Rev. Crim. / Volumen 64 - Número 3 - Septiembre-Diciembre 2022 - pp. 61-78 - ISSN 1794-3108 https://doi.org/10.47741/17943108.366

Tecnología de reconocimiento facial y sus riesgos en los derechos humanos*

Facial recognition technology and its risks to human rights

A tecnologia de reconhecimento facial e seus riscos para os direitos humanos

Fecha de recepción: 2021/05/11 | Fecha de evaluación: 2022/10/03 | Fecha de aprobación: 2022/06/10

Jesús E. Sanabria Moyano
Magíster en Derecho Público Militar
Profesor e Investigador
Centro de Investigaciones Jurídicas, Políticas y Sociales,
Facultad de Derecho,
Universidad Militar Nueva Granada
Bogotá D.C.
jesus.sanabria@unimilitar.edu.co
https://orcid.org/0000-0001-9715-5305

Marcela del Pilar Roa Avella
Magister en Derecho Penal
Profesora e investigadora
Centro de Investigaciones Jurídicas, Políticas y Sociales
Facultad de Derecho
Universidad Militar Nueva Granada
Bogotá D.C.
marcela.roa@unimilitar.edu.co
https://orcid.org/0000-0001-6307-3627

Oscar Iván Lee Pérez
Abogado
Asistente de investigación,
Centro de Investigaciones Jurídicas, Políticas y Sociales, Facultad de Derecho,
Universidad Militar Nueva Granada
Bogotá D.C.
oscarivan2400@gmail.com

Para citar este artículo / To reference this article / Para citar este artigo: Sanabria, J., Roa, M. & Lee, O. (2022). Tecnología de reconocimiento facial y sus riesgos en los derechos humanos. *Revista Criminalidad, 64*(3), 61-78. https://doi.org/10.47741/17943108.366

Resumen

El desarrollo de tecnologías dinamizadas por la inteligencia artificial (IA) representa un desafío adaptativo para ciencias tradicionales y rígidas como el derecho. Debido a las características de los diversos métodos o procedimientos usados de forma automatizada, se presenta una relación antagónica entre implementación de herramientas de reconocimiento facial y los derechos considerados garantías constitucionales y fundamentales en el sistema de derechos humanos. El objetivo es describir el funcionamiento de los sistemas de visión involucrados en la IA, presente principalmente en las herramientas de reconocimiento facial, examinando la manera como se relacionan con el derecho penal y reconociendo los riesgos a los derechos humanos en este proceso. Para ello, se usó una metodología cualitativa-inductiva, realizando análisis de fuentes primarias y secundarias, estudios de caso y legislaciones de diversas jurisdicciones relacionadas con reconocimiento facial y su aplicación en las etapas de indagación e investigación en el proceso penal. Como resultado se obtuvo que en dichas etapas existe un riesgo a las garantías de un debido proceso y de no discriminación.

Palabras clave:

Control social, derechos humanos, Inteligencia artificial (fuente: Tesauro del Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia – UNICRI). Garantías constitucionales, herramientas de reconocimiento facial, riesgos (fuente: autor).

* Este artículo es producto del proyecto de investigación INV-DER 3159 titulado "Inteligencia Artificial: retos y riesgos de los Derechos Humanos en el Sistema Penal", correspondiente al grupo de "Derecho Público", línea de investigación "Derecho Penal y Justicia Militar", que se adelanta en el Centro de Investigaciones Jurídicas, Políticas y Sociales de la Facultad de Derecho de la Universidad Militar Nueva Granada. Este proyecto fue financiado por la Vicerrectoría de Investigaciones de la Universidad Militar Nueva Granada –Convocatoria Proyectos Investigación Científica.

Abstract

The development of technologies powered by artificial intelligence (AI) represents an adaptive challenge for traditional and rigid sciences such as law. Due to the characteristics of the various methods or procedures used in an automated way, there is an antagonistic relationship between the implementation of facial recognition tools and the rights considered constitutional and fundamental guarantees in the human rights system. The objective is to describe the functioning of the vision systems involved in AI, mainly present in facial recognition tools, examining how they relate to criminal law and recognizing the risks to human rights in this process. For this purpose, a qualitative-inductive methodology was used, analyzing primary and secondary sources, case studies and legislation from various jurisdictions related to facial recognition and its application in the investigation and inquiry stages of the criminal process. As a result, it was obtained that in such stages there is a risk to the guarantees of due process and non-discrimination.

Key words:

Social control, human rights, Artificial intelligence (source: Criminological Thesaurus - United Nations Interregional Crime and Justice Research Institute- UNICRI). Constitutional guarantees, facial recognition tools, risks (source: authors).

Resumo

O desenvolvimento de tecnologias impulsionadas pela inteligência artificial (IA) representa um desafio adaptativo para as ciências tradicionais e rígidas, como o direito. Devido às características dos vários métodos ou procedimentos utilizados de forma automatizada, existe uma relação antagônica entre a implementação de ferramentas de reconhecimento facial e os direitos considerados garantias constitucionais e fundamentais no sistema de direitos humanos. O objetivo é descrever o funcionamento dos sistemas de visão envolvidos na IA, principalmente presentes nas ferramentas de reconhecimento facial, examinando como eles se relacionam com o direito penal e reconhecendo os riscos aos direitos humanos neste processo. Para este fim, foi utilizada uma metodologia qualitativa-indutora, analisando fontes primárias e secundárias, estudos de casos e legislação de várias jurisdições relacionadas ao reconhecimento facial e sua aplicação nas fases de investigação e inquérito de processos criminais. Como resultado, foi obtido que nestas etapas há um risco para as garantias de um processo justo e não-discriminação.

Palavras-chave:

Controle social, derechos humanos, Inteligência artificial (fonte: Thesaurus Criminológico - Instituto Inter-regional de Pesquisa em Crime e Justiça das Nações Unidas - UNICRI). Garantias constitucionais, ferramentas de reconhecimento facial, riscos (fonte: autores).

Introducción

El desarrollo de la inteligencia artificial (IA) ha permitido la creación de un sinnúmero de procesos automatizados, en diversos campos de interacción humana. Con ello, se ha generado una serie de retos para todas las ramas del conocimiento, entre ellas, la disciplina del derecho, la cual ha tenido que adaptarse al constante devenir de los avances tecnológicos, que van desde el *machine learning*, el *big data* y la *robótica,* hasta sistemas de visión como las herramientas de reconocimiento facial, usadas en la persecución criminal.

En ese sentido, se advierte un frecuente cambio social; los medios de producción se actualizan, articulando la cuarta revolución industrial, que ha pasado a dominar cada dimensión de la realidad, tanto de las estructuras económicas como de las superestructuras jurídicas. Los avances vertiginosos de la tecnología suponen una de las situaciones más complejas y demandantes para sistemas rígidos como el derecho, al abrirse la posibilidad de incluir este tipo de tecnologías, que implican la sistematización en su funcionamiento. Todo lo cual genera preocupación en torno a la autonomía de la voluntad individual.

Dentro de las muchas tecnologías derivadas de la IA, se encuentra la categoría de *sistemas de visión*, específicamente la "*image recognition*", definida como

la capacidad de un *software* para identificar lugares, objetos, individuos y acciones en las imágenes. En este escrito, el análisis se centra en las herramientas de reconocimiento facial, su funcionamiento y las consecuencias de su uso para el sistema jurídico, en particular en torno a los derechos y garantías de la ciudadanía.

En este orden de ideas, esta herramienta tiene una importante implicación en la criminología, la rama del derecho penal que busca explicar las posibles causas de la conducta criminal y, de esta forma, anticiparse a la comisión de un delito, a través de la prevención. En virtud de dicho propósito, la colaboración de herramientas tecnológicas representa un gran avance y un cambio en cuanto a la tarea de control social y el aumento de efectividad de la persecución penal, considerando la posibilidad de ubicuidad[1] y reconocimiento, tanto de hechos como de individuos, en tiempo real.

Varios autores han mencionado que, posiblemente, los algoritmos de reconocimiento facial en su mecánica contienen posibles sesgos, al ser implementados. Tal como señaló Worthy (2020), con respecto al caso *Robert Julian-Borchak Williams – Departamento de policía de Detroit*, en el cual se aplicó el algoritmo Face Plus – Digital PhotoManager, para el cual, evidenció una serie de violaciones a derechos fundamentales, sesgos raciales y una elevada tasa de inexactitud en la decisión. Asimismo, Jee (2019) y Perrigo (2020) presentaron evidencias que permitieron determinar que los algoritmos no son completamente neutrales, en tanto las herramientas tienen un margen de subjetividad. Ello, considerando que, además, los datos son obtenidos y conservados de forma inadecuada.

Si bien es cierto que existe preocupación por el uso de estos instrumentos en un ámbito general, no existen análisis específicos en torno a la relación entre dichas herramientas algorítmicas y la posible vulneración de derechos humanos que deben garantizarse en el proceso penal. Es así como el presente artículo analiza los sistemas de reconocimiento facial, a fin de identificar las dificultades y los desafíos de estos algoritmos, que están siendo usados en China, Inglaterra y Estados Unidos, principalmente.

