Rostros en la mira: El dilema del Reconocimiento Facial en Bogotá

Daniela Alejandra Prieto Otálora

Director
Diego Alonso García Ramírez

Título por el que opta

Profesional en Periodismo y Opinión Pública

Escuela de Ciencias Humanas

Periodismo y Opinión Pública

Universidad del Rosario

Bogotá - Colombia

2025

ERRORES QUE MARCAN ROSTROS:

De ama de casa a sospechosa por un fallo tecnológico

A las 2 de la tarde, una mujer disfruta un momento familiar en casa con su esposo y sus dos hijas, viendo televisión. De pronto, suena el timbre. Al abrir la puerta, se encuentra con seis policías que le informan que tienen una orden de captura contra Porcha Woodruff por robo violento de un automóvil.

Sorprendida, la mujer señala su avanzado embarazo como prueba de que no puede ser culpable. Sin embargo, es arrestada frente a su familia y llevada a un centro de detención, donde permanece 11 horas. Durante ese tiempo, sufre contracciones, es maltratada verbalmente y recibe atención médica negligente. A pesar de insistir en su inocencia, los agentes revisan su celular buscando pruebas que la incriminen.

Woodruff pasó horas detenida antes de ser acusada de atraco y robo de automóvil con violencia. Para quedar en libertad, ella y su esposo pagaron una fianza de 100.000 dólares, usando sus ahorros para comprar vivienda. Un mes después, el fiscal del condado de Wayne (Estado de Michigan) cerró el caso por falta de pruebas. Sin embargo, el incidente dejó secuelas que afectaron su acceso al empleo y al crédito

Porcha Woodruf, víctima de arresto por supuesta complicidad en un robo según datos obtenidos de un algoritmo de Inteligencia Artificial (IA).

Fotografía: Nic Antaya para el medio The New York Times.

Porcha Woodruff ha sido una de las víctimas de la infraestructura tecnológica de seguridad implementada en la ciudad de Detroit, estado de Michigan, Estados Unidos. Esta infraestructura incluye sistemas avanzados de circuitos cerrados de televisión (CCTV), que no solo monitorean constantemente el entorno urbano, sino que también incorporan funciones de inteligencia artificial.

Entre sus capacidades se encuentra el reconocimiento facial, una tecnología que analiza los rasgos de una persona para compararlos con bases de datos y determinar su identidad. En otras palabras, se trata de sistemas de reconocimiento facial (Facial Recognition Systems).

Más allá del riesgo inherente a la vigilancia constante de una ciudad, el uso del reconocimiento facial plantea preocupaciones adicionales. Lo más inquietante es cómo se han configurado estos sistemas: qué comandos se les han asignado para operar y, sobre todo, quiénes han tomado esas decisiones.

El rápido avance tecnológico de la última década se refleja en objetos cotidianos como neveras inteligentes, automóviles, datáfonos o reguladores de luz, que facilitan nuestra vida diaria. Estos dispositivos funcionan gracias al Internet de las Cosas (IoT), concepto que, según The Internet Society, describe entornos donde la conectividad y el procesamiento de datos se extienden a objetos comunes, permitiéndoles generar e intercambiar información con mínima intervención humana.

En hogares y lugares de trabajo es común encontrar estos dispositivos conectados a redes inalámbricas, procesando datos constantemente para personalizar su funcionamiento. Sin embargo, esto plantea preocupaciones sobre la sensibilidad de los datos tratados: ¿quién los recopila?, ¿qué tipo de datos son?, ¿con qué fin se usan?

Estos dispositivos han tenido éxito en seguridad y vigilancia, como las puertas inteligentes conectadas a alarmas y cámaras, o los sistemas CCTV comunes en espacios públicos y privados. Aunque suelen cubrir áreas pequeñas, pueden ampliarse para monitorear zonas enteras, incluso ciudades como Bogotá o Detroit, como en el caso de Porcha.

Creando un caso hipotético de una metrópoli activa las 24 horas con múltiples desafíos sociales, la seguridad requiere instituciones eficientes, pero es difícil contar con suficiente personal para vigilar toda la ciudad. Por eso, se recurre a herramientas de IoT que ayudan en esta tarea, aunque presentan retos económicos, tecnológicos y de infraestructura para su implementación.

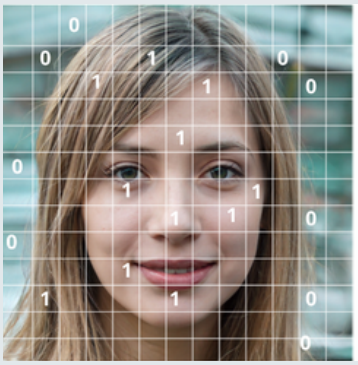
Ciudades de todo el mundo han enfrentado este desafío con resultados diversos. En 2025, Estados Unidos destina el 10,25 % de su PIB a defensa, unos 849.800 millones de dólares, según Datosmacro.com. Esta inversión impulsa el desarrollo de armamento avanzado, estrategias militares sofisticadas, sistemas de comunicación modernos y tecnología inteligente.

El reconocimiento facial ha ganado terreno en el sector de la seguridad, con un valor estimado de 6,61 billones de dólares en 2024 y proyecciones de alcanzar los 14 billones en 2029, siendo América del Norte el principal mercado. Este crecimiento despierta interés por conocer el origen de la tecnología y sus pioneros.

LOS ALGORITMOS DEL RECONOCIMIENTO:

cuando las matemáticas identifican rostros

El reconocimiento facial, conocido como RF, ha ganado popularidad en la última década gracias a dispositivos que lo incorporan. No obstante, sus inicios datan en los años sesenta con los investigadores norteamericanos Woodrow Wilson Bledsoe, Helen Chan Wolf y Charles Bisson pertenecientes a la compañía Panoramic Researchque desarrollaron las primeras semillas de lo que se conoce como patrón de reconocimiento automatizado.



A partir de la división en cuadrículas de imágenes en donde cada casilla se clasificaen 1 correspondiente a llena o 0 equivalente a vacía. Para así después, sumar cada uno de los espacios y compararlos con puntajes similares de otras imágenes.

