Revista YACHAQ Nº 18
Publicada el 31 de enero de 2025
Centro de Investigación de los Estudiantes de Derecho (CIED)
Universidad Nacional de San Antonio Abad del Cusco
ISSN: 2707- 1197 (en línea)
ISSN: 1817 - 597 (impresa)
Fecha de recepción: 28/09/2024
Fecha de aceptación: 20/01/2025
[pp.27-40]

El uso de sistemas biométricos con Inteligencia Artificial: ¿una vulneración a los derechos humanos?

The use of biometric systems with Artificial Intelligence: a violation of human rights?

Maggie Adriana Tapia Tacca[1]

Resumen: Hoy en día, la inteligencia artificial ha avanzado a pasos agigantados en nuestro día a día, prueba de ello, son los sistemas de videovigilancia a través de biometría que, además que sirven para brindar seguridad ciudadana, permiten identificar a personas con mucha mayor rapidez, eficiencia y precisión. Sin embargo, no todo es tan bueno como parece, pues, a pesar de conocer dichas ventajas, en los sistemas biométricos se ha logrado identificar que, en algunas oportunidades, estos pueden ser vistos como una invasión a la privacidad de las personas, así como, la utilización de esta inteligencia artificial puede contener sesgos en sus algoritmos, lo cual, puede generar discriminación por raza, color, sexo, nacionalidad, etc. Es decir, puede conllevar a errores en la identificación de las personas con características físicas específicas o de las personas pertenecientes a diferentes grupos étnicos.

Palabras claves: sistemas biométricos, inteligencia artificial, derechos humanos, privacidad, discriminación

[1] Estudiante del cuarto año de Derecho de la Universidad Nacional Mayor de San Marcos. Miembro principal del Taller "Círculo de Derechos Humanos" de la UNMSM. Investigadora independiente. maggie.tapia@unmsm.edu.pe

Abstract: Nowadays, artificial intelligence has advanced by leaps and bounds in our daily lives, proof of this are the video surveillance systems through biometrics that, in addition to serving to provide citizen security, allow to identify people with much greater speed, efficiency and precision. However, not everything is as good as it seems, because, despite knowing these advantages, in biometric systems it has been identified that, on some occasions, these can be seen as an invasion of people's privacy, as well as, the use of this artificial intelligence can contain biases in their algorithms, which can generate discrimination based on race, color, sex, nationality, etc. That is, it can lead to errors in the identification of people with specific physical characteristics or people belonging to different ethnic groups.

Keywords: biometric systems, artificial intelligence, human rights, privacy, discrimination

1. INTRODUCCIÓN

El uso de la inteligencia artificial (IA) se ha integrado de manera significativa en nuestra vida cotidiana, desde los teléfonos inteligentes hasta los sistemas biométricos que sirven para la propia seguridad ciudadana. Los sistemas biométricos con IA identifican necesariamente características físicas específicas en las personas, tales como huellas dactilares, reconocimiento facial, de voz, los exámenes de retina, las expresiones faciales y los signos vitales. Por consiguiente, a esto se suma que, para que realmente el uso de estos sistemas con IA sea efectivo para la seguridad de las personas, se analizan grandes cantidades de datos biométricos, los cuales, en muchas ocasiones, son para compararlos con la información almacenada en bases de datos, con el fin de verificar si la persona en cuestión es realmente quien afirma ser.

En ese sentido, somos conscientes que, en la actualidad, el impacto de la IA se refleja en la automatización de tareas, la toma de decisiones basadas en datos y su capacidad de adaptarse y evolucionar con el tiempo. Ahora bien, respecto al uso de la IA en los sistemas biométricos, hasta el momento, ha causado controversias al respecto, pues, si bien es un gran avance en temas de seguridad ciudadana y vigilancia, es cuestionado por su vulneración a la privacidad de las personas y su posible sesgo de discriminación en ciudadanos, es decir, ¿realmente el uso de la biometría con IA es un gran avance o más bien es una amenaza a los derechos humanos?

2. LA IMPLEMENTACIÓN DE LA INTELIGENCIA ARTIFICIAL EN LOS SISTEMAS BIOMÉTRICOS

La inteligencia artificial es usada en diversos contextos en nuestro día a día, en ese sentido, respecto a la utilización de la IA en los sistemas biométricos, en países, específicamente europeos, se ha vuelto últimamente de mucho uso en especial en diversas aplicaciones de seguridad, sistemas de vigilancia, etc., siendo ampliamente

reconocidos como una tecnología fundamental, si no indispensable, para la protección de personas e instalaciones.