El problema de investigación surge a través de la siguiente pregunta: ¿de qué manera la aplicación de las tecnologías de reconocimiento facial afecta los derechos humanos como los del debido proceso, intimidad, libertad e igualdad, en el marco de las etapas de indagación e investigación propias del proceso penal? Esta pregunta surge debido a la aplicación de tecnologías que tratan los datos biométricos[2] y los implementan en etapas de indagación e investigación, en procesos penales; y su relación con derechos humanos, tales como al debido proceso, la intimidad, la libertad y la igualdad. En esa medida, el trabajo aporta al conocimiento científico, toda vez que revela los riesgos potenciales a los derechos humanos, derivados del uso de herramientas tecnológicas en el proceso penal.

Para alcanzar este objetivo, se empleó una metodología cualitativa de tipo básico jurídico y multidisciplinaria, porque integra sistemas de análisis de las ciencias computacionales que permitirán un alcance descriptivo donde se identifican y analizan los elementos de los algoritmos de reconocimiento facial, que son utilizados para la vigilancia continua e identificación de personas sospechosas de cometer o participar en actividades delictivas. Por tanto, el método utilizado aquí es de tipo deductivo-inductivo, debido a que, primeramente, se realiza el análisis documental de fuentes primarias, secundarias y terciarias que describen el funcionamiento de los algoritmos, para deducir en ellos los elementos sobre los cuales podría generarse un conflicto frente a los derechos humanos. Por ello, es necesario identificar aquellos que se encuentran inmersos en el objeto y fin de la utilización de los algoritmos.

Este artículo expone aspectos trascendentales del entorno tecnológico con respecto a la IA, específicamente, el reconocimiento facial como herramienta para la persecución criminal y disciplina jurídico penal. De la misma forma, se presenta un análisis de algunos de estos mecanismos usados en el mundo y sus repercusiones en los derechos y libertades individuales.

Los resultados se presentan en tres partes. En la primera, se abordan aspectos fundamentales de funcionamiento, aproximando a los lectores al entendimiento de la IA y los ambientes tecnológicos en relación con el derecho penal. En la segunda parte, se unifican las preocupaciones jurídicas y las repercusiones generadas con respecto a sistemas de reconocimiento facial implementados en materia de persecución

1 Ubicuidad es la cualidad de estar presente en varios lugares a la vez, característica que el reconocimiento facial ofrece, pues, por medio de las herramientas tecnológicas, permite reconocer hechos y personas desde un punto remoto.

2 La biometría es definida como la disciplina que estudia los rasgos fisiológicos, morfológicos y los conductuales, de tal forma que mediante el desarrollo de técnicas busca el reconocimiento de individuos mediante rasgos corporales, a esto le sumamos el impulso de las Nuevas Tecnologías de la Información y de la Comunicación (TICs) se tendría una autentificación biométrica aún más fiable para medir y analizar las características físicas y del comportamiento humano con ayuda de la informática. (Mata, 2020)

criminal, enfatizando en las características e ilustrando con algunos ejemplos de casos de Estados Unidos. Finalmente, la tercera parte identifica los riesgos jurídicos más importantes tanto en la parte sustancial como procesal del derecho penal.

Consideraciones metodológicas

Esta investigación toma una perspectiva cualitativa que busca profundizar el análisis y la comprensión de las experiencias humanas frente al fenómeno tecnológico en el derecho (Álvarez-Gayou et al., 2014). De la misma forma, se construye bajo el enfoque interpretativo, en la medida en que busca dar sentido a las situaciones y hechos.

En esta misma línea es posible hablar de una metodología descriptiva que se apoya en la comparación y relación de estudios estadísticos que permitan encontrar características o patrones en el fenómeno que es objeto de estudio, así mismo es posible observar un estudio longitudinal que recolecta datos a través del tiempo, en períodos especificados, con el fin de hacer inferencias respecto al cambio, sus determinantes y sus consecuencias (Müggenburg & Pérez, 2007).

Es documental, pues en ella se consultan, contrastan y analizan datos, por medio de un proceso dinámico de recogida, clasificación, recuperación y distribución de la información que permite una evolución favorable sobre los conocimientos del tema (Gómez & Roquet, 2009). Por lo tanto, el método usado es el de revisión documental, específicamente la técnica de análisis documental que parte de la búsqueda de bases de datos, la cual estuvo centrada en temáticas como los algoritmos de reconocimiento facial, sistemas jurídicos, administración de justicia, relacionadas a lo largo del texto.

La gestión de análisis documental fue complementada con consulta en otras bases de datos, fuentes de información variada y medios periodísticos, clasificados como pertinentes para el desarrollo de la argumentación. También fue necesario usar técnicas como fichas de lectura, cuadros comparativos y tablas analíticas, para extraer sus principales planteamientos, realizar la interpretación y generar los argumentos.

Observaciones preliminares: uso y funcionamiento del sistema de reconocimiento facial en la administración de justicia

¿Qué es el reconocimiento facial y cómo funciona?

La IA presenta una dificultad en cuanto a comprensión, ya que carece de una definición exacta. Por lo que el objetivo de delimitar su alcance resulta ser un reto especial, concretando lo que se conoce como *efecto IA*, entendido como la imposibilidad de encasillar un proceso o método como integrante o derivado de la IA, debido a que cada nuevo avance que demuestre automatización sin actuación humana es considerado IA (Cáceres, 2021).

En la tarea de contextualizar, es necesario hablar de las ramificaciones específicas de IA, que permiten explicar el funcionamiento de las herramientas de reconocimiento facial, tales como el aprendizaje automático (*machine learning*) y los sistemas de visión con *image recognition*.

El *aprendizaje automático* es definido por Kour y Gondhi (2019) como una técnica de IA para entrenar modelos complejos, que pueden hacer que el sistema o la computadora funcionen de forma independiente, sin intervención humana. Así, este método permite identificar patrones en datos masivos con el fin de realizar predicciones que alcanzan cierto grado de autonomía. Dentro del *machine learning* se distinguen características y clases asignadas a cada elemento denominadas etiquetas y atributos, con lo que se configura el objetivo del sistema de aprendizaje automático: construir una función capaz de reseñar y asignar una etiqueta a cualquier objeto que requiera ser analizado (Scantamburlo et al., 2019).

En virtud de lo anterior, la forma de medir la efectividad de un algoritmo de aprendizaje en cuanto a desempeño correcto recae en la tarea de validar la información procesada, midiendo la cantidad de errores que el algoritmo cometa, teniendo en cuenta un número de datos conocidos y tratados previamente, terminando por analizar los resultados en una matriz de confusión[3], para dar claridad a la

3 Una matriz de confusión es una herramienta que permite la visualización del desempeño de un algoritmo que se emplea en aprendizaje supervisado. Cada columna de la matriz representa el número de predicciones de cada clase, mientras que cada fila representa las instancias en la clase real. Uno de los beneficios de las matrices de confusión es que facilitan evaluar si el sistema está confundiendo dos clases.

situación que podría causar suspicacia con respecto a la forma como podría equivocarse una herramienta de reconocimiento facial (tabla 1).

Tabla 1

Matriz de confusión

		Datos actuales	
		Positivo (Perro)	Negativo (Gato)
Datos predichos	Positivo (Perro)	VP (verdadero positivo) 	FP (falso positivo) 
	Negativo (Gato)	FN (falso negativo) 	VN (verdadero negativo) 

La efectividad del algoritmo y su rendimiento son de suma importancia en los sistemas de aprendizaje, debido a que el objetivo de predicción forja a este sistema como una estructura autónoma que brinda beneficios en la aplicación. La probabilidad juega un papel importante puesto que tiene en cuenta un panorama general de la temporalidad, dando importancia a evidencias y experiencias del pasado en forma de datos, para cuantificar actos futuros, según aciertos o errores cometidos en ciertas condiciones controlables.

En consonancia con lo anterior, los algoritmos que usan *machine learning* como proceso para generar una respuesta automática obtienen sus propios cálculos gracias a los datos recopilados por el sistema, usando el método de ensayo y error para perfeccionar sus acciones, dotándolas de mejorías y precisión. Según la Asociación para el Progreso de la Dirección (Redacción APD, 2019), existe una ramificación en cuanto a las clases de aprendizaje automático, donde se incluyen técnicas de reconocimiento.

El *reconocimiento facial* se define como un sistema de métodos y técnicas que permiten determinar la identidad de una persona, mediante el análisis de datos biométricos de carácter físico (iris ocular, ubicación de puntos característicos faciales, etc.) y psicológico, derivados, por ejemplo, de la gesticulación.

Para llegar a una decisión, los sistemas de reconocimiento facial deben cumplir con varios criterios, tales como (1) *universalidad* —indica cómo encontrar una característica común en todas las personas u objetos a reconocer—; (2) *carácter distintivo* —indica si dicha propiedad es suficientemente diferente entre un conjunto de personas u objetos diferentes; (3) *permanencia* —indica la estabilidad en el tiempo de dicha característica—; (4) *colectividad* —indica si la característica es fácilmente adquirida y medida por el sistema; (5) *rendimiento* —indica la precisión, velocidad y coste (recursos) necesarios para llevar a cabo el reconocimiento—; (6) *aceptabilidad* —indica en qué medida los individuos están preparados para aceptar el uso de esta técnica—; (7) *elusión* —indica la respuesta del sistema cuando alguien está tratando de engañarlo (Hernández, 2010).