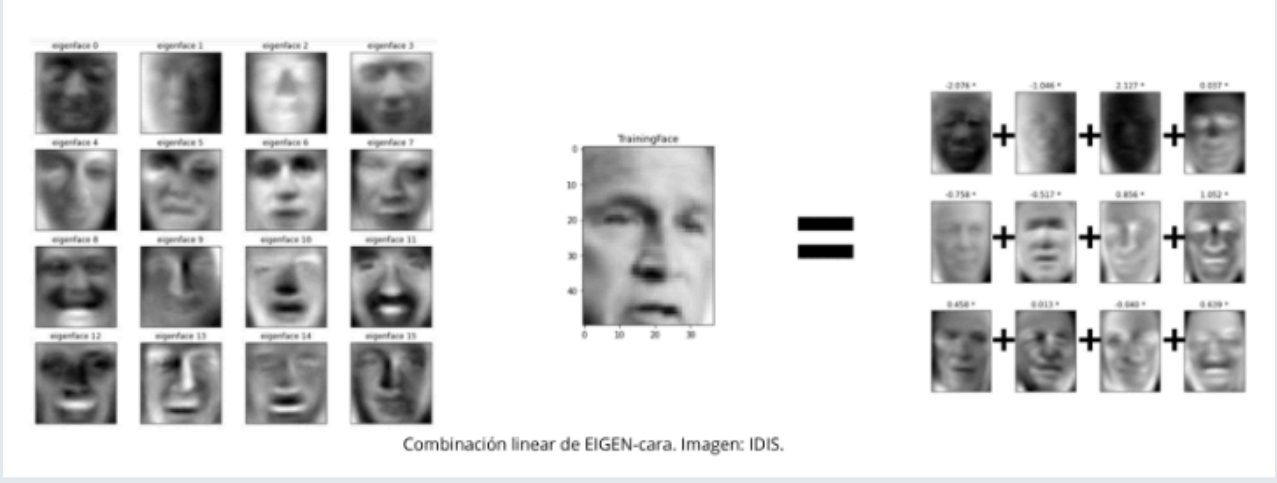
Modelo de Reconocimiento Automatizado diseñado por Woodrow Wilson Bledsoe. Imagen: Autoría propia.

El periodista Shaun Raviv, en su reportaje para Wired titulado “The Secret History of Facial Recognition”, narra la historia de Woody Bledsoe, pionero del reconocimiento facial. Raviv destaca el uso de la n-tupla, una secuencia matemática que agrupa coordenadas de imágenes faciales, como el primer paso hacia la automatización.

Bledsoe llamó a su avance “computer person” y lo probó con diez rostros humanos, según relatan Mark Andrejevic y Neil Selwyn en su libro Facial Recognition. Su trabajo atrajo el interés de agencias como la Agencia Central de Inteligencia, por su sigla en inglés CIA, aunque no hay registros oficiales que lo confirmen, salvo una solicitud del Departamento de Defensa en 1965 para identificar antecedentes raciales.

Se utilizaron registros policiales para probar el sistema comparando rostros de personas buscadas con una base de 400 hombres caucásicos. En los años sesenta, Panoramic Research marcó un hito al desarrollar reconocimiento facial en contextos como expresiones, envejecimiento y vello facial, aunque sus modelos eran exclusivamente de hombres blancos. Previamente, ingenieros de Bell Telephone Laboratories identificaron dos rasgos únicos —protuberancia de orejas y separación de cejas— como claves para la identificación.

En los años ochenta, los matemáticos Lawrence Sirovich y Michael Kirby desarrollaron la técnica de EIGEN-caras, que combina múltiples imágenes faciales en una sola para identificar patrones comunes. Concluyeron que esta técnica permite reconocer tanto un rostro promedio como sus rasgos distintivos.



Combinación linear de EIGEN-cara. Imagen: IDIS.

Con el tiempo, esta tecnología dejó de ser exclusiva de laboratorios y autoridades, integrándose silenciosamente en la vida cotidiana a través de redes sociales.

DE LA SELFIE AL MUNDO:

El Reconocimiento Facial en la vida cotidiana

El reconocimiento facial pasó de ser exclusivo de las autoridades a difundirse con las redes sociales. Una simple selfie, al publicarse, deja de ser privada y queda expuesta a quien pueda acceder a ella.

Al publicar una imagen en redes sociales, esta queda accesible para miles de personas, pero lo más valioso son los datos que contiene: rostros y actividades. Aunque parezcan irrelevantes, son altamente valiosos para agencias de seguridad y empresas. Al crear una cuenta en Instagram, se aceptan términos sin leerlos, lo que permite a la app acceder a datos personales como nombre, fecha de nacimiento, correo y rostro. Aunque se confía en su manejo seguro, estos datos pueden ser utilizados por terceros, incluso entidades externas, mediante tecnologías de reconocimiento facial, lo que plantea preocupaciones sobre privacidad y control.

Clearview AI ha sido destacado por medios como RTVE, BBC, La Vanguardia y Times Magazine por su uso en diversos contextos, incluyendo la guerra en Ucrania, donde ha servido para identificar infiltrados rusos, investigar crímenes de guerra y reconocer personas fallecidas.

Estudios han demostrado lo fácil que es extraer datos de redes sociales. Uno de ellos, de la Universidad de Uppsala, titulado Surveillance Using Facial Recognition and Social Media Data, destaca que herramientas como APIs y web scraping permiten recolectar información visual de plataformas como Facebook e Instagram.

Para identificar rostros, se requieren tecnologías avanzadas capaces de analizar millones de imágenes. Una de las más polémicas es Clearview AI, empresa mencionada por The New York Times, que afirma haber creado su base de datos con fotos disponibles en internet, utilizando plataformas como SocialMatter.

Por otra parte, se empleó por parte de las autoridades estadounidenses para identificar a los responsables del asalto al Capitolio en 2021 y en casos de explotación infantil.