Asimismo, es la implementación de la IA que facilita la búsqueda de información en otros ámbitos que a simple vista esto no puede ser identificado o reconocido por los seres humanos, he ahí su importancia en la identificación de personas, pues, además estos sistemas se basan en la recolección de datos personales para realizar un reconocimiento inequívoco, utilizando de forma automática técnicas aplicadas a los rasgos físicos o comportamentales de cada individuo.

3. ¿EL USO DE SISTEMAS BIOMÉTRICOS CON INTELIGENCIA ARTIFICIAL: ¿PRESENTAN RASGOS DE DISCRIMINACIÓN?

El uso inadecuado o la implementación deficiente de esta tecnología puede conducir a situaciones de discriminación y exclusión. Puesto que, sin un sistema verificado que respalde la autenticación basada en documentos de identidad, la efectividad en distintos grupos demográficos puede ser poco confiable, lo que restringiría el acceso de los usuarios a servicios esenciales. Ante ello, para poder responder si realmente el uso de estos sistemas biométricos genera discriminación es necesario analizar los diversos escenarios posibles que se presentan en el uso de sistemas biométricos, es decir, escenarios donde se puede apreciar la parcialidad de los algoritmos en los sistemas biométricos con IA, por lo cual las personas no son tratadas en igualdad de condiciones ante otras.

En primer lugar, dentro del uso de sistemas biométricos podemos encontrar el sistema de "caja negra" (Pasquale, 2015), el cual se refiere a la opacidad en los procesos de toma de decisiones de un modelo de IA, en ese caso, de los sistemas biométricos. Específicamente, describe una situación en la que los usuarios y, en muchos casos, incluso los desarrolladores, no pueden entender con claridad cómo el sistema llega a sus conclusiones o predicciones. En otras palabras, esto significa que el funcionamiento de algunos de estos sistemas nos dificulta entender por qué el algoritmo toma determinadas decisiones en relación con ciertas personas. En ese sentido, su falta de transparencia impide identificar si la discriminación se basó en el sexo, etnia, raza, edad, religión, ideología u otro factor, lo cual dificulta explicar cómo un algoritmo puede discriminar en ciertos casos.

Ahora bien, en segundo lugar, también están los sistemas que no hacen uso de la "caja negra", también llamados sistemas de IA transparentes (Miller, 2019), los cuales suelen ser más transparentes y explicables en su funcionamiento, pues en lugar de ocultar sus procesos de decisión, permiten que los usuarios, desarrolladores y reguladores comprendan cómo y por qué se llega a determinadas conclusiones o decisiones. Por consiguiente, es más sencillo identificar cómo un algoritmo discrimina, ya que generalmente la causa es que la información utilizada para entrenar el

algoritmo es incompleta o sesgada, lo que introduce criterios discriminatorios durante su entrenamiento. En otras palabras, al ser más accesibles para su análisis, es más sencillo identificar posibles sesgos o desigualdades en la toma de decisiones, lo que permite implementar ajustes.

En tercer lugar, otro sistema en donde el sistema biométrico con IA se puede ver sesgado, es cuando la base de datos del propio sistema contiene sesgos (O' Neil, 2017). Eso ocurre cuando la IA se entrena con datos incompletos o aprende a partir de una muestra sesgada, lo que lleva a que luego reproduzca esa parcialidad al momento de la identificación de las personas, lo cual conlleva que podrían identificar de manera desigual a personas de diferentes grupos étnicos, géneros, edades u otras características demográficas. Desafortunadamente, este es un problema común, ya que los datos utilizados en los sistemas de IA reflejan los prejuicios discriminatorios preexistentes en los seres humanos. En ese sentido, se ve afectada, gravemente, la precisión y la confianza en estas tecnologías, específicamente, en los sistemas biométricos con IA, lo cual es particularmente problemático en situaciones críticas, como la justicia penal o la seguridad.

En síntesis, la carencia de información sobre datos sensibles en ciertos casos podría llevar a la discriminación de grupos minoritarios. Por lo tanto, en algunos contextos, disponer de esta información sensible puede ser crucial para realizar distinciones o para evitar tratamientos desiguales. Ahora, si bien las bases de datos de algunos de estos sistemas biométricos contienen sesgos o se encuentran incompletas, los sistemas biométricos pueden replicar y amplificar prejuicios existentes, afectando desproporcionadamente a ciertos grupos en específico. Además, la falta de transparencia en el funcionamiento de estos sistemas, como, por ejemplo, el sistema de "caja negra", complica la identificación y corrección de estas desigualdades. Por lo tanto, aunque estos sistemas ofrecen avances tecnológicos significativos, es crucial abordar y mitigar los sesgos inherentes para garantizar que su uso sea justo y equitativo, protegiendo así los derechos de todas las personas y evitando prácticas discriminatorias.

