incluir disposiciones éticas para guiar la investigación y el desarrollo de la IA. Esto implica establecer límites éticos claros en la experimentación y el uso de datos, así como la consideración de posibles impactos éticos en la sociedad. Este análisis destaca la importancia de un marco regulatorio integral que aborde las complejidades jurídicas asociadas con la aplicación de la IA, asegurando así un desarrollo ético, responsable y conforme a los principios legales fundamentales.

La literatura existente muestra una diversidad de enfoques y regulaciones en distintos países, lo cual se refleja en el análisis comparativo de Flórez y Camelo (2023) sobre las tecnologías de

reconocimiento facial en Colombia. Además, los aspectos técnicos y éticos del tratamiento de datos biométricos se han debatido ampliamente en Europa (Garrós 2021). También se ha destacado la necesidad de abordar la discriminación algorítmica en estos contextos (Iturmendi 2023)

A nivel europeo y en el momento actual, son escasas las referencias explícitas que encontramos respecto al tratamiento masivo de datos biométricos, destacando el Reglamento (CE) n. 444/2009 del Parlamento Europeo y del Consejo, de 6 de mayo de 2009, por el que se modifica el Reglamento (CE) n. 2252/2004 del Consejo sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros; el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD); la Decisión de Ejecución (UE) 2023/1795 de la Comisión de 10 de julio de 2023 relativa a la adecuación del nivel de protección de los datos personales en el Marco de Privacidad de Datos UE-EE.UU. con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo [notificada con el número C(2023) 4745] y el Reglamento (UE) 2022/991 del Parlamento Europeo y del Consejo, de 8 de junio de 2022, por el que se modifica el Reglamento (UE) 2016/794 en lo que se refiere a la cooperación de Europol con entidades privadas, el tratamiento de datos personales por Europol en apoyo de investigaciones penales y el papel de Europol en materia de investigación e innovación. En cuanto a la regulación nacional, debemos destacar la Resolución de 6 de abril de 2016, del Servicio Público de Empleo Estatal, por la que se aprueba el sistema de firma electrónica mediante captura de firma digitalizada con datos biométricos para relacionarse presencialmente con el Servicio Público de Empleo Estatal; la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados, y la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 341-374
https://doi.org/10.18543/djhr.3199 • http://djhr.revistas.deusto.es/

6. **Preocupaciones sobre sesgos y su impacto en los derechos fundamentales**

La presencia de sesgos en sistemas de IA plantea inquietudes significativas, especialmente en relación con la posible afectación de los derechos fundamentales de los individuos. El uso diversificado de tecnologías biométricas, especialmente el reconocimiento facial, tiene el potencial de afectar prácticamente todos los derechos fundamentales de las personas (Sebé y Santilari 2022; Garrido 2023). La Agencia de la Unión Europea para los Derechos Fundamentales (FRA) destaca la implicación de derechos como la dignidad humana, el respeto a la vida privada, la protección de datos personales, la no discriminación, los derechos del niño y de los mayores, 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.

La sociedad democrática se ve amenazada por el control constante y la posible identificación en situaciones cotidianas, desde comprar pan hasta participar en manifestaciones, actividades políticas o religiosas, centros de salud, asistencia social, educativos, entre otros. El RIA reconoce que estos sistemas pueden generar una sensación de vigilancia constante, disuadiendo indirectamente el ejercicio de la libertad de reunión y otros derechos fundamentales. Además, estos sistemas ponen en entredicho la presunción de inocencia al considerar a todos como sospechosos, dificultando la defensa de aquellos que resultan positivos en estas estructuras. Los errores, sesgos y discriminaciones, aunque inadvertidos, son posibles dado que estos sistemas son probabilísticos y aplicados a grandes poblaciones. Los derechos asociados a la privacidad, intimidad y protección de datos se ven particularmente afectados, ya que la simple captación de datos, incluso si se eliminan inmediatamente después de su comparación, resulta impactante. La utilización y conservación posterior de estos datos procesados intensifican la afectación a estos derechos y aumentan el riesgo de un uso indebido.

El reconocimiento facial y estas tecnologías constituyen una amenaza directa a los derechos fundamentales, y su impacto va más allá de afectaciones individuales, alcanzando a la sociedad democrática en su conjunto. La respuesta jurídica no puede limitarse a aplicar técnicas específicas para afectaciones individuales; se requieren nuevas técnicas de cumplimiento normativo, responsabilidad reactiva, análisis multirriesgos y protección colectiva de derechos para abordar de manera integral estos desafíos éticos y legales. El sesgo en los sistemas

de IA puede llevar a decisiones injustas y discriminatorias. Es fundamental que los desarrolladores y reguladores trabajen juntos para minimizar estos riesgos (Castellanos 2024). La experiencia demuestra que la existencia de sesgos en los algoritmos de IA puede resultar en discriminación injusta hacia ciertos grupos. Esto podría manifestarse en decisiones discriminatorias en áreas como el empleo, la vivienda, o el crédito, entre otros. La discriminación basada en sesgos en sistemas de IA amenaza directamente el derecho a la igualdad y no discriminación, fundamentales en los derechos humanos.

Los sesgos en los sistemas de IA pueden afectar el derecho a la privacidad al influir en la recopilación y procesamiento de datos de manera desigual. Si los algoritmos muestran sesgos en la identificación de patrones o en la toma de decisiones, esto puede traducirse en un tratamiento diferenciado y, en última instancia, en la vulneración del derecho a la privacidad.

La aplicación de sistemas de IA en procesos legales, como la toma de decisiones judiciales o la evaluación de riesgos penales, podría verse afectada por sesgos inherentes. Esto plantea preocupaciones sobre el derecho a un juicio justo y a la igualdad ante la ley, ya que las decisiones automatizadas pueden favorecer o perjudicar a ciertos grupos de manera no equitativa.