El reconocimiento facial no requiere la interacción del individuo para su correcto funcionamiento. Sin embargo, con respecto al funcionamiento pueden presentarse dificultades, limitaciones e inconvenientes que podrían generar errores en el momento de emitir una respuesta o resultado. Esas dificultades surgen al analizar las imágenes de quien se quiere identificar, teniendo en cuenta que existen factores como la orientación del rostro, el ruido, la iluminación o la expresión facial, debida a objetos o accesorios, vello facial y envejecimiento (Hernández, 2010) que afectan la calidad del resultado.

Entonces, el uso de métodos como aprendizaje automático y reconocimiento facial en algoritmos representa una ayuda en el análisis desde el punto de vista tecnológico. Ello, teniendo en cuenta la necesidad del derecho de acoplar estas tecnologías de la información para un actuar más eficiente, no solo en temas de manejo de información, sino en toma de decisiones. Dicha adaptación está enmarcada por la implementación de algoritmos de decisión o sistemas de identificación de sospechosos, que hacen de los algoritmos una herramienta cada vez más frecuente en etapas de investigación y juzgamiento en el sistema de administración de justicia en materia penal.

Aplicación e influencia de las tecnologías de reconocimiento facial en el derecho penal

Los sistemas de reconocimiento facial han incursionado en un amplio espectro de vigilancia pública por parte del Estado, teniendo como herramientas principales las cámaras corporales, que permiten el escaneo y el análisis de datos biométricos. Los beneficios que presenta este sistema radican en el control social y la identificación, en la medida en que logran obtener una mayor certeza sobre la identidad del individuo sospechoso y, de ese modo, dinamizan las funciones de seguridad pública y la investigación, las cuales, son utilizadas en gran medida por los departamentos de Policía y agencias de seguridad para favorecer la disminución de la criminalidad (Ragas, 2020).

China es considerada pionera en la aplicación de estas tecnologías enfocadas a la persecución criminal, sin embargo, su implementación en el entorno social y la administración de justicia permite observar una serie de resultados lesivos frente a derechos colectivos e individuales, debido a la tipología de sistema jurídico-político imperante (SecureWeek, 2019). Otros sistemas, más cercanos a la democracia, como Estados Unidos e Inglaterra han realizado proyectos de inserción de algoritmos de reconocimiento facial, carentes de estudios de identificación de riesgos serios, lo cual ha generado una resolución de problemas sobre la marcha, debido a la falta de procesos de planeación y una afectación a cimientos del derecho penal, que van desde los conceptos de prevención general y especial hasta la calidad y mérito probatorio de una decisión algorítmica (Ragas, 2020).

La importancia del reconocimiento facial tiene una mayor repercusión en la recolección del material probatorio en el proceso penal, debido a que permite lograr un mayor grado certeza y determinar si se requiere la activación del aparato judicial por la comisión del hecho antijurídico en una situación específica. La decisión de un algoritmo es epicentro de una discusión jurídica frente a las etapas de indagación e investigación, en la que se pone en duda su carácter científico[4]. La herramienta algorítmica actúa como consultor experto y autónomo para evitar errores humanos (Beriain & Pérez, 2019). Esto nos lleva a comprender que este medio de prueba no es único ni irrefutable, también que se encuentra supeditado a la valoración judicial, la cual reconoce el mérito probatorio y cumplimiento de parámetros científicos en la etapa de juicio (Romeo-Casabona, 2018).

El uso de la tecnología de reconocimiento facial resulta muy efectivo en las etapas procesales, donde los organismos policiales recolectan y aseguran todos los elementos que presenten mérito probatorio, entregándolos al organismo titular de la acción penal. Esto le permite conocer la identidad de los presuntos autores y el cumplimiento de los supuestos legales para investigar la conducta (etapa de indagación). Asimismo, en la etapa en la que se imputan cargos y se fortalece el acervo probatorio con la finalidad de contar de una forma organizada y concatenada los hechos y la teoría del caso (etapa de investigación).

Experiencias en torno al reconocimiento facial y la justicia penal

Como se ha afirmado, el método de reconocimiento facial es muy significativo en la recolección de pruebas y evidencias que permiten establecer el cumplimiento de algunos de presupuestos legales para la configuración de una conducta punible. Su uso es una importante oportunidad estatal de ejercer control social estricto en tiempo real, a fin de prevenir la comisión de delitos e identificar al sujeto pasivo y activo del hecho, reconociendo sus antecedentes de forma eficiente. Estas características han sido muy atractivas para sistemas jurídicos que buscan implementar tecnologías de la información en su funcionamiento.

Según SecureWeek (2019), uno de los países que están a la vanguardia en temas de implementación de herramientas de reconocimiento facial es China. El país oriental tiene las ocho ciudades más vigiladas del mundo, con un total aproximado para 2020 de quinientos setenta millones de cámaras de seguridad en todo el territorio. Ello causa gran inconformismo entre la población que considera que, con ello, se afecta el derecho a los datos biométricos y se sume a la sociedad en un estado de intensa vigilancia. Países como Inglaterra y Estados Unidos han implementado estos sistemas de reconocimiento con mayor moderación y control tanto ético como jurídico con las siguientes herramientas:

1. *Departamento de policía de Londres tecnología Neoface*. En enero de 2020, el Departamento de Policía MET (Metropolitan Police), que tiene una jurisdicción importante en Londres, emitió un comunicado acerca de la implementación del proyecto de reconocimiento facial, ejecutado por la compañía japonesa NEC (Perrigo, 2020). Este

4 Según (Gozaíni, 2015), la prueba científica es un conjunto de elementos de convicción, resultado de avances tecnológicos y de los más recientes desarrollos en el campo experimental, que se caracterizan por una metodología regida por principios propios y de estricto rigor científico, cuyos resultados otorgan una certeza mayor que el común de las evidencias.

sistema de vigilancia tiene el objetivo primordial de identificar personas que se encuentran en una base de datos y que señala que requieren control por parte de la policía. Esto se hace con la finalidad de prevenir la reincidencia o la comisión de conductas contrarias a la ley. Dicha tecnología está basada en IA, con funciones de vigilancia y reconocimiento en tiempo real y cuenta con 627.707 cámaras CCTV.

Sin embargo, algunos han resaltado la inexactitud con la que empezó a funcionar este sistema, según Jee (2019), el 81 % de las decisiones que toma este algoritmo es errado, lo que genera gran desconfianza y preocupación. Ensayos realizados previamente desde agosto de 2016 en el Carnaval de Notting Hill y posteriormente en lugares como Leicester Square, Westfield Stratford y Whitehall en 2017; (Manthorpe & Martin, 2019) concluyeron que cuatro de cada cinco personas identificadas como sospechosas por el algoritmo eran inocentes.

2. *Departamento de policía de Chicago tecnología Clearview*. En el estado de Chicago (Estados Unidos), se ha identificado una serie de métodos usados para el apoyo de la actividad policial, específicamente, en las herramientas de reconocimiento facial. Aquí, toma importancia el caso de la implementación de la herramienta Clearview, como soporte en la recolección de pruebas, identificación de individuos y prevención en la comisión de delitos. Esta tecnología se apoya en los datos obtenidos en plataformas como Facebook o YouTube, que recolectan gran cantidad información por medio de la técnica de scraping[5], que permite el entrenamiento y la posterior toma de decisiones del algoritmo (Beltrán & Preminger, 2020).
3. *Departamento de policía de Michigan tecnología Face Plus – Digital PhotoManager*. La empresa DataWorks Plus fue creada en el 2000, con el objetivo abrir y expandir mercado referente al uso de cámaras y *software* de gestión de fotografías policiales. Posteriormente, desarrollaron herramientas de reconocimiento facial e hicieron más atractiva su adquisición para algunos departamentos de Policía, que usan los siguientes sistemas —tabla 2 (Plus, 2022)

Tabla 2.

Sistemas de reconocimiento facial usados en Estados Unidos por la empresa DataWorks Plus

Departamento de Policía	Sistema utilizado
Departamento del *Sheriff* de Los Ángeles (LASD)	Sistema automatizado de reservas (ABS). Con este sistema, los oficiales de campo pueden usar su tableta o MDT[6], en modo diurno o nocturno, para recopilar información durante un arresto, creando un registro con un número de identificación maestro. Los oficiales de campo y de reserva pueden usar ese número para editar o completar el registro en cualquier momento, lo cual es útil si el oficial que hizo el arresto solo tuvo tiempo de completar los campos obligatorios, antes de que la situación requiriera transporte inmediato. La aplicación es capaz de incluir huellas digitales capturadas, fotos policiales tomadas, e información de licencia de conducir importada, con registros creados por oficiales de campo o editados por oficiales de reserva, realizando el reconocimiento de datos biométricos para establecer la identidad del arrestado.
División de Aplicación de la Ley de Carolina del Sur (South Carolina Law Enforcement Division —SLED)	Sistema Face Plus – Digital PhotoManager. Este sistema ha proporcionado a un servidor central y ha creado una nueva base de datos para inscribir millones de imágenes de reservas faciales del repositorio de reservas estatal de SLED. Lo que permite cargar de forma segura imágenes de sonda para búsquedas rápidas de reconocimiento facial a través de un cliente basado en la web dentro de un navegador web estándar. Los algoritmos de búsqueda garantizan los resultados de las consultas. El sistema FACE Plus también proporciona a SLED muchas herramientas de investigación que maximizan la efectividad de las búsquedas de reconocimiento facial. Los resultados de las coincidencias se pueden imprimir, guardar y enviar por correo electrónico según sea necesario para ayudar con las investigaciones en curso. El *software* Digital PhotoManager también permite crear listas digitales de personas directamente a partir de los resultados de búsqueda de reconocimiento facial. Estas alineaciones también se pueden guardar e imprimir, o se pueden usar para ver testigos seguros para identificar sospechosos de manera positiva.
Oficina del *Sheriff* del Condado de Santa Bárbara	
Policía del estado de Michigan	
Policía del estado de Ohio	
Departamento del *Sheriff* del condado de King	
Policía estatal de Oregón	
Departamento del *Sheriff* del condado de Spokane	

5 Web scraping o raspado web es una técnica utilizada mediante *software* para extraer información de sitios web. Usualmente, estos programas simulan la navegación de un humano en la *World Wide Web* ya sea utilizando el protocolo HTTP manualmente, o incrustando un navegador en una aplicación.