4. ¿EL USO DE SISTEMAS BIOMÉTRICOS CON INTELIGENCIA ARTIFICIAL: ¿UNA INVASIÓN A LA PRIVACIDAD?

Dado que las actividades de IA en los sistemas biométricos implican la recopilación y análisis de información, incluyendo datos personales (a menudo sin el consentimiento de las personas afectadas), las normas internacionales también abarcan aspectos relacionados con la obtención, almacenamiento, conservación y acceso a dicha información[2]. En ese sentido, la capacidad de estos sistemas biométricos para recopilar, almacenar y analizar datos

[2]Corte IDH. Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 18 de octubre de 2023. Serie C No. 506, párr. 556.

biométricos, como huellas dactilares, patrones faciales y características del iris, genera preocupaciones significativas sobre cómo se manejan los datos personales sensibles. Ante ello, para responder si estos sistemas llegan a constituir una invasión a la privacidad, debemos de examinar los riesgos asociados con la recolección masiva de datos, el potencial para el abuso y la falta de control sobre la información personal en la era digital.

Ahora bien, los riesgos asociados se presentan, principalmente, por una recolección encubierta y poco transparente de datos personales, lo cual conlleva una falta de control sobre la información personal y una invasión a la privacidad de las personas, en muchos casos. Asimismo, existe el riesgo de que los datos se utilicen de manera diferente a la inicialmente prevista, o que se empleen para la toma de decisiones automatizadas, la predicción de comportamientos o la determinación de preferencias individuales en contextos específicos. Ante ello, se requiere establecer un marco de actuación para las autoridades en el ámbito de la recolección y uso de datos personales, con el objetivo de prevenir su obtención, utilización, almacenamiento, divulgación e intercambio de manera inadecuada o contraria a los derechos correspondientes[3]. Debido a que, la protección de datos continúa siendo, por defecto, la normativa aplicable cuando estos sistemas procesan información personal (Cotino, 2023).

Por ejemplo, en Perú, la Ley Nº 29733, Ley de Protección de Datos Personales[4] tiene como objeto garantizar el derecho fundamental a la protección de datos personales, previsto en el numeral 6 del artículo 2° de la Constitución Política del Perú, es decir, existe ya una regulación de datos personales en el ámbito de los datos biométricos y su empleo en la identificación de personas. Sin embargo, ¿esta regulación resulta suficiente?, si bien, al leerlo, nos podemos dar cuenta que resulta un punto de partida importante, no es del todo suficiente para abordar los desafíos específicos que presentan los sistemas biométricos con inteligencia artificial (IA). Dado que, estos sistemas implican particularidades y riesgos adicionales que requieren un enfoque más detallado y adaptado a sus características únicas.

Además, en el caso específico de los sistemas de reconocimiento facial, a través de sistemas biométricos, su creciente implementación podría eliminar el anonimato en los espacios públicos y permitir el monitoreo constante de las personas, lo cual significa que las personas se encuentran constantemente vigiladas, pues esto se expande en espacios públicos como calles, estaciones de transporte,

[3] Corte IDH. Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 18 de octubre de 2023. Serie C No. 506, párr. 571.

[4] véase en https://cdn.www.gob.pe/uploads/document/file/2096238/Sobre%20los%20datos%20biom%C3%A9tricos%20y%20su%20empleo%20en%20la%20identificaci%C3%B3n%20de%20personas%2C%20el%20tratamiento%20de%20datos%20personales%2C%20la%20obtenci%C3%B3n%20del%20consentimiento%2C%20la%20conservaci%C3%B3n%20de%20documentos%20digitales%2C%20la%20atenci%C3%B3n%20de%20derechos%20ARCO%20y%20registro%20de%20bancos%20de%20datos.pdf

centros comerciales y eventos masivos. En ese sentido, es este reconocimiento facial, el que permite identificar a las personas de manera inmediata y sin su consentimiento, lo que abre la puerta a un seguimiento constante y en tiempo real de sus movimientos y actividades. Ante ello, por ejemplo, las tecnologías de reconocimiento facial en tiempo real son ampliamente rechazadas por la población tanto en Europa como en otros países debido a su carácter invasivo, según un estudio de la FRA[5].

En síntesis, el uso de sistemas biométricos con inteligencia artificial plantea varios riesgos, lo cual, con efecto, conlleva a una serie de preocupaciones en torno a la invasión de la privacidad de las personas respecto a su uso de información personal y sensible. Como hemos podido observar, la falta de transparencia en el procesamiento de estos datos personales de las personas y el riesgo de que sean utilizados para fines no previstos, como la creación de perfiles o la discriminación, acentúa la necesidad de una regulación más robusta, a la que se puede ya tener en algunos países. En ese sentido, aunque estos sistemas ofrecen avances tecnológicos significativos, su uso sin las debidas salvaguardias amenaza la privacidad individual.