Si los algoritmos de IA muestran sesgos, el acceso a oportunidades fundamentales como empleo, educación y atención médica puede volverse inequitativo. Esto amenaza el derecho a la igualdad de oportunidades, ya que las decisiones basadas en sesgos pueden perpetuar desigualdades existentes y limitar el acceso a recursos esenciales.

Los sesgos en los algoritmos que determinan qué contenido se muestra a los usuarios pueden tener un impacto en la libertad de expresión e información. Si los usuarios son expuestos a información sesgada o limitada, esto puede afectar su capacidad para formar opiniones informadas y participar plenamente en el discurso público.

En entornos laborales donde se utilizan sistemas de IA para la toma de decisiones relacionadas con el empleo, los sesgos pueden influir en la contratación, la promoción y la evaluación del desempeño. Esto plantea preocupaciones sobre el derecho a un ambiente laboral justo y la igualdad en el trato en el ámbito laboral.

Abordar las preocupaciones sobre sesgos en la IA se convierte en una prioridad crucial para salvaguardar los derechos fundamentales y garantizar que la aplicación de estas tecnologías sea justa, equitativa y respetuosa con los principios fundamentales de la normativa que reconoce y garantiza los derechos humanos.

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 341-374
https://doi.org/10.18543/djhr.3199 • http://djhr.revistas.deusto.es/

7. **Especial referencia a los sistemas biométricos de categorización, reconocimiento de emociones y evaluación de la personalidad**

En el ámbito de las tecnologías biométricas e IA, la lectura de datos faciales, indicadores sanguíneos, pulsación de teclas y otros elementos está adquiriendo una relevancia creciente. Aunque estos datos son universales y singularizan a la persona, su uso se ha expandido más allá de la mera identificación. En la propuesta del RIA de abril de 2021, se define un "sistema de reconocimiento de emociones" como un sistema de IA destinado a identificar o inferir emociones a partir de datos biométricos. Se sugiere que esta definición debería incluir los "pensamientos" a través de interfaces cerebro-ordenador. Además, se introduce el concepto de "sistema de categorización biométrica", destinado a asignar a las personas a categorías específicas, como sexo, edad, color de pelo, entre otros, basándose en datos biométricos.

Estos sistemas, según la propuesta, permiten una evaluación a gran escala que se asemeja a la capacidad de un psicólogo para interpretar emociones, detectar veracidad en manifestaciones y prever comportamientos futuros. Además, posibilitan la rápida categorización de conjuntos de personas con afinidades específicas. A lo largo de los años, se han empleado estos sistemas en el control de fronteras, como el Agente Virtual Automatizado para la Evaluación de la Verdad en Tiempo Real (AVATAR) en los EE.UU. Asimismo, estos sistemas plantean cuestiones éticas adicionales debido a su capacidad para inferir características personales profundas a partir de datos biométricos, lo que podría ser explotado de manera indebida (Díaz 2023).

A pesar de sus beneficios potenciales, se han identificado preocupaciones (Andúgar 2023; Castellanos 2023), y varias instituciones han señalado el peligro que representan estos sistemas biométricos inteligentes. Empresas como Microsoft y Meta-Facebook han tenido en cuenta estas inquietudes, retirando o modificando sus sistemas de reconocimiento facial y de emociones. Aunque estos sistemas generan inquietudes, la regulación actual, como el RGPD y el RIA, presenta limitadas precauciones y garantías, especialmente cuando los datos biométricos no se utilizan con fines de identificación. La regulación futura y las llamadas a la prohibición o regulación más estricta por parte de importantes instituciones subrayan la necesidad de abordar de manera más integral estos desafíos éticos y legales asociados con la IA y las tecnologías biométricas.

8. **Implicaciones de privacidad en el escaneo de iris: análisis del caso worldcoin**

El escaneo de iris ha emergido como una tecnología biométrica innovadora que permite la identificación precisa de individuos mediante el análisis de los patrones únicos presentes en el iris del ojo. Esta tecnología ha encontrado una amplia gama de aplicaciones, desde el control de acceso en instalaciones de alta seguridad hasta la autenticación en dispositivos móviles. Sin embargo, a medida que el escaneo de iris se integra cada vez más en nuestras vidas cotidianas, también surgen importantes interrogantes sobre la privacidad y la protección de datos personales. En este contexto, es crucial entender cómo la regulación de la UE, como el RGPD, maneja la protección de estos datos sensibles (González Calvo 2022).

Worldcoin ha sido objeto de controversia por su método de escaneo del iris, que muchos consideran una invasión significativa de la privacidad. Este caso será examinado para ilustrar los desafíos prácticos y éticos en la implementación de tecnologías biométricas (Díaz 2023). El escaneo del iris como método de identificación implica el tratamiento de datos biométricos, que son considerados datos personales y están sujetos a regulaciones estrictas en España para proteger la privacidad y los derechos de los individuos. Las leyes y regulaciones aplicables, como la Ley Orgánica 7/2021, establecen condiciones específicas para el tratamiento, uso y protección de estos datos, asegurando que cualquier uso del escaneo del iris cumpla con los principios de protección de datos personales y respete los derechos fundamentales. El uso del escaneo de iris para identificar a las personas está permitido en España bajo ciertas condiciones específicas, principalmente en contextos relacionados con la aplicación de la ley. Además, el escaneo de iris es reconocido como un método efectivo y común de identificación biométrica en la Unión Europea, lo que refuerza su relevancia y adopción en diversos países miembros.