6 Modelo digital de terreno

4. *Proyecto de Wolfcom para proveer de cámaras corporales a Estados Unido*s. El Ministerio de Defensa de Estados Unidos ha tenido la intención de forjar una relación entre la administración de justicia y la IA, representada en la sinergia del sector privado y público, en pro del encuentro de una respuesta a los fenómenos criminales desplegados en las últimas décadas. En 2011, la empresa Wolfcom, pionera en fabricación de cámaras corporales para reconocimiento facial, creó un algoritmo que brinda una decisión sobre edad, género y expresión facial en tiempo real, dicha herramienta tuvo un auge en 2014, producto de un acontecimiento de abuso de autoridad policial[7].

   La empresa se relacionó con el departamento de defensa de Estados Unidos para el uso de esta tecnología en cuerpos policiales como los departamentos de Policía de los Lunas, Nuevo México y Bakersfield, California, así como el departamento del Sheriff del condado de Hardin en Ohio (Gershgorn, 2020). Al ser un algoritmo desarrollado por una empresa privada, el acceso a la información no se encuentra cobijado totalmente bajo los principios de publicidad y transparencia. De modo que los datos sobre los cuales se construyen las decisiones no son debatibles, ni verificables, entendiendo que cada proceso está amparado por el secreto comercial e industrial de una actividad económica.

5. *Caso Robert Julian-Borchak Williams* – Departamento de Policía de Detroit. El reconocimiento facial ha tenido situaciones bastante controversiales, puesto que, como se ha mencionado, el organismo encargado de dinamizar y utilizar este medio probatorio de IA, es la policía. Esta institución tiene la calidad de primer respondiente en los momentos de recolección de pruebas, creando un ambiente propicio para la exposición subsiguiente de la teoría del caso por parte de la fiscalía.

Una situación particular se presentó en el estado de Michigan, que implementó el sistema de reconocimiento facial para persecución criminal, creado por la empresa DataWorks Plus, la cual se ha vuelto reconocida en siete departamentos de Policía de Estados Unidos, por permitir el uso del algoritmo LiveScan Plus - Digital PhotoManager. Con este algoritmo nació el caso de Robert Julian-Borchak Williams un ciudadano de la ciudad de Detroit que fue arrestado tras ser identificado por dicho algoritmo, acusándolo de haber robado cinco relojes, por un valor de casi cuatro mil dólares en una tienda, en octubre de 2018.

El cotejo de las imágenes se hizo por un video de seguridad del establecimiento afectado y la licencia de conducción de Williams. En este caso, el algoritmo realizó una identificación deficiente, debido a la baja calidad y enfoque de la imagen, por lo que era poco clara la decisión del algoritmo, lo cual indujo a la policía a un error en la aprehensión del sujeto (Pérez, 2020).

El departamento de policía de Detroit detuvo a Williams por treinta (30) horas, e impuso una fianza personal de mil dólares. En el interrogatorio, los dos agentes de policía presentaron las imágenes de la cámara de seguridad, confrontándolas con las imágenes de la licencia de conducción del sospechoso. Encontraron que no existía similitud, los agentes decidieron retenerlo para obtener una confesión forzada, aun reconociendo que podría existir una equivocación en la decisión del algoritmo. Con ello, violentaron importantes garantías procesales y sustanciales del sospechoso (Cachemira, 2020). El caso concluyó con una disculpa del fiscal Kym L. Worthy por los perjuicios causados (Worthy, 2020).

El proceso que realiza el algoritmo LiveScan Plus - Digital PhotoManager es tomar una imagen fija de un video de seguridad granulado, denominada *imagen de prueba*, y procesarla por medio del algoritmo que realiza un mapeo de la cara, a fin de reconocer los patrones de los rasgos biométricos particulares del individuo, para cotejarlo con las imágenes de la red estatal de fotos de agencias (SNAP), compuesta por examinadores faciales capacitados, investigadores desde agencias policiales estatales, locales y federales con listas de fotografías digitales y búsquedas. En esta base de datos, se incluyen imágenes del arrestado, datos de identificación (nombre, fecha de nacimiento y edad, etc.); e imágenes del Departamento de Estado. De ese modo, la herramienta emite una decisión en la que se encuentran las coincidencias con los rasgos biométricos más cercanos, en un espacio muestral de 49 millones de fotos (Michigan State Police —MSP, 2019).

Las herramientas que comercializa la empresa DataWorks son desarrolladas por subcontratistas. En el momento de terminación y presentación de la herramienta, la empresa contratante realiza un test de efectividad, que consiste en hacer búsquedas utilizando imágenes de baja calidad de personas que sabe que están presentes en un sistema. Ello se hace sin medir la precisión ni la existencia de sesgos, terminando por definirse como una prueba de carácter no científico, al no cumplir con el rigor que estas exigen.

7 En 2014, se realizó un reconocimiento de un sujeto sospechoso de realizar un hurto menor, a quien se asoció con Michael Brown, que terminó asesinado por un agente de policía de Ferguson, Misuri.

Esta situación deja al descubierto las deficiencias de los sistemas de reconocimiento facial aplicados a la persecución criminal, en torno al respeto de derechos humanos y garantías penales propias de los Estados de derecho. Según Cachemira (2020), el trabajo policial incorrecto y la tecnología defectuosa resultan una mezcla peligrosa, donde se genera gran cantidad de falsos positivos y falsos negativos que perjudican, principalmente, a los afrodescendientes. Manthorpe y Martin (2019), del Instituto Nacional de Estándares y Tecnología (NIST), ha indicado que la existencia de sesgos identifica falsamente a rostros asiáticos y afrodescendientes de diez a cien veces más que a hombres caucásicos. Lo anterior parece ser una constante en los algoritmos predictivos de niveles de riesgo. De ese modo, estas herramientas de reconocimiento facial identifican erróneamente a las personas en los que grupos tradicionalmente discriminados y las minorías.

Debido a lo recién señalado, hay quienes consideran que, en Estados Unidos, se está en presencia de una violación sistemática de derechos, producto del error de un algoritmo de reconocimiento facial. Esta situación demanda un replanteamiento de las políticas públicas de seguridad, que tenga en cuenta la opacidad o falta de transparencia en el funcionamiento de los algoritmos, los eventuales sesgos, el uso de datos insuficientes o de baja calidad y la captura indiscriminada de datos privados. Considerando que esto conlleva prácticas de discriminación, intromisiones injustificadas a la privacidad, manejo indebido de datos personales y falta de regulación específica frente al uso de IA. Todo ello, teniendo en cuenta, además, que cuando la máquina realiza el proceso de aprendizaje automático construye su propia percepción de la realidad, basándose en ocasiones en datos sucios[8], lo cual tiene consecuencias importantes en derechos como la libertad, la igualdad, el debido proceso o la privacidad, entre otros.

Identificación de riesgos de violación de los derechos sustanciales en el reconocimiento facial

Según la Comisión Europea (2019), la implementación de IA en el actuar estatal comprende desafíos o dificultades importantes, con respecto a los derechos individuales y colectivos de los seres humanos. Esto implica la existencia de una planeación holística, donde se tengan en cuenta aspectos jurídicos, económicos, éticos y tecnológicos para un equilibrado funcionamiento de las innovaciones en la realidad social. Las preocupaciones más representativas con respecto a la IA en contraste con el sistema de derechos son:

- Libre albedrío, amenazado por las decisiones de máquinas autónomas
- Existencia de sesgos, discriminación y exclusión de minorías, producto de decisiones algorítmicas
- Perfilamiento algorítmico e incidencia en la decisión humana
- Correcto tratamiento de datos para una decisión algorítmica acertada

En particular, en relación con el uso de la IA en la persecución penal (actividad policial, investigación y juzgamiento de delitos), las inquietudes se generan en el marco de política de seguridad, centradas en el control cada vez más intenso de los ciudadanos, de lo que podría derivarse una violación sistemática de derechos humanos. Ejemplo de ello son las cámaras de seguridad que reconocen e informan a la entidad policial sobre cualquier situación sospechosa o cotidiana, lo que en el marco de sociedades democráticas puede convertirse en el paso hacia estados de vigilancia.