5. DERECHOS HUMANOS AFECTADOS POR EL USO DE LA INTELIGENCIA ARTIFICIAL EN LOS SISTEMAS BIOMÉTRICOS

Al hacer uso de los sistemas biométricos con IA, como se ha visto en apartados anteriores, se puede evidenciar la presencia de ciertos sesgos en dichos sistemas, así como, si su uso no es adecuado, una invasión a la privacidad de las personas que se encuentran en dichos países. En ese sentido, este avance tecnológico ha generado una grave implicancia en los derechos humanos en nuestro mundo actual, como el derecho a la privacidad y el derecho a la protección de datos personales, vinculados con el artículo 11 de la Convención Americana sobre Derechos Humanos (en adelante CADH); el derecho a la igualdad y no discriminación, establecido en el artículo 24 de la CADH. Por lo cual, resulta fundamental examinar de qué manera la implementación de estos sistemas impacta en los derechos humanos, lo cual se desarrollará líneas más abajo.

En primer lugar, respecto al derecho a la privacidad y el derecho a la protección de datos personales, se debe precisar que ya la Corte Interamericana de Derechos Humanos (en adelante Corte IDH) se ha pronunciado al respecto a través un caso reciente, Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia. En ese sentido, este caso revela gran importancia en materia de IA y protección de datos personales, pues evidencia, efectivamente la violación de derechos humanos, en materia de derecho a la privacidad y protección de datos. Ante ello, ¿cómo se puede saber desde qué momento o a partir de qué momento se

[5] Agencia Europea de Derechos Fundamentales (FRA, por sus siglas en inglés).

estaría vulnerando estos derechos con el uso, en específico, de los sistemas biométricos con IA?

Los estándares internacionales en protección de datos personales establecen que la recolección, almacenamiento, procesamiento y divulgación de estos datos personales solo es posible con el consentimiento libre e informado de su titular[6], lo cual también fue confirmado en una sentencia del Tribunal Europeo de Derechos Humanos, caso Leander Vs. Suecia[7], añadiendo además que la utilización de estos sin "garantías adecuadas y eficaces contra los abusos", legalmente previstas, suponían una interferencia ilegítima al derecho al respeto de la vida privada. O, en su defecto, solo es posible, bajo un marco legal que autorice explícitamente a los organismos públicos a llevar a cabo dichas acciones[8]. En ese sentido, se entiende que, se estaría vulnerando los derechos humanos cuando no existe un consentimiento libre e informado para que se efectúe dicha recolección de datos, así como, en el país en que se estaría realizando, no exista un marco regulatorio que autorice ello. Ahora bien, ¿esto resultaría suficiente para determinar si hubo o no una vulneración a la privacidad o al acceso de datos personales?, la respuesta es, claramente, no. Debido a que, la utilización de sistemas biométricos con IA en los países, deben de seguir con los principios de idoneidad, necesidad y proporcionalidad, es decir, con los elementos del test de proporcionalidad. En ese sentido, la Corte IDH[9], en diversos casos, menciona lo siguiente:

> **a)** que las acciones u operaciones de inteligencia que se emprendan sean idóneas o adecuadas para cumplir con el fin legítimo perseguido**; b)** que las actividades de inteligencia en general, y las acciones o métodos empleados en particular, sean necesarias, en el sentido de que sean absolutamente indispensables para conseguir el fin deseado y que no exista una medida menos gravosa, por su injerencia en el derecho a la vida privada o cualquier otro derecho que pueda verse afectado, entre todas aquellas otras acciones o estrategias que cuentan con la misma idoneidad para alcanzar el objetivo propuesto, **y c)** que las acciones de inteligencia resulten estrictamente proporcionales, de tal forma que el sacrificio inherente a la restricción del derecho involucrado no devenga

[6] Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con Anotaciones, pág. 32.
[7] TEDH, Caso Leander Vs. Suecia, No. 9248/81, Sentencia de 26 de marzo de 1987, párr. 48.
[8] Corte IDH. Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 18 de octubre de 2023. Serie C No. 506, párr. 573.
[9] Corte IDH. Caso Durand y Ugarte Vs. Perú. Fondo. Sentencia de 16 de agosto de 2000. Serie C No. 68, párr. 79; Caso Palamara Iribarne Vs. Chile. Fondo, Reparaciones y Costas. Sentencia de 22 de noviembre de 2005. Serie C No. 135, párr. 197; Caso Tristán Donoso Vs. Panamá, supra, párr. 76; Caso Escher y otros Vs. Brasil, supra, párr. 129; Caso Nadege Dorzema y otros Vs. República Dominicana, supra, párr. 85; Caso Norín Catrimán y otros (Dirigentes, Miembros y Activista del Pueblo Indígena Mapuche) Vs. Chile. Fondo, Reparaciones y Costas. Sentencia de 29 de mayo de 2014. Serie C No. 279, párr. 164; Caso Mujeres Víctimas de Tortura Sexual en Atenco Vs. México. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 28 de noviembre de 2018. Serie C No. 371, párr. 162, y Caso García Rodríguez y otro Vs. México, supra, párrs. 156 a 158.