Debemos destacar que el escaneo de iris representa un hito significativo en el campo de la tecnología biométrica debido a su capacidad para proporcionar una identificación precisa y única de individuos basada en características biológicas internas del cuerpo humano. A diferencia de otras formas de autenticación, como contraseñas o tarjetas de identificación, que pueden ser olvidadas, robadas o falsificadas, el escaneo de iris ofrece un nivel de seguridad y fiabilidad excepcionales. Una de las razones clave de la importancia del escaneo de iris en la tecnología biométrica radica en la singularidad y estabilidad del iris humano. Cada iris presenta patrones únicos que se

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 341-374
https://doi.org/10.18543/djhr.3199 • http://djhr.revistas.deusto.es/

desarrollan durante la gestación y permanecen prácticamente inalterados a lo largo de la vida de un individuo. Esta característica inherente hace que el escaneo de iris sea altamente confiable para la identificación biométrica, lo que lo convierte en una opción atractiva para una variedad de aplicaciones críticas, como la seguridad nacional, el control de acceso a instalaciones sensibles y la autenticación en sistemas de información.

Otra razón importante es la rapidez y facilidad de uso del escaneo de iris. A diferencia de otros métodos biométricos que pueden requerir interacciones físicas más complejas, como la huella dactilar o el reconocimiento facial, el escaneo de iris puede realizarse de manera rápida y sin contacto directo, lo que lo convierte en una opción conveniente para una amplia gama de situaciones y entornos. Además, el escaneo de iris ofrece un alto nivel de precisión y resistencia a la falsificación. Los patrones del iris son extremadamente detallados y difíciles de reproducir, lo que hace que sea extremadamente difícil para los impostores engañar al sistema. Esto lo convierte en una herramienta valiosa para combatir la suplantación de identidad y otros tipos de fraude.

En definitiva, el escaneo de iris juega un papel fundamental en la tecnología biométrica al ofrecer una combinación única de precisión, seguridad y facilidad de uso. Su capacidad para proporcionar identificaciones confiables y seguras lo convierte en una herramienta invaluable en una amplia variedad de aplicaciones, desde la seguridad nacional hasta la gestión de identidad en entornos empresariales y gubernamentales.

8.1. *Regulación*

La Ley Orgánica 3/2018[12] y la Ley Orgánica 7/2021[13] son fundamentales para entender el tratamiento de datos biométricos, como el escaneo del iris, en España. La Ley Orgánica 3/2018 establece que la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental, garantizando a los

[12] Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales. (Ley Orgánica 3/2018, de 5 de diciembre) BOE-A-2018-16673

[13] Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. (Ley Orgánica 7/2021, de 26 de mayo) BOE-A-2021-8806

individuos el control sobre sus datos personales. Esta ley se centra en salvaguardar la privacidad y los derechos de los ciudadanos en el ámbito digital y biométrico. La Ley Orgánica 7/2021 especifica que los datos biométricos se consideran una categoría especial de datos personales cuando se utilizan para identificar de manera unívoca a una persona. Esto implica que el tratamiento de estos datos está sujeto a regulaciones estrictas para proteger la privacidad de los individuos y asegurar que se manejen de manera ética y legal. Además, el Artículo 18.4 de la Constitución Española establece límites al uso de la informática para proteger la intimidad personal, lo cual es particularmente relevante en el contexto del escaneo de iris.

La Ley Orgánica 7/2021, de 26 de mayo, sobre la protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, establece que los datos biométricos, como el escaneo de iris, pueden ser utilizados legalmente para identificar de manera unívoca a una persona física en contextos específicos de aplicación de la ley. Esta ley, de ámbito nacional, tiene preeminencia sobre otras normativas autonómicas o más antiguas en caso de conflicto, dada su jerarquía y actualidad.

Normativa que, en conjunto, proporciona un marco robusto para el tratamiento de datos biométricos, asegurando que su uso se realice de manera responsable y en consonancia con los derechos fundamentales de los individuos. La regulación estricta y clara es esencial para equilibrar los beneficios del escaneo de iris como una herramienta de seguridad y autenticación, con la necesidad de proteger la privacidad y otros derechos fundamentales en una sociedad cada vez más digitalizada.

La Resolución n. PS-00120-2021 de la Agencia Española de Protección de Datos distingue entre identificación biométrica remota y autenticación biométrica, aclarando que la identificación biométrica remota, que puede incluir el escaneo del iris, debe realizarse bajo condiciones que respeten la normativa de protección de datos y los derechos individuales. Esta resolución establece directrices claras para el uso de tecnologías biométricas, garantizando que su implementación se alinee con las leyes de privacidad y protección de datos vigentes, asegurando así la protección de los derechos fundamentales de los individuos.

Los materiales secundarios, como los principios del Reglamento 2016/679/UE (RGPD) y las claves jurídicas sobre el registro de jornada, proporcionan contexto adicional sobre cómo se deben manejar los datos biométricos en diferentes contextos, como el laboral, y subrayan

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 341-374
https://doi.org/10.18543/djhr.3199 • http://djhr.revistas.deusto.es/

la necesidad de garantías adecuadas para proteger los derechos fundamentales al utilizar tecnologías como el escaneo del iris. Específicamente, el documento titulado *Los sistemas biométricos de reconocimiento facial en la Unión Europea en el marco del desarrollo de la Inteligencia Artificial*, de fecha 1 de junio de 2023, destaca que el escaneo de iris es un método común y altamente efectivo para la identificación biométrica. Este documento subraya la eficacia casi absoluta del uso del iris como dato biométrico para acceder a lugares o dispositivos, apoyando la proposición de su uso extendido en contextos donde se requiere una identificación segura y precisa. Estos materiales complementarios refuerzan la importancia de aplicar regulaciones estrictas y garantías adecuadas para proteger la privacidad y los derechos de los individuos en el uso de tecnologías biométricas avanzadas.