Los derechos humanos consagrados en los instrumentos internacionales que, a su vez, son incorporados en las constituciones y legislaciones de cada Estado tienen restricciones y limitaciones, las cuales se configuran como riesgos al libre y pleno ejercicio de los derechos humanos, para las personas[9]. Especialmente, en los Estados que buscan la implementación de sistemas de reconocimiento facial, bajo la temática de recolección y procesamiento de datos personales.

Debido a que la necesidad de información para alimentar las bases de datos y emitir resultados algorítmicos podría degenerar en un escenario en el que ciertos datos deban ser entregados (o puedan ser capturados) por el Estado para que funja como titular de estos y pueda ejercer sin resistencia el control de sus conciudadanos, propio de un sistema moderno de vigilancia líquida[10] que, según Bauman y Lyon (2013)

8 Según Richardson et al. (2019) los datos sucios son los producidos durante periodos documentados de imperfecciones raciales y políticas sesgadas e ilegales, bajo un sistema de vigilancia policial sucia. Estos datos son producto de la acción de crear datos que aumentan el riesgo de implantar datos inexactos, sistémicos o datos sesgados que alimentan los sistemas de vigilancia predictiva y, por tanto, no pueden escapar del legado de las prácticas policiales ilegales o sesgadas.

9 Artículos 30 y 27 de la Convención Americana Sobre Derechos Humanos, San José de Costa Rica, 22 de noviembre 1969.

10 La vigilancia líquida se define como el control monitorizado, el seguimiento, el rastreo, la clasificación, la comprobación y la observación sistemática que denominamos vigilancia.

cubre actividades de control social bajo el manto del secreto de seguridad nacional, que es uno de los elementos de restricción y limitación a los derechos humanos. Ello ocasiona una posible trasgresión de esos derechos que, por su naturaleza, son del núcleo duro y esencial del ser humano, como los derechos a la honra, la dignidad[11], la libertad y la igualdad, entre otros.

En este sentido, la tecnología de reconocimiento facial ofrece un escenario positivo, en cuanto a la reducción del delito. Pero, a su vez, coarta espacios de actividad de los individuos, al generar un espectro de control que afecta la naturaleza del comportamiento y pensamiento humano, puesto que borra o reconfigura las fronteras entre espacios públicos y privados, por lo que presiona y condiciona la naturaleza amplia y múltiple de los derechos a la intimidad y a la libertad individual y colectiva, debido a riesgos como los mencionados enseguida.

1. *Riesgo en el derecho a la intimidad*. Este es uno de los riesgos que representa mayor preocupación desde el punto de vista de la privacidad como derecho humano. Si bien esta situación debe ser comprendida desde el concepto de una sociedad moderna, caracterizada por la necesidad de consumo y acumulación, inmersa en el intercambio de información y mercancías (Bauman, 2000). Este contexto describe a un individuo que se desprende de su información personal a medida de que avanza la tecnología, proporcionando datos que terminan en los algoritmos que identifican y relacionan conductas por medio de procesos complejos, a partir de información como la localización, búsquedas en internet, época del año, datos biométricos, preferencias para predecir comportamientos; esto conlleva de forma progresiva a que se pierda la sensibilidad de los datos personales, pasando a ser de dominio público y a que dependan de la automatización junto con el Estado como regulador y garante de los derechos.

China es un ejemplo claro de inexistencia de regulación frente al uso de datos personales, en el que se afecta no solo a los nacionales sino también a cualquier persona que tenga interacción con sus sistemas de información, debido a las restrictivas políticas comerciales y a la falta de garantías en el ordenamiento jurídico (Voss et al., 2016), que podría concluir en la no existencia de intimidad o privacidad en una sociedad cada vez más transparente a los ojos de quien ejerce el control social.

2. *Riesgo en la protección de datos personales*. Una de las limitaciones reconocidas por Amnistía International (2021) es la que refiere al derecho a la protección de datos personales, el cual se ve afectado en el momento en el que los datos personales son recopilados, almacenados y procesados por modelos algorítmicos, con fines analíticos. En consonancia, es posible reconocer la intromisión en la esfera del derecho a la privacidad o vida privada[12], relacionado con el tratamiento de la información de movimientos en el espacio público, escáner de datos biométricos, consultas por GPS, información sobre actividades profesionales o laborales, movimientos vehiculares, información sobre tipo de ropa, prendas o pertenencias personales y todos los datos generados, en un proceso de recopilación de información personal (Caso Gillan & Quinton vs. Reino Unido, 2010).

Con respecto a estos procesos de tratamiento de datos en el uso de cámaras de reconocimiento facial, los titulares de los derechos no tendrían manera de autorizar su uso, puesto que el hecho de transitar zonas donde las hayan instalado permite a las autoridades policiales ejecutar actividades de investigación individual y colectiva, con fines de seguridad para reconocimiento y posterior aprehensión, tal y como sugieren modelos predictivos implementados como Clearview[13].

3. *Riesgo en el libre actuar del ser humano*. Identificado como una de las principales consecuencias de control invasivo, que termina por afectar la esfera del derecho humano a la libertad, puesto que, al tener en funcionamiento herramientas de reconocimiento facial con las características de vigilancia que actúan bajo los sistemas de control y poder moderno, es posible encuadrar estas herramientas algorítmicas en el concepto de panóptico (Bentham, 1979). Con ello, se resalta la afectación en el libre actuar de la sociedad, al proyectar sin filtro una realidad carente de zonas de intimidad, donde la libertad esta coartada, como consecuencia de la transparencia, la visibilidad y la predictibilidad de un modelo de disciplina social que tiene un sistema vigilante de carácter automatizado, que identifica hechos y responsables.

Como consecuencia, la percepción del espacio público se redefine, al tener la posibilidad de usar una tecnología que actúa en tiempo real para observar e inspeccionar de forma invasiva la cotidianidad social. De ese modo, se condiciona el comportamiento de las

11 El Artículo 17 del Pacto Internacional de Derechos Civiles y Políticos consagra el derecho a la vida privada y familiar y Artículo 11 de la Convención Americana sobre Derechos Humanos.

12 Artículo 12 de la Declaración Universal de Derechos Humanos (DUDH); el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (CCPR); el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH); y el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea (CFREU).

13 En Europa, la Directiva UE 2016/680 establece la obligación de respetar el derecho a la protección de datos, pues requiere que cualquier autoridad policial realice análisis de información una base legítima de procesamiento adecuada al respeto de criterios de minimización y proporcionalidad.

personas, al sentirse observadas en todo momento, ejerciendo en los seres humanos principios de vigilancia carcelaria como el de "custodia segura"[14]. Así, se establece una herramienta de poder fundamentada en el miedo a ser castigado, que termina por imponer la transparencia invasiva sobre la libertad y plantea un sistema de panóptico moderno y automatizado (Grajales & Marín, 2017).

De igual forma, se reconocen también riesgos a la esfera de la libertad de expresión, centrados en la existencia de herramientas tecnológicas de reconocimiento facial que, si bien tienen en teoría una naturaleza neutra y cuyo objetivo es el aumento de seguridad en la sociedad, pueden ser usadas por el gobierno para afectar a las minorías que actúan como oposición, delimitando su actividad, disminuyendo su fuerza o transgrediendo garantías como la libre expresión, oposición política, reunión pacífica o protesta (Jiménez, 2017).

4. *Riesgo en el derecho a la libertad de expresión*. Este riesgo puede ser visible en la rigurosidad de las políticas de seguridad nacional, puesto que cualquier expresión de desaprobación o crítica puede ser tomada como una posible amenaza y, en virtud del ejercicio del poder, implicaría la puesta en marcha del aparato judicial. Con los sistemas de reconocimiento facial, se materializaría la posibilidad para el Estado de identificar a quienes no estén conformes con el actuar de los entes gubernamentales y, por medio de la manifestación, expresan su inconformidad, estableciendo un escenario de doble trasgresión.

En primer lugar, al vigilar de forma tan invasiva, se crea una situación de incertidumbre para el ser humano, que se encontraría controlado por diversos medios tecnológicos que cambian y se articulan constantemente. Esto limita las acciones humanas cotidianas, redefiniendo espacios y creando escenarios de desconfianza que conllevan a generar angustia existencial. En este estricto sentido, Bauman (2000) expone que pude existir la confrontación entre seguridad y libertad, situación que legitima la seguridad, debido al papel de información cambiante que se difunde y a la fragilidad de los vínculos humanos, denominándolos líquidos[15], puesto que estos son momentáneos, por lo que ante la inestabilidad del mundo las sociedades consideran necesario sobreponer la opción que permita mayor autosatisfacción, supervivencia y facilite el control social.

En segundo lugar, se usa la identificación de sistemas de reconocimiento facial para etiquetar y coaccionar a los individuos que pretendan usar sus opiniones o raciocinios en espacios públicos, castigándolos por expresar su posición de inconformidad de forma pacífica (Romine, 2020), usando el poder punitivo del Estado para imputar delitos políticos a personas con algún grado de influencia y buscando hacer un cambio de perspectiva, pasando de definir a personas como manifestantes y recalificándolos como delincuentes, que terminan por dejar en la conciencia social una aceptación universal del castigo por ejercer tales derechos (Foucault, 2002).