exagerado o desmedido frente a las ventajas que se obtienen mediante tal restricción y el cumplimiento de la finalidad perseguida

Esto quiere decir que, este test de proporcionalidad, que debe de ser realizado por los países que emplean el uso de sistemas biométricos con IA, tiene como objetivo garantizar que cualquier limitación a los derechos humanos sea adecuada, necesaria y proporcionada en relación con el fin que se busca, por lo cual se busca que no se socave los derechos humanos de manera innecesaria o desmedida y, de esta manera, permitir un equilibrio adecuado entre los intereses legítimos del Estado y la protección de los derechos humanos de los ciudadanos.

Ahora bien, respecto al marco legal que se debe de tener en cada país respecto al uso o autorización de los datos personales, se debe de tomar en cuenta que, se debe de crear un marco legal unificado que se fundamente en principios éticos como la transparencia, la responsabilidad y la no discriminación, tal como ha sido reafirmado por el Informe de la comisión especial sobre Inteligencia Artificial en la Era Digital (AIDA)[10]. Así como, desde la normativa interna, se contempla la necesidad de establecer "un sistema claro y completo para la autorización, monitoreo y supervisión" de las actividades de inteligencia en situaciones específicas.

En ese sentido, en la Unión Europea, se tiene el Reglamento General de Protección de Datos (RGPD)[11], el cual entró en vigor en el año 2018. Se tiene algunos principios relativos al tratamiento de los datos biométricos establecidos, específicamente, en el artículo 5. Como, por ejemplo, el principio de licitud, lealtad y transparencia, en el cual se explica que los datos personales deben de ser tratados de manera legal, justa y transparente. Por lo tanto, no está permitido recopilar datos biométricos sin que la persona esté informada. El principio de limitación de la finalidad, en el cual solo se puede recoger los datos para fines específicos y explícitos, lo cual garantiza que no se utilicen para objetivos distintos sin consentimiento adicional. El principio de integridad y confidencialidad, por el cual los datos deben ser tratados de manera que se garantice su seguridad adecuada, pues, en definitiva, es el objetivo que se busca al momento de la implementación de sistemas biométricos con IA, brindar seguridad. Por último, otro principio es el de exactitud, en el cual datos personales deben ser exactos y estar, constantemente, actualizados, lo cual es sumamente importante, en materia de derecho a la igualdad y no discriminación, que se abordará más adelante.

En ese sentido, se determina que la privacidad de los datos personales está vinculada al derecho que posee cada individuo sobre sus datos biométricos, pues tal como lo menciona Muñoz (2017) lo

[10]véase en https://www.europarl.europa.eu/doceo/document/A-9-2022-0088_ES.html

[11]véase en https://www.boe.es/doue/2016/119/L00001-00088.pdf

relevante es la facultad del titular de los datos para decidir con quién y cómo compartir su información personal, en especial, aquella de carácter sensible. Por lo cual, como principio esencial, se requiere el consentimiento expreso y voluntario de las personas para el uso de dichos datos y cualquier uso sin autorización previa será considerado una vulneración al artículo 11 de la CADH, pues es este derecho el que genera la protección contra interferencias arbitrarias o ilegales en la vida privada de las personas. Por eso, al momento en que los sistemas biométricos con IA llegan a recopilar información sensible, como huellas dactilares, reconocimiento facial o patrones de comportamiento, sin el consentimiento explícito de los individuos, se estaría vulnerando este derecho humano.

En segundo lugar, respecto al derecho a la igualdad y no discriminación, se debe precisar que la Corte IDH[12], ya ha establecido en numerosos casos que el principio de igualdad ante la ley, la igual protección bajo la ley y la no discriminación son normas de jus cogens, ya que constituyen la base del marco jurídico tanto a nivel nacional como internacional. Por lo cual, este principio fundamental es esencial y está presente en todos los sistemas jurídicos. En ese sentido, actualmente, no se acepta ningún acto jurídico que contravenga este principio fundamental. En otras palabras, no se permite la discriminación contra ninguna persona por motivos de género, raza, color, idioma, religión, creencias, opiniones políticas o de otro tipo, origen nacional, étnico o social, nacionalidad, edad, situación económica, patrimonio, estado civil, lugar de nacimiento u otras condiciones[13].