La Sentencia 119/2022 del Tribunal Constitucional[14] es crucial en el marco legal español, ya que confirma que los datos biométricos, incluido el escaneo del iris, son considerados datos personales y, por lo tanto, están protegidos bajo la legislación de protección de datos personales en España. Esta sentencia no solo reafirma la clasificación de los datos biométricos como datos personales, sino que también subraya la obligación de cumplir con todas las normativas de protección de datos al tratarlos. El Tribunal Constitucional, en esta sentencia, enfatiza que el tratamiento de datos biométricos debe realizarse en estricto cumplimiento con la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) y el RGPD. Esto incluye principios fundamentales como la licitud, lealtad y transparencia, la limitación de la finalidad, la minimización de datos, la exactitud, la limitación del plazo de conservación, la integridad y confidencialidad, y la responsabilidad proactiva.

La sentencia también aborda la necesidad de un consentimiento explícito e informado por parte de los individuos cuyo iris se va a escanear, así como la obligación de implementar medidas de seguridad adecuadas para proteger estos datos sensibles de accesos no

[14] Pleno Sentencia 119/2022, de 29 de septiembre de 2022. Recurso de amparo 7211-2021. Promovido por Saltoki Araba, S.A., en relación con las resoluciones dictadas por las salas de lo social del Tribunal Supremo y del Tribunal Superior de Justicia del País Vasco en proceso por despido. Vulneración de los derechos a la utilización de los medios de prueba pertinentes y a un proceso con todas las garantías, en conexión con el derecho a la tutela judicial efectiva: resoluciones judiciales que, sin un verdadero motivo jurídico, declaran improcedente la prueba videográfica aportada por la empresa y admitida en la instancia. Voto particular. BOE n. 262, de 1 de noviembre de 2022, páginas 149412 a 149442.

autorizados y usos indebidos. Esta protección se extiende a todos los ámbitos donde se pueda utilizar el escaneo de iris, incluyendo tanto el sector público como el privado. Además, la STC 119/2022 recalca la importancia de que las organizaciones que manejen datos biométricos establezcan políticas claras y transparentes sobre su tratamiento, incluyendo información detallada sobre los fines del procesamiento, los derechos de los individuos respecto a sus datos, y los procedimientos para ejercer estos derechos. Esto refuerza la interpretación de que cualquier tratamiento de datos biométricos debe ser riguroso y estar alineado con las mejores prácticas de protección de datos.

8.2. *Limitaciones*

Las principales limitaciones al uso del escaneo del iris para identificación incluyen la necesidad de cumplir con regulaciones estrictas de protección de datos, garantizar el consentimiento informado de los individuos y proporcionar medidas de seguridad adecuadas para proteger los datos personales. La legislación española, reforzada por la STC 119/2022, subraya la importancia de estos requisitos para asegurar que los datos biométricos se manejen de manera ética y legal. Además, cualquier uso de esta tecnología debe considerar el contexto específico y las regulaciones aplicables, como las que se aplican en contextos laborales o en la Comunidad Valenciana para los establecimientos de juego. Por ejemplo, en el ámbito laboral, es crucial que el uso del escaneo de iris cumpla con las regulaciones sobre protección de datos y derechos laborales, garantizando que no se vulneren los derechos de los empleados.

Aunque el escaneo de iris es legalmente permitido en contextos específicos de aplicación de la ley, su uso podría estar sujeto a restricciones en otros contextos, especialmente en relación con la protección de datos personales y la privacidad individual. La legislación sobre protección de datos personales puede imponer limitaciones en el tratamiento de datos biométricos, como el escaneo de iris, fuera de los contextos específicamente amparados por la ley. Por ejemplo, fuera del ámbito de la seguridad y la aplicación de la ley, cualquier uso de tecnologías de identificación biométrica debe cumplir con los principios de proporcionalidad, necesidad y minimización de datos, garantizando que solo se recopilen y procesen los datos estrictamente necesarios para el propósito específico.

Además, el uso de tecnologías biométricas debe estar alineado con los derechos fundamentales de los individuos, asegurando que

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 341-374
https://doi.org/10.18543/djhr.3199 • http://djhr.revistas.deusto.es/

cualquier implementación respete la privacidad y no conduzca a un uso excesivo o indebido de los datos personales. Las organizaciones deben ser transparentes en sus prácticas de manejo de datos biométricos y proporcionar a los individuos información clara sobre cómo se utilizarán sus datos, las medidas de seguridad implementadas y los derechos que tienen para controlar el uso de su información personal. Estas limitaciones y requisitos reflejan la necesidad de un enfoque cuidadoso y bien regulado en el uso del escaneo de iris, asegurando que esta tecnología se utilice de manera responsable y en consonancia con las normativas vigentes, protegiendo así los derechos y la privacidad de los individuos en un entorno cada vez más digitalizado.

8.3. *Fundamentos del escaneo de iris*

El escaneo de iris es una tecnología biométrica que utiliza patrones únicos en el iris del ojo para identificar a las personas. El iris es la parte coloreada del ojo que rodea la pupila y tiene patrones complejos que son únicos para cada individuo. Estos patrones se forman en los primeros años de vida y permanecen prácticamente inalterados a lo largo del tiempo, lo que los convierte en una característica ideal para la identificación biométrica. El proceso de escaneo de iris implica capturar una imagen de alta resolución del iris utilizando una cámara especializada. Esta imagen se procesa mediante algoritmos que extraen características específicas del patrón del iris, creando una plantilla biométrica. Esta plantilla se almacena en una base de datos y se utiliza para comparar con futuras imágenes del iris para verificar la identidad de la persona.