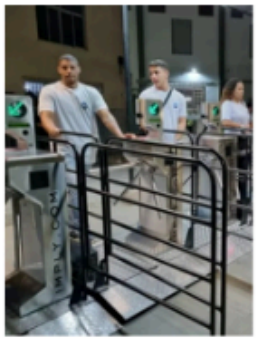
Clearview AI se promociona como una herramienta eficaz para la justicia, destacando su papel en la seguridad pública y privada. Afirma ser líder en EE. UU. y el mundo occidental, con más de 40 mil millones de imágenes y una precisión del 99,9 % en identificación étnica.

Aunque afirma trabajar con gobiernos y empresas, no especifica cuáles. Se presenta como una empresa privada que usa imágenes “públicas” de Internet, sin aclarar qué significa eso, lo que genera preocupaciones sobre el uso no consentido de fotos personales. Esto implica que cualquiera podría estar en su base de datos sin saberlo, lo que plantea serias dudas sobre la privacidad. Además, tecnologías similares se están adoptando en Latinoamérica sin suficiente transparencia.

LATINOAMÉRICA,
entre la innovación y la protección de derechos

Ahora bien, Latinoamérica no se queda atrás con esta problemática. Es cuestión de consultar los medios, que con titulares de celebración aplauden la nueva adquisición tecnológica del estadio del club de fútbol Vasco Da Gama, conocido popularmentecomo Estadio São Januário, ubicadoen la ciudad de Río de Janeiro, Brasil.

Allí medios locales como Vasco, O Globo y GE anunciaron la aplicación de una sistema de reconocimiento facialen el año 2023, donde lo catalogan como un método efectivo para el ingreso de aficionados, miembros y visitantes “el promedio de accesos por minuto fue de 400 aficionados” citó el medio HeadTopics. En este caso, ya no está la necesidad de imprimir el boleto o llevar el código QR en el celular para el ingreso a un juego, simplemente con el escaneo del rostro es suficiente para validar el ingreso.



Máquinas de Reconocimiento Facial que favorecen el ingreso al estadio. Imagen: Tébaro Schmidt/ge - Divulgação / Imply

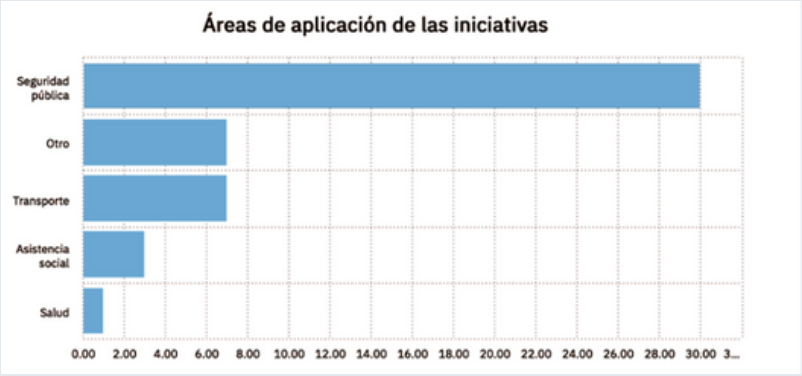
Además de Brasil, la región latinoamericana también ha adoptado esta tecnología en diversas áreas donde el uso común recae en la seguridad. Así lo describe una investigación realizada por AlSur, un conjunto de once organizaciones de la sociedad civil y la academia de América Latina que buscan fortalecer los derechos humanos en el entorno digital dentro del informe titulado.

"Reconocimiento facial en América Latina: tendencias en la implementación de una tecnología perversa".

El informe analiza el uso creciente del reconocimiento facial en la región, señalando su carácter invasivo, impreciso y discriminatorio, especialmente hacia personas racializadas, mujeres y personas trans. Tras estudiar 38 iniciativas en 9 países, revela una preocupante falta de regulación y transparencia, mientras gobiernos y empresas lo aplican para vigilancia, seguridad y control migratorio.

Tipos de áreas en donde se aplica el uso de Reconocimiento Facial en Latinoamérica.

Gráfica: AlSur.



Un caso similar al de Porcha Woodruff ocurrió en Buenos Aires, Argentina, donde Guillermo Ibarrola fue encarcelado durante una semana por una falsa alerta del Sistema de Reconocimiento Facial de Prófugos (SRFP). Según El Clarín, el error se debió a una orden de detención mal elaborada: el verdadero prófugo tenía el mismo nombre, pero vivía en otra zona. Un fallo humano en la identificación provocó que la alerta se emitiera contra el Ibarrola equivocado, residente de Ezeiza.

Ibarrola fue detenido en una estación de trenes tras ser identificado como supuesto prófugo de un violento robo cometido en el año 2017.

Imagen: El Clarín Argentina.

Este caso, difundido por medios como Infobae, El Clarín, WIRED en Español, generó controversia en 2019 entre organizaciones defensoras de derechos digitales en Argentina, como el CELS y la Fundación Vía Libre, que acudieron a instancias legales para solicitar la suspensión del sistema. El Sistema de Reconocimiento Facial de Prófugos (SRFP), implementado ese mismo año para identificar prófugos, era operado con el software Danaide S.A.

Una orden judicial suspendió indefinidamente el sistema, pese a que el gobierno defendió su efectividad tras capturar 1.743 prófugos. Las partes acordaron elaborar un plan conforme a los requisitos de una auditoría que supervise su uso.