Ahora bien, ese derecho no solo ha sido desarrollado en la jurisprudencia de la Corte IDH, sino que ha sido establecido en opiniones consultivas, tales como la Opinión Consultiva OC-27/21[14] o la Opinión Consultiva OC - 24/17[15], la cual menciona lo siguiente:

> Los Estados están obligados a adoptar medidas positivas para revertir o cambiar situaciones discriminatorias existentes en sus sociedades, en perjuicio de determinado grupo de personas. Esto implica el deber especial de protección que el Estado debe ejercer con respecto a actuaciones y prácticas de terceros que, bajo su tolerancia o aquiescencia, creen,

[12] Corte IDH. Condición jurídica y derechos de los migrantes indocumentados. Opinión Consultiva OC-18/03 de 17 de septiembre de 2003. Serie A No. 18, párr. 101. Corte IDH. Caso Furlan y familiares Vs. Argentina. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 31 de agosto de 2012. Serie C No. 246, párr. 267. Corte IDH. Caso de las niñas Yean y Bosico Vs. República Dominicana. Sentencia de 8 de septiembre de 2005. Serie C No. 1305, párr. 141. Corte IDH. Caso Yatama Vs. Nicaragua. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 23 de junio de 2005. Serie C No. 127, párr. 186. Corte IDH. Caso Atala Riffo y niñas Vs. Chile. Fondo, Reparaciones y Costas. Sentencia de 24 de febrero de 2012. Serie C No 239, párr. 82.

[13] Corte IDH. Condición jurídica y derechos de los migrantes indocumentados. Opinión Consultiva OC-18/03 de 17 de septiembre de 2003. Serie A No. 18, párr. 101.

[14] véase en https://www.corteidh.or.cr/docs/opiniones/seriea_27_esp1.pdf

[15] Asimismo, Naciones Unidas, Comité de Derechos Humanos, Observación General No. 18, No discriminación, 10 de noviembre de 1989, CCPR/C/37, párr. 5.

> mantengan o favorezcan las situaciones discriminatorias. (párr. 65)

Esto quiere decir que, por parte de los Estados, siempre debe haber el compromiso y proactividad para combatir la discriminación en todos sus ámbitos, lo cual, significa que incluso en el uso de la IA, en específico, el uso de sistemas biométricos con IA. Por consiguiente, no es suficiente con tener leyes que prohíban la discriminación, sino que los Estados deben ser activos en la implementación de medidas que rectifiquen desigualdades y asegurar que las prácticas discriminatorias no sean toleradas ni permitidas. Es decir, no solo se debe de ver materializado en la teoría, sino en la práctica de los Estados.

Ahora bien, esto también ha sido desarrollado por el Tribunal Europeo de Derechos Humanos[16], el cual menciona que una medida general, por ejemplo, llevándolo al caso concreto, el uso de sistemas biométricos con IA puede ser considerada discriminatoria si tiene un impacto desproporcionadamente negativo en un grupo específico, incluso si no estaba destinada explícitamente a ese grupo. Es decir, este enfoque permite ayudar a identificar y abordar las desigualdades en la práctica y asegura que todos los grupos tengan igualdad de oportunidades y protección.

En materia de IA, actualmente, las tecnologías digitales emergentes intensifican y amplifican las desigualdades preexistentes, muchas de las cuales están relacionadas con la raza, etnia y origen nacional[17]. Por ejemplo, un estudio realizado en 2019 que evaluó 189 algoritmos de reconocimiento facial desarrollados por 99 programadores de diversas partes del mundo reveló que "las probabilidades de que muchos de estos algoritmos identificasen incorrectamente una fotografía de un rostro negro o con rasgos de Asia Oriental eran entre 10 y 100 mayores que si se tratase de la fotografía de una persona blanca"[18]. Es decir, los sistemas de reconocimiento facial presentaban tasas de error más elevadas al identificar a personas de raza negra o asiática en comparación con individuos de raza blanca, lo cual, efectivamente, puede conducir a discriminación en campos como la seguridad, la vigilancia y la identificación.

Ante ello, también se podría mencionar que resulta importante un marco legal en materia de no discriminación e igualdad de trato en sistemas basados en IA, en ese caso, en el uso de sistemas biométricos, por parte de los países. Un ejemplo de ello es la Ley 15/2022 de igualdad de trato y la no discriminación establecida en España[19], el cual aborda la igualdad de trato y no discriminación en el ámbito de la inteligencia artificial y

[16] TEDH, Caso Hoogendijk Vs. Holanda, No. 58641/00, Sección Primera, 2005; TEDH, Gran Camara, D. H. y otros Vs. República Checa, No. 57325/00, 13 de noviembre de 2007, párr. 175, y TEDH, Caso Hugh Jordan Vs. Reino Unido, No. 24746/94, 4 de mayo de 2001, párr. 154.