El escaneo de iris tiene una amplia gama de aplicaciones debido a su alta precisión y fiabilidad. En el sector de la seguridad, se utiliza en aeropuertos y fronteras para verificar la identidad de los viajeros y prevenir el uso de documentos falsificados. También se emplea en instalaciones de alta seguridad, como centrales nucleares y edificios gubernamentales, para controlar el acceso y garantizar que solo las personas autorizadas puedan entrar. Asimismo, en el ámbito financiero, algunas instituciones utilizan el escaneo de iris para autenticar a los clientes en cajeros automáticos y servicios bancarios en línea, proporcionando una capa adicional de seguridad. Además, en dispositivos móviles, el escaneo de iris se utiliza como una forma segura de desbloquear teléfonos y acceder a aplicaciones sensibles.

8.4. *Implicaciones de privacidad*

La recopilación y el almacenamiento de datos biométricos del iris plantean importantes cuestiones de privacidad. Dado que estos datos son extremadamente sensibles y únicos para cada individuo, su manejo requiere un cuidado especial. Las organizaciones deben asegurar que la recopilación de datos biométricos se realice con el consentimiento informado de los individuos y que estos datos se almacenen de manera segura para evitar accesos no autorizados y posibles filtraciones (Martínez Martínez 2020).

A pesar de la robustez del escaneo de iris, existen riesgos de seguridad y posibles vulnerabilidades. Los sistemas de escaneo de iris pueden ser objeto de ataques, como la falsificación de plantillas biométricas o la captura de imágenes de alta resolución sin el conocimiento del individuo. Es crucial implementar medidas de seguridad avanzadas, como el cifrado de datos biométricos y la detección de *liveness* (pruebas de vida), para mitigar estos riesgos y proteger la integridad de los datos biométricos.

El uso indebido de datos biométricos del iris puede tener graves consecuencias para la privacidad de los individuos. Si estos datos caen en manos equivocadas, pueden ser utilizados para el robo de identidad, seguimiento no autorizado y otras actividades malintencionadas. Además, la recopilación masiva de datos biométricos puede llevar a la creación de bases de datos que, si no se gestionan adecuadamente, pueden ser vulnerables a brechas de seguridad. Por este motivo, es fundamental que las organizaciones que utilicen escaneo de iris adopten políticas claras y transparentes sobre el manejo de datos biométricos, aseguren que se cumplan las normativas de protección de datos y proporcionen a los individuos información y control sobre el uso de sus datos personales. Esto ayudará a proteger la privacidad y los derechos fundamentales de los individuos en una era de creciente digitalización y dependencia de tecnologías biométricas.

8.5. *Desafíos éticos y legales*

Uno de los principales desafíos éticos en el uso del escaneo de iris es garantizar que los individuos otorguen su consentimiento informado de manera libre y voluntaria. Esto significa que las personas deben estar plenamente informadas sobre cómo se recopilarán, utilizarán y almacenarán sus datos biométricos, así como sobre sus derechos para acceder, rectificar y eliminar esta información. La

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 341-374
https://doi.org/10.18543/djhr.3199 • http://djhr.revistas.deusto.es/

autonomía del individuo debe ser respetada, permitiéndole tomar decisiones informadas sobre su participación en sistemas que utilizan escaneo de iris.

El tratamiento de datos biométricos está sujeto a estrictas normativas y regulaciones diseñadas para proteger la privacidad de los individuos. En la Unión Europea, el RGPD establece principios claros sobre el procesamiento de datos biométricos, incluyendo la necesidad de bases legales sólidas, como el consentimiento explícito o intereses legítimos claramente justificados. Además, la Ley Orgánica 3/2018 en España refuerza estas protecciones a nivel nacional, asegurando que cualquier uso de datos biométricos cumpla con los estándares legales más rigurosos.

Las organizaciones que recopilan y procesan datos biométricos del iris tienen la responsabilidad de implementar medidas adecuadas para proteger estos datos. Esto incluye la adopción de políticas de privacidad robustas, la formación de empleados en prácticas seguras de manejo de datos y la implementación de tecnologías avanzadas para prevenir accesos no autorizados. Las organizaciones deben ser transparentes en sus prácticas y ser responsables ante cualquier violación de privacidad o mal manejo de los datos biométricos.

8.6. *Estrategias de mitigación de riesgos*

Para minimizar el riesgo de violaciones de privacidad, las organizaciones deben adoptar un enfoque proactivo en la gestión de datos biométricos del iris. Esto incluye la realización de evaluaciones de impacto sobre la privacidad antes de implementar tecnologías de escaneo de iris, así como la revisión regular de las prácticas de manejo de datos para identificar y mitigar posibles riesgos.

Las buenas prácticas en la gestión de datos biométricos del iris incluyen la limitación de la recopilación de datos al mínimo necesario, el almacenamiento seguro de estos datos y la implementación de políticas claras sobre su uso y retención. Además, es crucial asegurar que los datos sean accesibles solo a personal autorizado y que se mantengan registros detallados de cualquier acceso o uso de los datos biométricos. Además, el uso de tecnologías de cifrado y anonimización es fundamental para proteger la privacidad de los usuarios cuyos datos biométricos se recopilan. El cifrado asegura que los datos sean ininteligibles para cualquier persona no autorizada que pueda acceder a ellos, mientras que la anonimización reduce el riesgo de que los datos puedan ser asociados con individuos específicos. Estas

tecnologías deben ser parte integral de cualquier sistema que maneje datos biométricos del iris.

8.7. *Consideraciones éticas y sociales*

Encontrar un equilibrio entre la necesidad de seguridad y la protección de la privacidad es un desafío constante en el uso del escaneo de iris. Si bien esta tecnología ofrece altos niveles de seguridad y precisión en la identificación, su implementación debe ser cuidadosamente gestionada para evitar invasiones de privacidad y garantizar que los derechos individuales no sean comprometidos.