5. *Riesgo en el Derecho de libertad de reunión y asociación*[16]. Este riesgo se identifica, principalmente en las políticas de control propias del ejercicio del poder estatal que somete a los administrados a una vigilancia masiva, no cumpliendo con las obligaciones de brindar garantías a los derechos humanos de asociación y protesta, debido a que con este tipo de tecnología es posible identificar o clasificar a las personas a escala basándose en sus características físicas, tratando los demás datos sensibles; estas prácticas causan una inhibición en la libertad de expresión y opinión[17]. Según Amnistía Internacional (2021), el que exista la posibilidad de identificar a una multitud anónima crea un estado de amenaza que disuade a las personas que deseen asistir libremente a reuniones pacíficas.

Así, comprendiendo que el uso legítimo de la fuerza pertenece al Estado, al igual que la información que individualiza a las personas que hacen parte de manifestaciones por medio de las herramientas de reconocimiento facial, se crea un escenario de incertidumbre. Este estado se basa en la posibilidad de represalias que amedrantan y limitan cualquier acción de oposición político-económica. En tal sentido, el actuar de quienes ostentan el poder político se basa una vigilancia invasiva y represiva, que conlleva a un posible castigo (Foucault, 2002). Se concluye, pues, que esta relación podría generar una trasgresión arbitraría al desarrollo de la libertad de expresión, libertad de reunión o asociación.

Continuando con la identificación de problemáticas relacionadas con los sistemas de visión y reconocimiento facial, se advierten afectaciones

14 La custodia segura consta de una serie de directrices y principios que garantizan control sobre una cantidad de individuos que requieren orden y disciplina, basando su funcionamiento en características de estructuras, recursos e itinerarios para ejercer de forma correcta poder y autoridad sobre el comportamiento.

15 La liquidez de los vínculos humanos hace referencia a los líquidos, pues tienen la cualidad de la fluidez, debido a que estos sufren continuos cambios y no conservan su forma. Entonces, las cosas líquidas no se atan de ninguna forma al espacio ni al tiempo, son libres es su fluir y constante devenir por donde quieran, siempre de manera transitoria.

16 Artículos 15 y 16 de la Convención Americana de Derechos Humanos.

17 Artículo 13 de la Convención Americana de Derechos Humanos.

al derecho a la igualdad[18] y la garantía de no discriminación. Se evidencian, principalmente, en los sesgos algorítmicos y trato diferencial por razones raciales, observadas en el tratamiento policial, por ejemplo, a afrodescendientes, latinos, asiáticos o árabes, en Estados Unidos.

6. *Riesgo en el derecho a la igualdad*. Se identifica una intromisión importante en este este derecho, principalmente, por los errores de los algoritmos reflejados en estadísticas, que afectan en menor proporción a las personas caucásicas y en mayor proporción a las afrodescendientes (Grother et al., 2019), es decir, basándose en el tono racial se construye un nivel de peligrosidad con el que se califican las coincidencias en los rasgos biométricos.

Esta situación es evidente en dos sectores que hacen parte de la cadena de funcionamiento. El primer escenario que se busca describir aplica en las actuaciones policivas que mantienen un prejuicio racial en las etapas de investigación, y es reforzado por la información emitida por los algoritmos de reconocimiento facial. Según Wakefield (2018), el segundo escenario es en las etapas de programación y funcionamiento técnico de los algoritmos, considerando que la mayoría de los programadores contratados mantiene el mismo prejuicio racista y sexista, lo que induce a la trasgresión a la igualdad de las minorías ante los ojos de la ley. Al mismo tiempo, refuerza el trato diferencial hacia ciertos grupos sociales. Entonces, la naturaleza del sesgo puede ser intencional, pero puede derivarse también del tratamiento o la selección inadecuada de datos; inclusive, puede replicar los sesgos y factores de discriminación asentados y normalizados en una determinada sociedad.

La naturaleza de este tipo de herramientas tecnológicas de control social tiene un fundamento filosófico para su aplicación; y corresponde a lo que Bauman y Lyon (2013) denominaron *banóptico*[19]. Este concepto expone la necesidad de una vigilancia de mayor severidad a ciertos sujetos o grupos sociales. La preocupación surge de que la autoridad policial es quien determina qué grupos deben ser vigilados y qué nivel de compatibilidad presenta un sospechoso con la informacion o imagen proyectada por el algoritmo. Este hecho afecta de forma desproporcionada a las comunidades afrodescendientes, puesto que en las bases de datos aparecen datos biometricos de ciudadanos afro en gran cantidad (Garvie & Frankle, 2016).

7. *Riesgo en la creacion de perfiles etnicos*. Es una dificultad reconocida en la construcción de perfiles étnicos[20] en actividades de control, vigilancia e investigación judicial, que resulta nociva para la población en general. Ello, en la medida en que se crea un estado de vulnerabilidad para ciertos grupos sociales con características particulares como la religión, el color de la piel o la ubicación geográfica dentro de una urbe, pues expone a colectivos de personas y sectores a una marginación o no integración efectiva en la sociedad. Lo cual conlleva al refuerzo de los sesgos raciales existentes, que van desde la recolección de datos hasta la actuación de quien ejerza la autoridad para identificar e investigar. Esto llevaría a concluir la existencia de hechos de discriminación, al crear un perfil de personas sujetas a mayor control del Estado, lo que resulta ser, en su mayoría, a personas afrodescendientes, los cuales se enfrentan actuaciones hostiles debido a condiciones étnicas, raciales y socioeconómicas. Por ello, las decisiones tomadas resultan perjudiciales para el derecho expuesto (Meijer & Wessels, 2019).

Desde otra perspectiva, para evitar las violaciones de estos derechos humanos derivados del uso de tecnologías de reconocimiento facial, se requiere que la medida que aplica estas herramientas esté prescrita por la ley y se ajuste a los mandatos legales. Como segunda medida, debe perseguir un fin legítimo. Finalmente, debe ser estrictamente necesaria para lograrlo. A manera de ejemplo: proteger la seguridad nacional o el orden público y llevarse a cabo de manera proporcionada a ese fin (Clérico, 2018).

Pese lo anterior, la proporcionalidad exige límites para el cumplimiento de un fin legítimo; y es la justificación de la necesidad de afectar derechos humanos. Por ejemplo, no se evidencia la proporcionalidad si se instalan y ponen en funcionamiento, sin previo aviso, cámaras para escanear y recopilar datos de todos los rostros que se encuentran dentro de su radio para la elaboración de perfiles sobre la base de que la etnia, la raza, el origen nacional, el género, la condición económica o cualquier otra categoría generan una amenaza a la seguridad nacional.

18 Artículo 24, en relación con el 1.1 de la Convención Americana de Derechos Humanos.

19 Un panóptico es un sistema de vigilancia que por medio de tecnologías permite la elaboración de perfiles con el fin de determinar quién debe ser objeto de una vigilancia estricta. Este planteamiento describe la preocupación de la "(in)seguridad globalizada", junto con el desarrollo de actividades coordinadas de los "gestores de la preocupación", como la policía, los agentes de aduanas y las compañías aéreas.

20 Los perfiles étnicos incluyen el uso de atributos personales (como la raza, el color, la ascendencia, la nacionalidad y el origen étnico), no solo como factores decisivos independientes, sino también en combinación con otros factores.

Sin embargo, por ahora, se proyecta una serie de daños antijurídicos que afectan a las comunidades, independientemente de si se trata de Estados democráticos que reconocen los derechos humanos, puesto que los fundamentos jurídicos y constitucionales estandarte en tales Estados reciben una afectación directa con los novedosos sistemas de vigilancia. Las vulneraciones van desde el ámbito psicológico y conductual por la presión de sentirse vigilado, hasta intromisiones en la intimidad, notorias trasgresiones a la libertad, igualdad, tratamiento de datos y al debido proceso como se detalla enseguida.

8. *Riesgos identificados en las garantías procesales*. Con respecto a las diversas fases de los procesos judiciales, su esencia y rigurosidad están supeditadas al debido proceso, considerado como un conjunto de garantías mínimas articuladas para brindar al procesado un resultado justo y equitativo que se haya mantenido durante las actuaciones judiciales o administrativas. Este fundamento jurídico universal tiene una especial incidencia en el proceso penal, puesto que blinda a las partes respecto del desconocimiento de sus derechos en el desarrollo del proceso penal, estableciendo un equilibrio entre estos y las pretensiones de justicia en torno a la reacción social derivada del delito.

Teniendo en cuenta lo anterior, la mayoría de las dificultades nacen a partir de la implementación de sistemas de reconocimiento facial, que tratan al sospechoso o procesado con arbitrariedad o mayor severidad, desconociendo garantías generales establecidas en la normatividad internacional e interna. Dentro del proceso penal, se identifican importantes situaciones que ponen en peligro el cuerpo mínimo de garantías de debido proceso, según Rescia (1998) deberían considerarse los siguientes riesgos.

9. *Riesgo en la garantía de igualdad procesal.* Este riesgo es identificado en el momento en que se genera un sesgo racial, étnico, o por pertenencia a minorías, creando una distinción no justificable, imponiendo a las minorías un prejuicio en las etapas de creación y recopilación probatoria, que afecta el reconocimiento de derechos, en especial en el momento de aprehensión policial. Existen estudios que señalan que, en el diseño y entrenamiento de los algoritmos, pueden replicarse los sesgos personales del diseñador o los factores de discriminación presentes y normalizados en las sociedades.