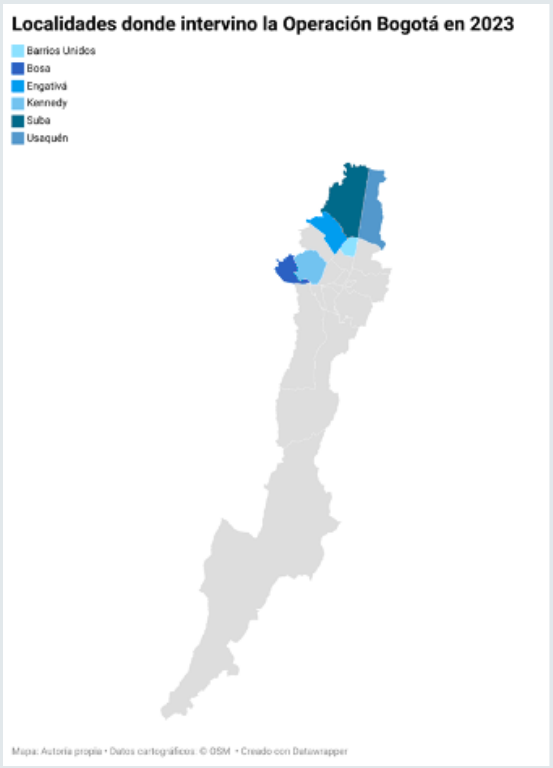
OJOS DIGITALES SOBRE LA CAPITAL:

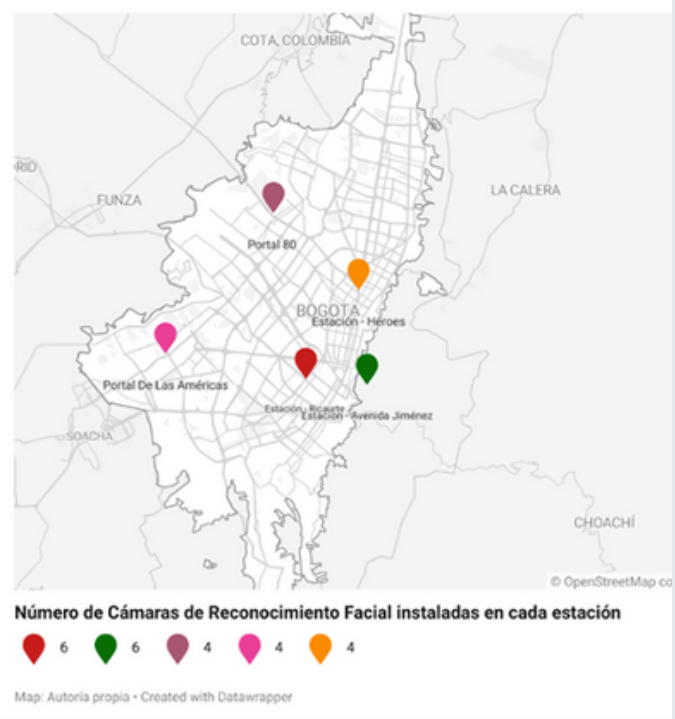
Tecnología y Seguridad en Bogotá

Aunque en otros países el reconocimiento facial ha sido restringido por fallos judiciales, en Bogotá su uso sigue en expansión. Desde octubre de 2023, la Policía Metropolitana implementó el software Corsight AI en TransMilenio, con 783 cámaras activas como parte del plan piloto “Operación Bogotá”, coordinado con la Fiscalía y autoridades distritales por orden del expresidente Iván Duque y el exministro Diego Molano.

La operación involucró recursos humanos, profesionales, logísticos y tecnológicos para prevenir delitos y proteger la tranquilidad ciudadana. Se ejecutó en seis localidades: Barrios Unidos, Bosa, Engativá, Kennedy, Suba y Usaquén, como lo muestra el mapa.

Como lo informa el comunicado de prensa publicado en el año 2023 por la Policía Nacional anunciando esta operación, uno de los pilares fue la adquisición de herramientas tecnológicas capaces de “identificar, plenamente y en tiempo real, a cualquier persona y verificar sus antecedentes, mediante huella dactilar, reconocimiento facial o el iris”. Como resultado de la operación, se instalaron 24 cámaras de reconocimiento facial en cinco estaciones de Transmilenio con alto flujo de personas: Portal 80, Héroes, Ricaurte, Portal Las Américas y Avenida Jiménez. Estas fueron seleccionadas por su alta afluencia de usuarios y frecuencia de hurtos.





Varias de las estaciones seleccionadas coinciden con una nota de prensa de la Personería de Bogotá (2023), que identificó las estaciones con más denuncias por hurto: Avenida Jiménez, Universidades, Portal Norte, Banderas, Calle 76, Las Aguas, Marly, Calle 72 y Calle 26.

El objetivo de emplear cámaras de reconocimiento facial era identificar individuos que contaran con orden de captura judicial vigente en la ciudad de Bogotá. El comandante de la Policía de Transmilenio, para ese entonces el teniente coronel, Jader Llerena, explicó a varios medios de comunicación como El Espectador, RED +, El Tiempo, entre otros, que para el funcionamiento de este sistema se esperaba contar con una base de datos de aproximadamente 5 mil personas con antecedentes judiciales vigentes en la capital, cedida por la Registraduría Nacional. Llerena explicó que, al tratarse de un piloto, el sistema permitiría identificar fallas y fortalezas para evaluar su implementación futura.

Medios especializados como Business Wire,Biometric Update e Ifsec Insider difundieron esta información. Según notas de prensa, las cámaras alertaron a las autoridades sobre 10 sospechosos con orden judicial, logrando la captura de 6 (1 por homicidio y 5 por hurto).

Andrés Macias, experto en seguridad y docente de la Universidad Externado de Colombia, se refiere a la posible razón detrás de los escasos resultados conocidos sobre este plan piloto. En primer lugar, señala que “debería hacérsele el seguimiento correspondiente para ver si funciona o no”. Aunque aclara que no se puede afirmar que el proceso no se haya llevado a cabo, enfatiza que los resultados posiblemente no fueron socializados adecuadamente con la población.

Reflejo de esta hipótesis es la falta de interés por parte de las autoridades para divulgar información completa sobre este tema hacia la población, ya sea por "... por ejemplo, no funcionó y no les interesa que se evidencie que no funcionó o porque no es la prioridad. Entonces hay otros temas que son más urgentes y mayor inmediatez que requieren más atención. Puede que también sea por un cambio en las prioridades de problemas públicos de la administración (de ese entonces)".

Por otra parte,Macías enfatiza en la imposibilidad de asegurar que a partir de los resultados arrojados por la institución frente a los SRF, de un veredicto de si es una herramienta funcional. Sustenta su postura respecto a que las rúbricas establecidas por las autoridades para evaluar este artefacto pudieron contener indicadores bajos o simplemente que no se planteó un objetivo de concreto que diera indicios de utilidad.