El uso del escaneo de iris puede afectar la percepción de privacidad personal de los individuos. La sensación de estar constantemente vigilado y la intrusión en la vida personal pueden generar desconfianza y resistencia hacia esta tecnología. Es crucial abordar estas preocupaciones mediante la transparencia, la educación y la comunicación abierta sobre los beneficios y las medidas de protección asociadas con el escaneo de iris.

La utilización de datos biométricos del iris para fines diversos, más allá de la seguridad y la autenticación, plantea importantes cuestiones éticas. Esto incluye el uso de datos biométricos en el marketing, la investigación y otros ámbitos que pueden no estar claramente justificados desde una perspectiva de privacidad y derechos individuales. Las organizaciones deben considerar cuidadosamente los impactos éticos de sus prácticas y asegurar que cualquier uso de datos biométricos esté alineado con los valores y principios éticos aceptados.

8.8. *El proyecto Worldcoin*

La AEPD emitió una medida cautelar que prohíbe a Worldcoin continuar recopilando y tratando los datos biométricos del iris de los usuarios en España[15]. Esta medida implica que la empresa no puede

[15] Ref.: EXP202312448 Asunto: Acuerdo de adopción de medida provisional. Véase: https://www.aepd.es/documento/co-000297-2023-medida-provisional.pdf. La Sección Primera de la Sala de lo Contencioso – Administrativo de la Audiencia Nacional avaló, a través de auto dictado el 11 de marzo de 2024, el Acuerdo de la AEPD. Véase: https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Noticias-Judiciales/La-Audiencia-Nacional-avala-el-cese-cautelar-de-la-recopilacion-de-datos-a-traves-del-iris-de-Worldcoin-acordado-por-la-Agencia-de-Proteccion-de-datos.

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 341-374
https://doi.org/10.18543/djhr.3199 • http://djhr.revistas.deusto.es/

seguir operando en centros comerciales situados en territorio español, en los que se ofrecía intercambiar información del iris a cambio de criptomonedas WLD. La AEPD destaca en su acuerdo que el iris es un dato personal y biométrico que requiere una protección especial, señalando además que Worldcoin vulnera la normativa europea al no facilitar información adecuada a los usuarios, ni permitirles retirar su consentimiento o eliminar la información recopilada.

Worldcoin no exigía documentos de identidad a los usuarios y se comprometió a llevar a cabo únicamente el escaneo de mayores de edad, aunque ha quedado acreditado que también escaneó el iris de menores de edad. La medida cautelar de la AEPD puede extenderse por hasta tres meses, y se comparte con el Comité Europeo de Protección de Datos, dado que Worldcoin opera a nivel comunitario. La empresa enfrenta posibles multas de hasta el 4% de sus ingresos anuales si no cumple con la orden de la AEPD. En respuesta, el jefe de protección de datos de Worldcoin ha criticado la medida, acusando a la AEPD de difundir afirmaciones inexactas y eludir la ley de la UE.

El asunto que nos ocupa presenta varios aspectos relevantes en términos de protección de datos y cumplimiento normativo. Entre estos, podemos destacar los siguientes:

a) Protección de datos personales: La recopilación y tratamiento de datos biométricos, como el escaneo del iris, se considera una actividad especialmente sensible desde el punto de vista de la protección de datos personales. La normativa europea, en particular el RGPD, establece requisitos estrictos para el manejo de estos datos, incluyendo la necesidad de obtener un consentimiento informado y garantizar la seguridad y privacidad de la información.
b) Consentimiento informado y autonomía del individuo: Uno de los principales puntos de conflicto en el caso de Worldcoin es la falta de un consentimiento informado adecuado por parte de los usuarios. La ley exige que el consentimiento para el tratamiento de datos biométricos sea específico, informado y otorgado libremente. En este caso, la empresa ha sido acusada de no proporcionar información suficiente sobre el proceso de escaneo del iris y de no permitir a los usuarios retirar su consentimiento.
c) Derechos de los individuos y responsabilidad de las organizaciones: La normativa de protección de datos otorga importantes derechos a los individuos, incluido el derecho a la supresión de datos y a la privacidad. Las empresas, como Worldcoin, tienen la ineludible responsabilidad de respetar estos derechos y garantizar que el tratamiento de datos se realice de

manera legal y ética. La infracción de estas normas puede resultar en sanciones significativas, incluyendo multas.

Conclusiones y recomendaciones

Primera. La aplicación de la IA en el tratamiento de datos biométricos presenta desafíos éticos considerables, desde sesgos y discriminación hasta preocupaciones sobre la privacidad y la seguridad de los datos. Estos desafíos tienen implicaciones directas en los derechos fundamentales de los individuos, exigiendo una evaluación y abordaje ético y jurídico integral.

Segunda. La falta de transparencia en los algoritmos de IA y en la recopilación de datos biométricos plantea inquietudes significativas. Garantizar la transparencia y la explicabilidad en el desarrollo y aplicación de sistemas de IA es esencial para fomentar la confianza, facilitar la rendición de cuentas y permitir que los individuos comprendan cómo se toman las decisiones que los afectan.

Tercera. La ausencia de un marco regulatorio sólido contribuye a la incertidumbre ética y jurídica en el uso de la IA y datos biométricos. Se requiere una legislación clara y específica que aborde los desafíos identificados, establezca límites éticos y defina responsabilidades para garantizar un despliegue ético y respetuoso de estas tecnologías. Las investigaciones indican que es esencial desarrollar marcos regulatorios robustos y éticamente responsables para el uso de tecnologías biométricas, como se ha argumentado en varios estudios recientes (Garrós 2021). Esto garantizará no solo la protección de los derechos individuales sino también el uso seguro y eficaz de estas tecnologías en la sociedad moderna.

Cuarta. La preservación de derechos fundamentales, como la igualdad, la privacidad o la interdicción de la discriminación, debe ser prioritaria en el desarrollo y aplicación de sistemas de IA. Los sesgos y discriminación inherentes deben abordarse para evitar violaciones de derechos fundamentales y garantizar que estos sistemas beneficien a la sociedad en su conjunto.