[17] véase en https://documents.un.org/doc/undoc/gen/g20/151/09/pdf/g2015109.pdf

[18] Véase ww.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racialbias

[19] véase en https://www.boe.es/eli/es/l/2022/07/12/con

mecanismos de toma de decisión automatizados. Por consiguiente, un marco legal es fundamental para regular el uso de IA, ya que, de esta manera, se protege a mayor grado los individuos de posibles discriminaciones y garantizando la igualdad de trato en el contexto de un mundo cada vez más digital y automatizado.

En ese sentido, el uso de sistemas biométricos con IA puede generar la vulneración de derecho a la igualdad ante la ley amparado en la CADH, puesto que, los conjuntos de datos empleados por los sistemas de IA, pueden contener sesgos históricos no intencionados -como los ejemplos dados con anterioridad- u omisiones en la gestión. En ese sentido, la persistencia de estos sesgos puede resultar en prejuicios y discriminación, ya sea directa o indirectamente, contra ciertos grupos o individuos, lo que puede intensificar estereotipos y aumentar la marginación. En otras palabras, la presencia de sesgos históricos y errores en la gestión de datos puede tener un impacto significativo en la precisión y justicia de los sistemas de IA. Por lo cual, la ausencia de datos representativos de ciertos grupos o condiciones puede llevar a que los modelos de IA no sean efectivos o precisos al tratar con esos grupos

6. CONCLUSIONES

Primera. - Los sistemas biométricos con IA representan un riesgo considerable en los derechos humanos, tales como el derecho a la invasión a la privacidad y datos personales, así como, el derecho a la igualdad y no discriminación. Si bien la implementación de estas tecnologías presenta un gran avance para la humanidad, hoy en día, por lo cual, en un futuro no lejano, muchos de los países en el mundo, las implementarán en sus estados. Sin embargo, esta tecnología para que genere un efecto positivo y más bien, no vulnere derechos humanos, es necesario procurar que esta la tecnología se utilice para promover el bienestar general, la igualdad y la no discriminación, siempre procurando el respeto a los derechos humanos.

Segunda. -La biometría y la IA, como se planteó en un inicio, se destacan, principalmente, como herramientas útiles para realizar diversas tareas en el mundo actual, específicamente, estos sistemas biométricos, para brindar seguridad y eficiencia. No obstante, se ha demostrado que la tecnología no está exenta de fallos y puede reflejar las mismas imperfecciones que sus desarrolladores. Estos errores y/o imperfecciones pueden manifestarse de diversas formas, como el mal funcionamiento en contextos específicos o la perpetuación de prejuicios preexistentes. Por ejemplo, se han documentado fallos significativos en la identificación de personas pertenecientes a ciertos grupos raciales o étnicos, lo que genera -aunque no sea el fin de estos sistemas- discriminación en estos grupos específicos.

Tercera. -Ahora bien, se debe precisar que, como es evidente, la legislación no ha avanzado al mismo ritmo que la IA, en especial, en el uso de sistemas biométricos con IA, lamentablemente. En otras palabras, la ausencia de regulaciones sólidas deja un

vacío que puede ser usado de mala manera por países que no prioricen el respeto por los derechos humanos. Lo cual, incluye la recolección de datos biométricos sin consentimiento informado y la posibilidad de que estos sistemas biométricos con IA agraven los sesgos ya existentes en la sociedad. Por lo cual, actualmente, nos encontramos en una situación de gran inseguridad jurídica, debido a la complejidad del tema. Sin embargo, es necesario destacar que, la mayor parte de regulación en materia de IA y, la presencia de un evidente avance en esta materia se presenta en Europa.

Cuarta. -Por tanto, el uso de sistemas biométricos basados en IA plantea importantes desafíos en relación con la protección de los derechos humanos, por lo cual resulta de suma importancia que los Estados hayan o no hayan implementado estos sistemas, empiecen por desarrollar políticas, regulaciones, normativas que permitan un equilibrio del avance tecnológico que estamos teniendo hoy en día con la protección de los derechos humanos. Por consiguiente, los Estados deben estar atentos a la evolución de estas tecnologías y anticiparse a los posibles impactos negativos, lo cual incluye no solo la creación de normativas nacionales, sino también la cooperación internacional para procurar, siempre, el bienestar general de las personas.