Esta falta de criterios claros para evaluar su efectividad contrasta con el hecho de que el reconocimiento facial no es una novedad en la ciudad, sino una herramienta que ha sido implementada desde hace casi una década.

UN RECORRIDO DE CÓMO LA CAPITAL

adoptó el Reconocimiento Facial

Aunque el sistema se presenta como novedoso, registros mediáticos indican que los SRF existen en Bogotá desde 2016, como parte de políticas de seguridad implementadas por las administraciones de Gustavo Petro, Enrique Peñalosa, Claudia López y Carlos Fernando Galán.

Desde 2016, Bogotá ha intensificado el uso de cámaras con reconocimiento facial como parte de su estrategia de seguridad urbana. Ese año, bajo la administración de Gustavo Petro, se instalaron 24 cámaras en estaciones de TransMilenio, con una inversión superior a los 7.700 millones de pesos. Tres años después, durante el Paro Nacional, la Policía Metropolitana admitió haber utilizado esta tecnología para identificar a manifestantes involucrados en disturbios.

En 2022, se creó el Centro Nacional de Monitoreo, que cuenta con más de 200 cámaras en el sector de San Victorino, impulsado por la administración del centro comercial GranSan.

La expansión continuó en 2023 con la Operación Bogotá, que sumó 788 cámaras biométricas conectadas al sistema de transporte masivo y a una base de datos de más de 5.000 personas. Mientras que, en 2024, la tecnología se trasladó a los escenarios deportivos con 100 cámaras instaladas para detectar asistentes con antecedentes judiciales durante la final de la Liga Betplay.

Línea del tiempo sobre la aplicación del uso de Reconocimiento Facial en la ciudad de Bogotá

Gráfico: Autoría propia.

Para conocer el estado actual del reconocimiento facial en Bogotá, se revisaron notas de prensa de 2023 y 2024. Ante la escasa información pública, se consultó a las autoridades sobre los beneficios de estas cámaras. Aunque fueron parte del piloto de la Operación Bogotá, muchas siguen instaladas. El objetivo fue entender cómo se percibe el sistema y su situación actual.

Por eso, se envió un derecho de petición a tres entidades: Policía Metropolitana de Bogotá, Secretaría de Seguridad y Convivencia y Transmilenio.

El 9 de junio de 2023 se radicó un derecho de petición a Transmilenio S.A.S. solicitando información sobre ubicación, cantidad, propósito, operatividad, indicadores de éxito, proceso de licitación y entidades vinculadas al uso de cámaras de reconocimiento facial. La entidad respondió lo siguiente:

“TRANSMILENIO S.A. A la fecha no cuenta con un sistema de reconocimiento facial operando en su sistema de video vigilancia, es de aclarar que este tipo de tecnología para efectos judiciales es de potestad única de autoridades competentes. Por lo tanto, dando respuesta a los puntos II, III, IV, V y VI donde solicita le sea suministrada información sobre... (las preguntas enviadas). Como se indicó en el punto (i), TRANSMILENIO S.A. A la fecha no cuenta con un sistema de reconocimiento facial operando en su sistema de video vigilancia”.

Sin embargo, notas de prensa exponen la existencia desde el año 2015 del Sistema Integrado de Videovigilancia Inteligente para Transmilenio (SIVIT) durante el gobierno del entonces alcalde, Gustavo Petro. Este sistema fue implementado por el Fondo de Vigilancia y Seguridad de Bogotá y tenía el objetivo de garantizar la seguridad de la población que hace uso del sistema de transporte masivo –Transmilenio-. Estaba compuesto de elementos de video vigilancia concretamente de 24 cámaras de reconocimiento facial instaladas en 10 estaciones del sistema.

Map: Autoría propia - Created with Datawrapper

El software inicial adquirido para hacer uso de este sistema se llamaba FaceFirst encargado de “que, en el momento del cotejo, generaba una alarma visual y sonora desde un servidor central al operador indicando la coincidencia” según lo respondido en el derecho de petición por la entidades de transporte. La base de datos, denominada en el documento legal como “lista negra” empleada para el funcionamiento de este software iba a ser suministrada por parte de la Policía Nacional.

No obstante, la entidad aceptó que el modelo de reconocimiento facial dentro del SIVIT nunca funcionó debido a que FaceFirst no se activó por la falta de la "lista negra" que iba a ser cedida por parte de esta autoridad. De modo, que en el 2018 la Secretaria Distrital de Seguridad, Convivencia y Justicia reactivó estas cámaras como apoyo de vigilancia, pero sin la herramienta del reconocimiento facial y siguen vigentes hasta la actualidad.

Titulares del año 2023 como: "Así funciona el sistema de reconocimiento facial que se implementa en Transmilenio" de Noticias RCN, ***"TransMilenio los estará observando: instalan más de 700 cámaras con software de reconocimiento facial"***

Ante la respuesta negativa de la entidad con el uso de SRF, en vez de generar respuestas aparecen más dudas e incluso incertidumbre frente al por qué una entidad niega el uso de estos artefactos cuando existenregistros en los medios de comunicación que confirman lo contrario. Notas de prensa de Publimetro o de la misma Alcaldía de Bogotá. son pruebas de su existencia.

Con el fin de indagar aún más sobre las razones por las cuales se niega el uso de este sistema por parte de Transmilenio, se decidió enviar otro derecho de petición el día 28 de junio del 2023. Esta vez cuenta con la particularidad de exponer exactamente la situación expuesta por los medios y cuestionarles el por qué la negación de su uso. A diferencia del primer radicado, este se notificó su traslado a la Secretaría de Seguridad el día 13 de julio del 2023, con el fin de dar respuesta.

El 24 de julio de 2024 se notificó que la entidad no podía responder y trasladó el caso nuevamente a Transmilenio con otro número de radicado. Esto evidencia demoras y falta de coherencia en la comunicación entre entidades.