10. *Riesgo en la garantía de valoración razonable de la prueba*. Como se mencionó, el material probatorio que emerge de la actividad tecnológica de un algoritmo de reconocimiento facial dentro del proceso penal es clasificado según el análisis de sus elementos y su carácter científico. La decisión algorítmica debe contener un componente tecnológico y metodológico, una serie de principios autónomos y criterios de rigor que otorguen mayor convicción con respecto a otros medios de prueba, estos requisitos catalogan a una prueba como científica (Gozaíni, 2012).

En este orden de ideas se hará énfasis en los criterios de cientificidad mínimos, valorados por un juez, para otorgar valor probatorio dentro del proceso a la actividad de los sistemas de reconocimiento facial. Según Rojas (2014), para probar efectos científicos de una tecnología de estas características deben tenerse en cuenta: (1) los estudios realizados en espacios determinados, proclives y no proclives a la comisión de delitos que demostraran los efectos negativos o positivos de la vigilancia en dichos espacios de convivencia. (2) los estudios estadísticos que revelan cierta similitud entre la estructura social de las zonas elegidas, determinando su peligrosidad, estableciendo coincidencias con cierta tipología de personas y determinando factores incidentes en los delitos cometidos. (3) Los estudios estadísticos que revelan los porcentajes de error de estos algoritmos comprendidos entre falsos positivos y falsos negativos. Y (4) el recálculo (no publicado) de estudios sociológico-estadísticos anteriores que han encontrado una relación causal entre factores sociales, culturales, económicos; la comisión de delitos y las tipologías de delitos predominantes.

El análisis de la tecnología de reconocimiento facial y los estudios realizados con miras a medir su efectividad no ha arrojado resultados totalmente seguros hasta la fecha, lo que permite identificar un riesgo derivado del valor que se otorgue a estas pruebas en el proceso. Por ejemplo, se otorga valor probatorio al sistema japonés NeoFace, implementado en Londres, el cual tiene una tasa de error de 81 % en cuanto al reconocimiento de patrones biométricos (Jee, 2019) y al sistema Norte Americano SolidWorks Plus, cuya probabilidad de equivocarse es 10-100 veces mayor con afrodescendientes que con hombres caucásicos (Grother et al., 2019), lo cual evidencia sesgos raciales y alto margen de error.

Una de las explicaciones que evidencia el estudio de Grother et al. (2019) es la existencia de subcontratación para la creación y puesta en funcionamiento de herramientas de reconocimiento facial, lo que fisura la continuidad en la cadena de producción y genera que estas pierdan el rigor científico, ya que se hace imposible determinar en qué momento se produjeron los sesgos en la creación o la implementación del algoritmo. A lo anterior, se suma que no existen protocolos que guíen su creación ética, que conduzcan a la identificación de tales sesgos, o que obliguen a la incorporación

de auditorías. En ese escenario, la única garantía de estos derechos yace en la valoración probatoria que realice el funcionario judicial sobre los resultados de un algoritmo.

11. *Riesgo en la aplicación del principio de transparencia y publicidad de la prueba*. Acerca de este riesgo, cabe señalar que se encuentra totalmente ligado al principio de contradicción de la prueba y acceso a los medios necesarios para preparar la defensa[21]. Por eso, es una de las garantías del proceso penal más importantes, puesto que se debate acerca de la legalidad y validez de las pruebas, entendiendo que estas son comunes y de acceso para las partes involucradas en el proceso.

Este riesgo es identificado por la relación generada entre la necesidad de publicidad y trasparencia de la prueba dentro del proceso penal, y la protección a la propiedad intelectual en conjunto con el secreto de empresa (Matin, 2019). Cuando los algoritmos o herramientas de IA son desarrollados por empresas privadas, se afecta de forma importante la actividad de la defensa. Ello se debe a que no es posible acceder a información que describa el funcionamiento y arquitectura del algoritmo, a efectos de conocer los criterios considerados para generar una decisión de reconocimiento; la ponderación o correlación establecidos entre ellos; y los datos biométricos sobre los cuales se generaron las coincidencias al realizar el mapeo facial.

12. *Riesgo en el principio de no autoincriminación*. Al respecto es importante resaltar la incidencia de este riesgo en las etapas de indagación e investigación, puesto que después proceso de decisión algorítmica y aprehensión policial, se realiza un interrogatorio intenso, con la finalidad de conseguir una confesión voluntaria, podrían mostrarse imágenes para inducir a que el procesado declare contra sí mismo, lo que afecta el derecho a una sentencia justa, basada en el respeto a las garantías penales relacionadas con la dignidad humana (Cachemira, 2020).

13. *Riesgo en el cambio a un sistema penal acto*. Este riesgo está ligado íntimamente con el papel de la criminología y la política criminal, en su relación con el derecho penal, en la medida en que la implementación del uso de datos biométricos y su tratamiento conlleva la construcción de perfiles sociológico-criminológicos, por medio de métodos como el *big data*, el aprendizaje automático y el reconocimiento facial. Dichas herramientas algorítmicas reconocen y clasifican las facciones del rostro humano y pueden llegar a revivir los ya superados presupuestos Lombrosianos; ya que no podemos perder de vista que, en materia de Biometría, tal como lo refiere Díaz Rodríguez (2013), se enraízan en el famoso Origen de las especies de Darwin, Bertillón, con la fotografía métrica, la eugenesia promovida por Galton sin que podamos dejar por fuera la craneometría de Gall y la antropología criminal popularizada por Cesare Lombroso.

En definitiva, es natural considerar que las garantías del proceso penal reconocidas en tratados internacionales y propias de los ordenamientos internos se encuentran en riesgo, por la implementación de herramientas de reconocimiento facial, sobre todo, en los casos que adquieren relevancia probatoria y no son sometidas a un análisis ético y jurídico que equilibre el funcionamiento de IA, lo que puede concluir en violación sistemática de derechos humanos como los mencionados anteriormente.

Conclusiones

Los algoritmos de reconocimiento facial son herramientas que utilizan sistemas de IA como la *image recognition*, el *machine learning* y el *big data*. La integración de estos métodos, que permite cumplir con funciones de análisis y reconocimiento de datos biométricos de forma casi instantánea, conlleva mejoras en procesos ligados con la investigación criminal, la eliminación de incertidumbre en cuanto a la comisión de los hechos y la reducción importante, en cuanto al tiempo y la calidad en la recolección de elementos probatorios en etapas de indagación e investigación.

El análisis realizado muestra que la implementación de sistemas de reconocimiento facial en materia penal se encuentra, principalmente, en las etapas de investigación, en cabeza de los departamentos de policía que lo utilizan para identificar, aprehender y recolectar material probatorio, lo que puede generar una situación riesgosa para los derechos y las garantías de la persona enfrentada a un proceso penal. Lo anterior, debido a que estas tecnologías consisten en algoritmos capaces de almacenar grandes cantidades de datos, por ejemplo, imágenes y fotografías; y analizarlas hasta encontrar coincidencias que estimen una probabilidad razonable en rasgos biométricos de sospechosos en la comisión de una conducta punible. Sin embargo, estas herramientas presentan una tasa de inexactitud que ronda el 81% en las experiencias registradas en países como Inglaterra y Estados Unidos, en los que se han reportado análisis predictivos inexactos, conllevando impactos desfavorables, en detrimento de derechos y garantías procesales, lo que supone un desequilibrio entre riesgos versus las ventajas ofrecidas.

Entonces, es necesaria una cobertura de los factores de riesgo en los usos de las herramientas

21 Artículo 8.2 de la Convención Americana de Derechos Humanos.

de reconocimiento facial en el escenario penal, considerando que disminuyen la actuación humana en cuanto a carga argumentativa en las actuaciones judiciales o investigativas, favoreciendo un escenario donde el juez da preponderancia al peso de la matemática algorítmica y menos al racionamiento humano. Se ha demostrado que las decisiones de los algoritmos presentan sesgos e información incorrecta o inexacta, lo cual pone en duda su efectividad, terminando por generar afectaciones en materia probatoria y de las garantías que se desprenden del debido proceso.

En principio, se planteaba que la utilidad de herramientas de reconocimiento facial derivaba principalmente de su rapidez, seguridad y exactitud. Pero, a medida que su implementación fue materializándose en los departamentos de Policía de diferentes ciudades, fueron evidentes las dificultades por violación de derechos y los reclamos de la veeduría ciudadana. De ese modo, quedó evidenciada la necesidad de ponderación entre el derecho a la propiedad intelectual de las empresas desarrolladoras y comercializadoras de los algoritmos y el derecho al debido proceso, en cuanto al acceso al funcionamiento del algoritmo como garantía de la posibilidad de controversia del dictamen.

Dado que una de las preocupaciones más representativas fue el cambio de percepción del espacio público con los sistemas de reconocimiento facial, esta transición puede significar el paso hacia un estado de hipervigilancia que afecte el normal actuar de las personas y su sometimiento a un control continuo, lo que termina por afectar la libre determinación como fundamento esencial de la naturaleza humana.