Quinta. La evolución rápida de la tecnología exige una consideración ética continua en el desarrollo e implementación de sistemas de IA. Los diseñadores, desarrolladores y responsables de políticas deben comprometerse a evaluar y mitigar los impactos éticos a medida que surgen nuevas aplicaciones y desafíos.

Sexta. Debemos establecer políticas claras y transparentes sobre el uso de datos biométricos del iris, asegurando que los individuos

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 341-374
https://doi.org/10.18543/djhr.3199 • http://djhr.revistas.deusto.es/

comprendan cómo se recopilarán, utilizarán y protegerán sus datos. Obtener consentimiento informado de manera clara y comprensible, respetando la autonomía del individuo y sus derechos sobre sus datos personales. Garantizar el cumplimiento de normativas como el RGPD y la Ley Orgánica 3/2018, que establecen estándares estrictos para el tratamiento de datos biométricos y la protección de la privacidad.

Séptima. Implementar medidas de seguridad robustas, incluyendo tecnologías avanzadas de cifrado y anonimización, para proteger los datos biométricos del iris contra accesos no autorizados y posibles vulnerabilidades es una necesidad imperiosa en estos momentos. Además, debemos proporcionar formación continua a empleados y usuarios sobre las mejores prácticas en el manejo de datos biométricos, concienciándolos sobre la importancia de la privacidad y sus derechos respecto a sus datos personales.

Octava. Urge investigar y desarrollar técnicas avanzadas para mejorar la anonimización y el cifrado de datos biométricos, garantizando una protección efectiva de la privacidad. Evaluar el impacto social y ético del escaneo de iris en diferentes contextos, identificando posibles riesgos y beneficios, así como adaptar normativas para abordar los avances tecnológicos y los desafíos emergentes en la protección de datos biométricos.

Novena. Por último, subrayar que debemos fomentar una mayor colaboración interdisciplinaria entre expertos en tecnología, ética, derecho y políticas públicas. Esto permitirá anticipar mejor los riesgos emergentes en el uso de datos biométricos y la IA, y crear marcos adaptativos que se mantengan actualizados con los rápidos avances tecnológicos. Además, se deberían promover iniciativas educativas para el público en general, aumentando la conciencia sobre los derechos de privacidad y el impacto que las tecnologías biométricas pueden tener en su vida cotidiana, garantizando una adopción más responsable y ética a nivel global.

Podemos afirmar que el uso de la IA en el tratamiento de datos biométricos presenta oportunidades significativas, pero también plantea riesgos sustanciales para los derechos fundamentales y la equidad. Abordar estos desafíos requiere una colaboración integral entre expertos en ética, juristas, tecnólogos y responsables de políticas para desarrollar soluciones que equilibren la innovación con la protección de los derechos individuales y colectivos. Es imperativo que futuras investigaciones continúen explorando los impactos legales y sociales del uso de datos biométricos, con énfasis en la necesidad de regulaciones más claras y específicas. Además, es recomendable que se realicen estudios empíricos para evaluar la efectividad de las políticas actuales y su implementación práctica.

Bibliografía

Aliaga, Laura, y Mª Estrella Gutiérrez. 2020. «Reino Unido: Reconocimiento facial en lugares públicos realizado por Fuerzas y Cuerpos de Seguridad en el marco de la prevención e investigación de delitos. La visión del ICO». *La Ley privacidad* 3: 18.

Álvarez, Nelia, y David Sanz. 2021. «Advertencia de la Agencia Española de Protección de Datos con respecto a la utilización de técnicas de e-proctoring en la evaluación online por la UNIR». *La Ley privacidad* 10: 6.

Andúgar, Miguel Á. 2023. «Videovigilancia, control de accesos y datos biométricos». En *La protección de datos en el ámbito parlamentario: guía práctica*, editado por Esther de Alba, 201-219. Madrid: Asociación de Delegados y Delegadas de Protección de Datos de Parlamentos.

Arroyo, Alicia. 2022. «Vehículos autónomos, responsabilidad y seguro: Avances legislativos y perspectivas». *Revista de Derecho del Sistema Financiero: mercados, operadores y contratos* 3: 4.

Baz, Jesús. 2021. *Los nuevos derechos digitales laborales de las personas trabajadoras en España: vigilancia tecnificada, teletrabajo, inteligencia artificial, Big Data*. Madrid: Wolters Kluwer España.

Barona, Silvia. 2024. «Tecnología biométrica y datos biométricos. Bondades y peligros. No todo vale». *Actualidad Jurídica Iberoamericana* 21: 298-331.

Bestard, Juan J. 2021. *La gestión de datos personales y el delegado de protección de datos en la sanidad pública: Con atención especial a la Comunidad de Madrid*. Tesis doctoral. Acceso el 18 de octubre de 2024: https://repositorio.uam.es/handle/10486/699704

Castellanos, Jorge. 2023. *Inteligencia artificial y democracia: garantías, límites constitucionales y perspectiva ética ante la transformación digital*, Barcelona: Atelier.

Castellanos, Jorge. 2024. «Una reflexión acerca de la influencia de la inteligencia artificial en los derechos fundamentales». en *Ciencia de datos y perspectivas de la inteligencia artificial*, editado por Francisca Ramón, 271-300. Valencia: Tirant Lo Blanch.