Es así, que finalmente la Secretaría de Seguridad de Bogotá envía un documento dando respuesta a la pregunta el proceso de licitación y contratación de estos equipos. Allí notifican que por medio del contrato 880 de 2014 que cuenta con un valor inicial de $7.753.870.425 mil millones de pesos para la Empresa de Telecomunicaciones de Popayán S.A. EMTEL E.S.P. No obstante, el valoral final de contrato el 18 de septiembre de 2015 fue de $11.758.251.357 mil millones de pesos.

Dentro de las funciones del contratista eran “Coordinar esfuerzos técnicos, logísticos, administrativos y financieros para desarrollar una solución integral en tecnología, información y comunicaciones que permita implementar un sistema inteligente de videovigilancia en Transmilenio. Este sistema incluiría reconocimiento facial, identificación de individuos y generación de alertas, con el fin de fortalecer la seguridad en el transporte público, conforme al convenio 782 del 9 de diciembre de 2014.”.

Lo llamativo en la respuesta de la Secretaría de Seguridadde la respuesta de la Secretaría de Seguridad es su reiterada negación sobre la adquisición de esta tecnología, a pesar de que existen registros públicos que indican lo contrario. Pero, confirman que en el año 2023 realizaron la compra e implementación de un Sistema de Analítica de Video fuera de línea (forense) para que *“apoye y facilite el cumplimiento de la misionalidad en la operación e investigación en la comisión de delitos y/o contravenciones que afecten la seguridad y tranquilidad de los ciudadanos”*.

A diferencia de un sistema de reconocimiento facial, esta captura todos los datos emitidos dentro de un video almacenado y los compara posteriormente con fuentes de imágenes para generar similitudes y así tomar decisiones.

Respecto a quién gestiona las cámaras, las entidades coincidieron en el Centro de Comando, Control, Comunicaciones y Cómputo (C4). Creado durante la segunda administración de Enrique Peñalosa, este centro integra los servicios de emergencia para ofrecer respuesta rápida las 24 horas. Depende de la Secretaría de Seguridad y reúne instituciones como la Policía Metropolitana, la Línea 123, el Cuerpo Oficial de Bomberos (UAECOB), entre otros. Está equipado con cámaras de videovigilancia, software, radios y operadores telefónicos.

El C4 supervisa gran parte de las cámaras de seguridad en espacios públicos de Bogotá, como estaciones de Transmilenio. A través de su directora, Ada Luz Sandoval, respondió al derecho de petición negando la adquisición de dispositivos de reconocimiento facial.

Una de las preguntas que se le realizó al ente fue respecto al número de cámaras con el que cuentan y en qué ubicación están. A lo que la entidad no brindó respuesta por este medio, sin embargo, en un documento externo se evidenció que para la empresa de TransMilenio S.A.S. existen dos modalidades en lo que respecta el uso de cámaras de seguridad dentro de las estaciones, portales y vehículos de transporte.

Una parte de estas cámaras, que incluye a las equipadas con reconocimiento facial son operadas directamente por la entidad, mientras que las restantes, son tercerizadas, aunque como lo estipula el documento la información recolectada es propiedad única de Transmilenio.

Se conoce que 88 estaciones y portales de este medio de transporte cuentan con cámaras de seguridad, siendo 8 de estas estaciones con registro de SRF mencionadas previamente (Estación Ricaurte, Portal 80, Portal Américas, Estación Jiménez, Estación Héroes, Estación Calle 26, Estación Aguas y Estación Calle 22). No obstante, las autoridades aclaran que a pesar de contar con esta herramienta tecnológica la falta de infraestructura respecto al registro de bases de datos y la misma infraestructura de seguridad en la ciudadson un obstáculo para el funcionamiento del mismo. De modo que, en la actualidad funcionan, pero únicamente como cámaras de videovigilancia operadas por el C4.

Frente a este punto, Macías explica que “en (el periodo entre) 2021-2024 hubo trabas en la implementación debido a la infraestructura necesaria y la inversión. Se necesita una infraestructura tecnológica muy robusta y personal para el análisis de imágenes, ya que las cámaras por sí solas no son 100% confiables”. Asegura que en Bogotá ha habido la intención de interconectar todas las cámaras públicas y privadas, pero que el personal no da abasto y ha habido problemas para que esa interconectividad opere bien, lo cual dificultaría aún más el funcionamiento de cámaras de reconocimiento facial. Finalmente, visibiliza que se necesitaría de una infraestructura impresionante para registrar a toda la población de Bogotá en la base de datos necesaria para alimentar el sistema, una tarea que por el momento no se logrado por entes como la Registraduría Nacional”.

En medio de estas limitaciones técnicas y logísticas, surge una pregunta clave: ¿Quién está detrás del software que las autoridades han decidido implementar en la ciudad?

LOS ROSTROS DETRÁS DEL ALGORITMO:

¿Quiénes están detrás del software de Reconocimiento Facial en Bogotá?

Investigando sobre el origen del software utilizado por las autoridades, este arrojó un nombre: Corsight AI. Una compañía privada israelí fundada en el año 2019, que cuenta con su sede principal en Tel Aviv (Israel) y con una fortuna de 9.1 millones de dólares. Por lo que exhiben en su página web, la empresa hace parte de la industria de la seguridad e investigaciones.

Este software ha ganado la confianza de empresas privadas y gobiernos como Google, Oracle, aeropuertos del espacio Schengen y la Policía Nacional de Colombia. Fortify, desarrollado por una empresa israelí, identifica patrones, anomalías y activa alertas en tiempo real para mejorar la experiencia del cliente, el servicio y la seguridad, mediante inteligencia facial autónoma.

Sin embargo, mientras empresas y gobiernos celebran las capacidades de estos sistemas, organizaciones defensoras de derechos humanos advierten sobre los riesgos que su uso desregulado puede generar.