Finalmente, se hace latente la necesidad de realizar estudios ético-jurídicos con respecto al uso de tecnologías, previamente a su implementación, especialmente, en la persecución criminal puesto que los algoritmos de reconocimiento facial no solo miden rasgos biométricos, sino que también reconocen la gesticulación con la finalidad de identificar emociones y hasta reconocer la parte cerebral activa con ayuda de la neurociencia.

Así, se abre una peligrosa oportunidad de acceder a información privada, pues se lograría conocer y modificar la identidad mental, lo que abre la posibilidad del riesgo a los derechos humanos de la esfera individual como la vida, la integridad personal desde el área psíquica, honra y dignidad, libertad e igualdad. Lo anterior implica la creación de regulación específica de restricciones, que respondan a la proporcionalidad y necesidad de la utilización de estas herramientas tecnológicas sobre las garantías fundamentales.

Referencias

Álvarez-Gayou J. L., Camacho, S. M., Maldonado, G., Trejo C. A., Olguín, A., & Pérez M. (2014). *La investigación cualitativa*. https://www.uaeh.edu.mx/scige/boletin/tlahuelilpan/n3/e2.html

Amnistía Internacional (2021, 11 de junio). *Amnistía Internacional pide que se prohíba el uso de tecnología de reconocimiento facial con fines de vigilancia masiva*. https://bit.ly/3DM2Nr9

Bauman, Z. (2000). *Modernidad líquida*. Fondo de Cultura Económica de Argentina.

Bauman, Z. & Lyon, D. (2013). *Vigilancia líquida*. Paidós.

Beltrán, V., & Preminger D. (2020). Inteligencia artificial en el sistema de justicia criminal: Algunas reflexiones sobre su aplicación en el derecho chileno. *Revista de Derecho Aplicado*, *5*(5), 1-17. https://doi.org/10.7764/rda.0.5.9996

Bentham, J. (1979). *Genealogía del poder. El Panóptico*. Ediciones la Piqueta.

Beriain, I. de M., & Pérez, M. J. (2019). La inteligencia artificial en el proceso penal español un echnolo de su admisibilidad sobre la base de los derechos fundamentales implicados. *RDUNED. Revista de Derecho UNED*, (25), 531-561.

Cáceres, A. M. (2021). El impacto de la inteligencia artificial en el Derecho. *Advocatus*, (39), 39-71. https://doi.org/10.26439/advocatus2021.n39.5117

Cachemira, C. D. (2020, junio). Wrongfully accused by an algorithm. *The New York Times*, http://nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

Clérico, L. (2018). *Derechos y proporcionalidad: violaciones por acción, por insuficiencia y por regresión Miradas locales, interamericanas y comparadas.* Instituto de Estudios Constitucionales del Estado de Querétaro.

Comisión Europea —CE (2019). *Comunicación de la comisión al parlamento europeo* (COM 2019 640 final). Autor. https://bit.ly/3y77J6v

Convención Americana sobre Derechos Humanos. Art. 27 y 30, 7 al 22 de noviembre de 1969 (San Jose de Costa Rica).

Díaz Rodríguez, V. (Junio de 2013). Sistemas Biométricos en materia criminal: un estudio comparado. *Revista del Instituto de Ciencias Jurídicas de Puebla, 7*(31), 28-47. https://doi.org/10.35487/rius.v7i31.2013.19

Foucault, M. (2002). *Vigilar y castigar*. Siglo XXI.

Garvie, C., & Frankle, J. (abril de 2016). *The Atlantic*. https://apexart.org/images/breiner/articles/FacialRecognitionSoftwareMight.pdf

Gershgorn, D. (2020, 05 de marzo). *OneZero*. https://onezero.medium.com/exclusive-live-facial-recognition-is-coming-to-u-s-police-body-cameras-bc9036918ae0

Gómez, D. R., & Roquet, J. V. (2009). *Univerisdad de Catalunya*. Metodología de la investigación, Univerisdad de Catalunya. https://bit.ly/3UHlUlm

Gozaíni, O. A. (2012). Pruebas científicas y verdad. *Derecho & Sociedad Asociación Civi*l, (38), 169-175.

Grajales, J. F., & Marín, M. S. (2017). El panóptico más allá de vigilar y castigar. *Revista Kavilando*, 9(2), 511-529.

Grother, P., Ngan, M., & Hanaoka, K. (2019, diciembre). *National institute of standards and technology*. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

Hernández, R. G. (2010, julio). *Estudio de técnicas de reconocimiento facial* (Tesis de grado, Universidad Politécnica de Cataluña). http://hdl.handle.net/2099.1/9782

Jee, C. (2019, 04 de julio). London police's face recognition system gets it wrong 81% of the time. *MIT Technology Review*. https://bit.ly/3LE4KYv

Jiménez, A. G. (2017, 27 de marzo). *Reconocimiento facial: un reto jurídico en la protección de derechos fundamentales*. https://bit.ly/3BCxFrx

Kour, H., & Gondhi, N. (2020). Machine learning techniques. A survey. En J. Raj, A. Bashar y S. Ramson (Eds.), *Innovative Data Communication Technologies and Application*. ICIDCA 2019 (Lecture Notes on Data Engineering and Communications Technologies, vol 46, pp. 226-275). Springer, Cham. https://doi.org/10.1007/978-3-030-38040-3_31

Mata, F. B. (diciembre de 2020). BIOMETRÍA E INVESTIGACIÓN CRIMINAL. *Revista Eletrônica de Direito Processual – REDP., 21*(3), 121-125. https://www.e-publicacoes.uerj.br/index.php/redp/article/view/54200/34874

Manthorpe, R., & Martin, A. (2019 04 de julio). 81% of 'suspects' flagged by Met's police facial recognition technology innocent, independent report says. *Sky News*. https://bit.ly/2J8Jj3h

Matin, N. B. (2019). Algoritmos predictivos al servicio de la justicia. ¿Una nueva forma de minimizar el riesgo y la incertidumbre? *Revista de Facultade Mineira de Dereito, 22*(43), 1-31.

Meijer, A., & Wessel, M. (2019). Predictive Policing: Review of Benefits and Drawbacks. *International Journal of Public Administration, 42(*12), 1031-1039. https://doi.org/10.1080/01900692.2019.1575664

Michigan State Police (2019, septiembre). *Facial recognition – Frequently asked questions. Last revised: June 2022*. https://bit.ly/3ixizOl

Müggenburg, M., & Pérez, I. (2007). Tipos de estudio en el enfoque de investigación cuantitativa. *Revista de Enfermería Universitaria, 4*(1), 35-38.

Pérez, E. (2020, junio). *30 horas detenido por el error de un algoritmo: primer caso de un hombre falsamente acusado por el reconocimiento facial*. https://bit.ly/3ZxE6am

Perrigo, B. (2020, 24 de enero). London Police to deploy facial recognition cameras despite privacy concerns and evidence of high failure rate. Diario *Time*. https://time.com/5770976/london-facial-recognition-police/

Plus, D. W. (2022). dataworksplus.com. Obtenido de https://www.dataworksplus.com/bioid.html#face

Ragas, J. (2020). La batalla por los rostros: el sistema de reconocimiento facial en el contexto del "estallido social" chileno. *Revista Chilena de Estudios Latinoamericanos*, (14), 1-12.

Redacción Asociación para el Progreso de la Dirección —APD. (2019, 04 de marzo). *Qué es machine learning*. https://www.apd.es/que-es-machine-learning/

Rescia, V. M. (1998). *El debido proceso legal y la convención americana sobre derechos humanos*. https://www.corteidh.or.cr/tablas/a17762.pdf

Richardson, R., Schultz, J., & Crawford, K. (mayo de 2019). Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. *New York University Law Review, 94*, 193-228. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333423

Rojas, C. V. (2014). Sobre la cientificidad de la prueba científica en el proceso judicial. *Anuario de Psicología Jurídica, 24*(1), 65-73. https://doi.org/10.1016/j.apj.2014.09.001

Romeo-Casabona, C. M. (2018). Riesgo, procedimientos actuariales basados en inteligencia artificial y medidas de seguridad. *Revista Derecho Empresa y Sociedad, (13)*, 165-179.

Romine, C. H. (15 de enero de 2020). *Instituto Nacional de Estandares y Tecnologia*. Instituto Nacional de Estandares y Tecnologia. https://www.nist.gov/speech-testimony/facial-recognition-technology-part-iii-ensuring-commercial-transparency-accuracy

Scantamburlo, T., Charlesworth A., & Cristianini, N. (2019). *Machine decisions and human consequences*. https://arxiv.org/ftp/arxiv/papers/1811/1811.06747.pdf

SecureWeek (2019 19 de agosto). *Las ciudades más vigiladas del mundo*. https://www.secureweek.com/las-ciudades-mas-vigiladas-del-mundo/

Voss, A., Hohlmeier, M., Gál, K., & Boni, M. (2016, 17 de junio). *Personal data transfers to China - what protection for EU citizens?* https://www.europarl.europa.eu/doceo/document/O-8-2016-000091_EN.html

Wakefield, J. (2018, 20 de junio). Así funciona "la mente" de Norman, el algoritmo psicópata del MIT que solo ve lo más tenebroso de la red. BBC Mundo. https://www.bbc.com/mundo/noticias-44482471

Worthy, K. L. (2020). *WCPO statement in response to New York Times article wrongfully accused by an algorithm, June 24, 2020*. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html