BIBLIOGRAFÍA

Caso Atala Riffo y niñas Vs. Chile. Fondo, Reparaciones y Costas. Sentencia de 24 de febrero de 2012. Serie C No 239.

Caso Durand y Ugarte Vs. Perú. Fondo. Sentencia de 16 de agosto de 2000. Serie C No. 68.

Caso de las niñas Yean y Bosico Vs. República Dominicana. Sentencia de 8 de septiembre de 2005. Serie C No. 1305.

Caso Furlan y familiares Vs. Argentina. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 31 de agosto de 2012. Serie C No. 246.

Caso Gran Cámara, D. H. y otros Vs. República Checa, No. 57325/00, 13 de noviembre de 2007.

Caso Hoogendijk Vs. Holanda, No. 58641/00, Sección Primera, 2005.

Caso Hugh Jordan Vs. Reino Unido, No. 24746/94, 4 de mayo de 2001.

Caso Leander Vs. Suecia, No. 9248/81, Sentencia de 26 de marzo de 1987.

Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 18 de octubre de 2023. Serie C No. 506

Caso Mujeres Víctimas de Tortura Sexual en Atenco Vs. México. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 28 de noviembre de 2018. Serie C No. 371.

Caso Norín Catrimán y otros (Dirigentes, Miembros y Activista del Pueblo Indígena Mapuche) Vs. Chile. Fondo, Reparaciones y Costas. Sentencia de 29 de mayo de 2014. Serie C No. 279.

Caso Palamara Iribarne Vs. Chile. Fondo, Reparaciones y Costas. Sentencia de 22 de noviembre de 2005. Serie C No. 135.

Caso Yatama Vs. Nicaragua. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 23 de junio de 2005. Serie C No. 127.

Comisión Europea. (2021, 21 de abril). *Dictamen conjunto 5/2021 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) del 18 de junio de 2021.* https://www.edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_es.pdf

Comité Jurídico Interamericano. (2021). *Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con anotaciones.* https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Commatteo, G., & Moreyra, P. (2022). Discriminación 4.0: una aproximación a los problemas que suscitan la biometría y los sistemas de reconocimiento facial. *Revista Internacional de Derechos Humanos, 12*(1), 15-53.

Convención Americana sobre Derechos Humanos, 22 de noviembre, 1969, https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

Domínguez, A. G. (2024). Los derechos ante los sistemas biométricos que incorporan Inteligencia Artificial. DERECHOS Y LIBERTADES. *Revista de Filosofía del Derecho y derechos humanos,* (51), 117-149.

Cotino, L. (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), 29.

Ley 15/2022. (2022, 12 de julio). Congreso de la República, España. https://www.boe.es/eli/es/l/2022/07/12/15/con

Ley Nº 29733. (2011, 03 julio), Congreso de la República. Diario oficial El Peruano. https://cdn.www.gob.pe/uploads/document/file/272360/Ley%20N%C2%BA%2029733.pdf.pdf?v=1618338779

Miller, T. (2019). *Explanation in artificial intelligence: Insights from the social sciences. Artificial intelligence*, 267, 1-38.

Muñoz Gallardo, S. (2017). *Datos Biométricos y Derechos Fundamentales* [Tesis de pregrado, Universidad de Chile]. Archivo digital. https://repositorio.uchile.cl/handle/2250/145203

Naciones Unidas. (2020). *Informe de la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia; La discriminación racial y las*

tecnologías digitales emergentes: un análisis de los derechos humanos, A/HRC/44/57 .https://documents.un.org/doc/undoc/gen/g20/151/09/pdf/g2015109.pdf

Naciones Unidas. (2021). *Informe del Relator Especial sobre el derecho a la privacidad, Joseph A. Cannataci, la inteligencia artificial y la privacidad, así como la privacidad de los niños, A/HRC/46/37*. https://documents.un.org/doc/undoc/gen/g21/015/68/pdf/g2101568.pdf

Opinión Consultiva N° 032-2021-JUS/DGTAIPD

Opinión Consultiva OC-18/03 de 17 de septiembre de 2003. Serie A No. 18.

Opinión Consultiva OC-24/17 de 24 de noviembre de 2017. Serie A No. 249

Opinión Consultiva OC-27/21 de 5 de mayo de 2021. Serie A No. 27

Parlamento Europeo. (2020). *Informe de la comisión especial sobre Inteligencia Artificial en la Era Digital (AIDA).* https://www.europarl.europa.eu/doceo/document/A-9-2022-0088_ES.html

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information.* Harvard University Press.

Reglamento General de Protección de Datos. (2016, 27 de abril). Comité Europeo de Protección de Datos. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_es

O'neil, C. (2017). *Weapons of math destruction: How big data increases inequality and threatens democracy.* Crown.