TECNOLOGÍA Y LEYES:

La Regulación del Reconocimiento Facial en el Mundo Moderno

El reconocimiento facial ha llegado a múltiples ámbitos, lo que ha motivado a organizaciones defensoras de derechos humanos como Amnistía Internacional, De Justicia, Fundación Karisma y AlSur a emitir alertas mediante informes e incluso acciones judiciales. Buscan que la sociedad comprenda los riesgos y que los gobiernos asuman la responsabilidad de usar esta tecnología, dadas sus implicaciones sobre derechos como la privacidad, la no discriminación, la libertad de expresión, reunión y debido proceso.

Ante la creciente preocupación por regular la inteligencia artificial, la Unión Europea ha liderado el debate global sobre sus usos, riesgos y alcances. En 2023, el Comité Europeo de Protección de Datos (CEPD) y el Supervisor Europeo de Protección de Datos (SEPD) publicaron las *"Directrices 5/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley" con recomendaciones para evitar abusos en territorio europeo.*

El reconocimiento facial se basa en datos biométricos, que según la Unión Europea pueden usarse para control individual o masivo. Aunque permite procesar datos a gran escala, también implica riesgos de discriminación y errores. Por ello, su uso debe ajustarse a la Directiva sobre protección de datos en el ámbito penal (DAP) y a la Carta de los Derechos Fundamentales de la UE, que exigen notificar al ciudadano cada vez que sus datos biométricos sean capturados y tratados.

Aclaran que publicar una fotografía en redes no implica autorizar la extracción de datos biométricos. Además, la UE prohíbe ciertas prácticas relacionadas con este tipo de extracción

Situaciones prohibidas por la UE para el tratamiento de datos biométricos.

Imagen: Autoría propia.

Finalmente, la UE sugiere unas recomendaciones que han contribuido como modelo de discusión en la formulación de leyes en otros países para SRF.

A diferencia de Europa, Colombia no cuenta con legislación específica sobre reconocimiento facial. Aunque existen casos de uso, la ausencia de lineamientos claros permite que los operadores actúen de forma autónoma, lo que puede afectar derechos fundamentales por falta de regulación.

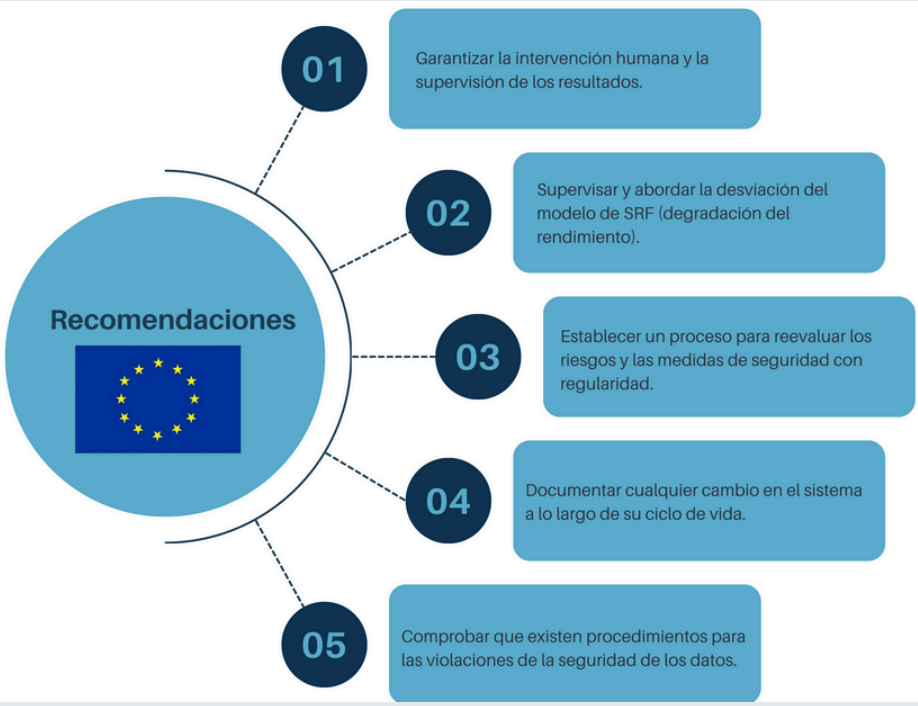


Imagen: Autoría propia.

La ley colombiana reconoce los datos biométricos como sensibles, según la Ley 1581 de 2012. Su tratamiento está prohibido, salvo excepciones como la autorización explícita del titular. La Superintendencia de Industria y Comercio, a través de la Delegatura para la Protección de Datos Personales, es responsable de garantizar el cumplimiento de esta normativa.

Un dato personal se entiende como “Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables”. Mientras que un dato considerado sensible para esta ley se compone de “datos relativos a la salud, a la vida sexual y los datos biométricos”. Para el tratamiento de un dato biométrico, la ley lo prohíbe exceptuando en cinco situaciones:

- El Titular debe dar su autorización explícita para el Tratamiento, excepto cuando la ley no lo requiera. Sin esta autorización, el Tratamiento no puede llevarse a cabo.

- El Tratamiento es necesario para proteger el interés vital del Titular cuando esté física o jurídicamente incapacitado. En estos casos, los representantes legales deben otorgar la autorización.

- El Tratamiento se realiza en actividades legítimas por parte de organizaciones sin ánimo de lucro con fines políticos, filosóficos, religiosos o sindicales. Los datos solo pueden referirse a sus miembros y no se pueden compartir con terceros sin autorización.

- El Tratamiento se refiere a datos necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial. Estos datos son esenciales para la correcta administración de justicia.

- El Tratamiento tiene fines históricos, estadísticos o científicos. En estos casos, se deben tomar medidas para suprimir la identidad de los Titulares.

Para que pueda llevarse a cabo el procesamiento de datos personales, incluidos los sensibles, se insiste en la existencia del consentimiento previo, expreso e informado al titular de los datos. Adicional a ese hecho, el manejo de los datos únicamente se hará por la parte autorizada por el titular y/o lo autorizado por la ley.