Cotino, Lorenzo. 2022. «Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal». *El Cronista del Estado Social y Democrático de Derecho* 100: 68-79. Acceso el 18 de octubre 2024. https://www.uv.es/cotino/publicaciones/cronistacotinopublicado.pdf

Cotino, Lorenzo. 2023. «Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos». *Derecho público de la inteligencia artificial*, 347-402. Acceso el 18 de octubre 2024: https://www.fundacionmgimenezabad.es/sites/default/files/Publicar/publicaciones/documentos/oc27_13_lorenzo_cotino_es_o.pdf

Cotino, Lorenzo. 2023. «Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial. Los altos estándares

que exigen el Tribunal Constitucional alemán y otros tribunales, que no se cumplen ni de lejos en España», *Revista General de Derecho Administrativo* 63: Iustel (RI §425995)

Díaz, Juan. 2023. «Datos biométricos para el control de presencia y accesos». *I+S: Revista de la Sociedad Española de Informática y Salud* 157: 62. Acceso el 13 de julio de 2024. https://seis.es/is-157/

Díaz Lima, David. 2023. «Datos biométricos y acceso a eventos deportivos. Comentarios al Informe de la AEPD». *La Ley privacidad* 15.

Espuga, Gerard. 2023. «La (i)licitud del tratamiento de datos biométricos para el registro de jornada». en *Más allá de la oficina: desafíos laborales emergentes en un mundo hiperconectado*, editado por Francisco Trujillo, 139-160. Cizur Menor: Aranzadi.

Etxeberria, José F. Pilar Martín, César A. Villegas y José L. Rodríguez. 2023. «Datos biométricos y reconocimiento facial en el proceso penal». En *La tecnología y la inteligencia artificial al servicio del proceso*, dirigido por María Luis Domínguez, Pilar A. Villegas y José L. Rodríguez Lainz, 107-126. A Coruña: Colex.

Flórez, Mª Lorena, y Angélica Mª Camelo. 2023. «Tecnologías de reconocimiento facial en Colombia: Análisis comparativo en relación con la protección de datos». *Ius et Praxis* 29 (1): 3-26. Acceso el 14 de junio de 2024: https://www.revistaiep.utalca.cl/wp-content/uploads/2023/03/02.-Florez-Maria-Lorena-y-Camelo-Angelica.pdf

Garrido, Andrea. 2023. «El derecho al respeto a la vida privada: ¿el precio a pagar por una Europa segura en la era tecnológica?» *Revista Integración Regional & Derechos Humanos* 11 (2). Acceso el 1 de junio de 2024: http://www.derecho.uba.ar/institucional/centro-de-excelencia-jean-monnet/revista-electronica/009/garrido-raya.pdf

Garriga, Ana, Cristina Pauner, Rosario García Mahamut y Beatriz Tomás. 2023. «La especial posición de los datos biométricos en el RGPD: peculiaridades derivadas de su naturaleza y riesgos asociados a su tratamiento», en *La implementación del reglamento general de protección de datos en España y el impacto de sus cláusulas abiertas,* coordinado por Jorge A. Viguri, 115-144. Valencia: Tirant lo Blanch.

Garrós, Imma. 2021. «Las categorías especiales de datos personales y su régimen aplicable». *Revista Aranzadi Doctrinal* 2.

González Calvo, Marcos. 2022. «¿Hacia nuevas restricciones en el uso de datos biométricos?» *Actualidad jurídica Aranzadi* 990.

Han, Byung–Chul. 2020. «La emergencia viral y el mundo del mañana». *El País.* 22 de marzo. Acceso el 22 de mayo de 2024. https://elpais.com/ideas/2020-03-21/la-emergencia-viral-y-el-mundo-de-manana-byung-chul-han-el-filosofo-surcoreano-que-piensa-desde-berlin.html.

Harari, Yuval N. 2024. *Nexus. Una breve historia de las redes de información desde la Edad de Piedra hasta la IA*. Barcelona: Debate.

Iturmendi, José M. 2023. «La discriminación algorítmica y su impacto en la dignidad de la persona y los derechos humanos: Especial referencia a los

inmigrantes». *Revista Deusto de derechos humanos* 12: 257-284. https://djhr.revistas.deusto.es/article/view/2910. Acceso el 2 de mayo de 2024

Martínez Martínez, Ricard. 2020. «Tecnología de verificación de identidad y control en exámenes online». *Revista de educación y derecho* 22. doi.org/10.1344/REYD2020.22.32357

Ponce, Julio. 2024. «Inteligencia Artificial. Decisiones administrativas discrecionales totalmente automatizadas y alcance del control judicial: ¿Indiferencia, insuficiencia o deferencia?», *Revista de Derecho Público: Teoría y Método* 9: 172-220. DOI: 10.37417/RPD/vol_9_2024_2151

Razquin, Martín M. 2022. «La identidad digital como derecho». *Derecho Digital e Innovación* 14.

Romano, Andrea. 2023. «Derechos fundamentales e inteligencia artificial emocional en iBorderCtrl: retos de la automatización en el ámbito migratorio». *Revista catalana de dret públic* 66: 237-252. doi.org/10.58992/rcdp.i66.2023.3928.

Sebé, Sonia, y Manel Santilari. 2022. «Los datos biométricos como categorías especiales de datos. Debate a raíz de las directrices del Comité Europeo de Protección de Datos sobre reconocimiento facial». *Comunicaciones en propiedad industrial y derecho de la competencia* 97: 23-43.

Sempere, Javier. 2020. «¿Se puede utilizar la huella para el control de accesos a un gimnasio?». *La Ley privacidad* 3.

Serrano, Fernando. 2022. *El uso de la inteligencia artificial para optimizar los ingresos tributarios.* Informe 7. Caracas: CAF. https://scioteca.caf.com/handle/123456789/1933 Acceso el 18 de marzo de 2024.

Simón, Pere. 2021. *Justicia cautelar e inteligencia artificial. La alternativa a los atávicos heurísticos artificiales*. Barcelona: Bosch Editores.

Simón, Pere y Lorenzo Cotino (Dirs.). 2024. *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*. Madrid: Aranzadi.