Otro aspecto del problema con los sistemas de reconocimiento facial es su vínculo con la Inteligencia Artificial, que en Colombia aún carece de una legislación específica. No obstante, ya se han iniciado debates en el Congreso, con dos proyectos de ley en curso, entre ellos el Proyecto de Ley 091 de 2023 “Mediante la cual se establece el deber de información para el uso responsable de la Inteligencia Artificial en Colombia” y Proyecto de Ley 130 de 2023, *“Por medio de la cual se crea la armonización de la Inteligencia Artificial con el derecho al trabajo de las personas”.*

El proyecto de interés para este reportaje fue aprobado en la Comisión Sexta del Senado y espera debate en plenaria. Su propósito es establecer principios éticos y legales para el uso responsable de la Inteligencia Artificial en Colombia.

Aunque esta regulación es solo un primer paso, se enfoca en la inteligencia artificial en general, dejando temas específicos como el reconocimiento facial pendientes de un análisis más profundo. En 2024, la Comisión Primera del Senado realizó una mesa técnica sobre la implementación y regulación de la IA, con participación de congresistas y expertos, quienes coincidieron en la necesidad de legislar y continuar el debate.

El reconocimiento facial ha avanzado rápidamente, integrándose en la sociedad y generando preocupaciones sobre la violación de derechos fundamentales. Aunque organizaciones de derechos humanos han trabajado para visibilizar sus riesgos, aún falta mayor compromiso de gobiernos, academia y medios para concientizar sobre su impacto en la democracia.

Ese reconocimiento facial pasó de ser una herramienta privada de seguridad a difundirse en redes sociales (un espacio público). Casos como los de Porcha y Guillermo alertan sobre los riesgos de usar esta tecnología sin considerar sus implicaciones éticas. También se señala la falta de transparencia por parte de las autoridades, lo que genera preocupación sobre sus motivaciones.

La Unión Europea busca regular el reconocimiento facial por sus riesgos de discriminación y la violación de derechos, sirviendo de ejemplo para otros países. En contraste, Colombia carece de legislación clara, lo que deja un vacío que puede afectar derechos fundamentales. Aunque hay avances desde el Congreso, se espera que no queden en el olvido. Las autoridades, principales responsables, suelen desconocer el alcance y desafíos de esta tecnología.

En síntesis, la Unión Europea ha establecido regulaciones claras sobre el reconocimiento facial, mientras que Colombia aún enfrenta retos por la falta de legislación específica. Esto evidencia la urgencia de normativas que protejan los derechos ciudadanos ante el uso creciente de esta tecnología por redes sociales, entidades públicas y privadas.

Vale aclarar que la existencia de otros factores como la falta de infraestructura tecnológica, el desconocimiento de las autoridades, el retraso en la digitalización de la información de la población, la falta de recursos (humanos, logísticos, entre otros) y la falta de transparencia en la entrega de resultados son obstáculos que impiden el normal funcionamiento de estas herramientas tecnológicas que terminan convirtiéndose en una inversión perdida.

Por otro lado, esta investigación evidenció la falta de cooperación, el desconocimiento y la incoherencia por parte de las entidades públicas al momento de realizar consultas puntuales sobre temas que supondrían estar dentro de su competencia. Después de diversos traslados de derechos de petición realizados entre las mismas entidades o respuestas incompletas e inconvincentes, solo deja un sinsabor al respecto de ellas mismas. Sin embargo, ello no logró ser un obstáculo para continuar con esta investigación y brindó más motivos para entender la razón de esa acción.

Vale aclarar que la existencia de otros factores como la falta de infraestructura tecnológica, el desconocimiento de las autoridades, el retraso en la digitalización de la información de la población, la falta de recursos (humanos, logísticos, entre otros) y la falta de transparencia en la entrega de resultados son obstáculos que impiden el normal funcionamiento de estas herramientas tecnológicas que terminan convirtiéndose en una inversión perdida.

Por otro lado, esta investigación evidenció la falta de cooperación, el desconocimiento y la incoherencia por parte de las entidades públicas al momento de realizar consultas puntuales sobre temas que supondrían estar dentro de su competencia. Después de diversos traslados de derechos de petición realizados entre las mismas entidades o respuestas incompletas e inconvincentes, solo deja un sinsabor al respecto de ellas mismas. Sin embargo, ello no logró ser un obstáculo para continuar con esta investigación y brindó más motivos para entender la razón de esa acción.

Aunque las autoridades han anunciado en repetidas ocasiones la instalación de cámaras con reconocimiento facial en Bogotá, hoy en día muchas de estas no están en funcionamiento. La razón oficial: nunca se concretó la compra de los equipos. Sin embargo, esta versión contrasta con múltiples reportajes de medios de comunicación que documentaron su instalación, uso y hasta resultados operativos en eventos públicos y espacios como Transmilenio (expuestos a lo largo de este trabajo periodístico). La contradicción entre lo que se afirma desde las instituciones y lo que se ha reportado públicamente deja más preguntas que respuestas.

Cuando se solicita una explicación clara a las autoridades sobre esta aparente incongruencia, la respuesta es evasiva o simplemente inexistente. No hay una narrativa coherente que justifique por qué se anunció una tecnología que, según ellos mismos, nunca se adquirió.

Esta falta de transparencia alimenta la desconfianza ciudadana y pone en entredicho la gestión de los recursos públicos destinados a la seguridad. Unos recursos destinados a un modelo que, sí cuenta con un informe de resultados, pareciera no estar disponible a la ciudadanía o incluso nunca se llevó a cabo.

El problema de fondo, sin embargo, va más allá de la tecnología: recae en la ausencia de control institucional. No hay claridad sobre qué ocurrió con el dinero invertido en estos proyectos, ni evidencia de auditorías que verifiquen su ejecución. En un contexto donde la vigilancia digital avanza sin regulación clara, la falta de rendición de cuentas sobre estos contratos no solo es preocupante, sino que también abre la puerta a posibles casos de negligencia o corrupción.

Por otro lado, las múltiples remisiones de derechos de petición entre instituciones y las respuestas incompletas o poco convincentes generaron un claro sin sabor respecto a su actuar. No obstante, estas dificultades no representaron un obstáculo para el desarrollo del trabajo. Por el contrario, reforzaron el propósito de la investigación periodística al brindar nuevas razones para profundizar en la comprensión de esta problemática.