

POSITION ARTICLE

Facial recognition and migration regularization in Ecuador: Legal feasibility from a human rights perspective***Reconocimiento facial y regularización migratoria en Ecuador: viabilidad jurídica desde un enfoque de derechos humanos***Cristina Madelaine Vera Mendoza¹  
Yina María Vélez Triviño¹  Gyomar Beatriz Pérez Cobo¹  
Camila Alcívar Trámpuz²  ¹ Universidad San Gregorio de Portoviejo, Ecuador² Abogada de los Juzgados y Tribunales de la República del Ecuador.

Citar como: Vera, C.M., Vélez, Y.M., Pérez, G.B., & Alcívar, C. (2026). Facial recognition and migration regularization in Ecuador: Legal feasibility from a human rights perspective. *Revista San Gregorio*, 1(Especial_3), 149-157. http://dx.doi.org/10.36097/rsan.v1iEspecial_3.4080

Received: 12-02-2026

Accepted: 27-07-2026

Published: 31-08-2026

ABSTRACT

This study analyzes the legal feasibility of using biometric data, particularly facial recognition, as a support tool in migration regularization processes in Ecuador. To this end, it adopts the form of a legal reflection and argument-based position paper, developed through a qualitative approach, a documentary research design, and an analytical and proposal-oriented scope. The research employs a critical integrative review, a method that brings together sources of different types in order to identify concepts, tensions, regulatory gaps, and divergent perspectives, while also enabling the formulation of an original theoretical or normative interpretation. The study argues that facial recognition and the processing of biometric data may pose significant risks to privacy, informational self-determination, equality, the presumption of innocence, and human dignity. Consequently, their use may lead to stigmatization, discrimination, and judgments based on an individual's identity or past rather than on their current conduct. At the same time, the study maintains that these technologies are not inherently harmful and that, under an appropriate regulatory framework, they could contribute to identity verification, reduce administrative processing times, and streamline migration regularization procedures. It concludes that Ecuador's traditional migration management mechanisms require review to strengthen regional cooperation and administrative efficiency. In this regard, the article proposes promoting a Latin American agreement that would enable states to exchange basic and verifiable information, with the aim of facilitating the identification and regularization of persons in situations of human mobility.

Keywords: Migration status; Biometric data; Human mobility; Human rights; Regularization.

RESUMEN

El presente estudio analiza la viabilidad jurídica del uso de datos biométricos, en particular del reconocimiento facial, como herramienta de apoyo en los procesos de regularización migratoria en Ecuador. Para ello se realizó un estudio de reflexión jurídica y posición argumentada, desarrollado mediante un enfoque cualitativo, un diseño documental y un alcance analítico-propositivo. La investigación adoptó una revisión integrativa de carácter crítico, modalidad que permite articular fuentes de distinta naturaleza con el propósito de identificar conceptos, tensiones, vacíos y perspectivas divergentes, así como formular una interpretación teórica o normativa propia. Se sostiene que el reconocimiento facial y el tratamiento de datos biométricos pueden generar riesgos relevantes para la privacidad, la autodeterminación informativa, la igualdad, la presunción de inocencia y la dignidad humana, por tanto, puede producir estigmatización, discriminación y juicios basados en la identidad o en el pasado de la persona, en lugar de atender a su conducta actual. Al mismo tiempo, el estudio plantea que estas tecnologías no son intrínsecamente perjudiciales y que, bajo una regulación adecuada, podrían contribuir a verificar identidades, reducir tiempos administrativos y agilizar los procesos de regularización migratoria. Se concluye que los mecanismos tradicionales de gestión migratoria en Ecuador requieren una revisión orientada a mejorar la cooperación regional y la eficacia administrativa. En este sentido, propone promover un convenio latinoamericano que permita intercambiar información básica y verificable entre los Estados, con el fin de facilitar la identificación y regularización de las personas en situación de movilidad humana.

Palabras clave: Estatus migratorio; Datos biométricos; Movilidad humana; Derechos humanos; Regularización.



INTRODUCCIÓN

En la actualidad, la tecnología desempeña un papel central en la configuración de la vida social, administrativa y jurídica, y se ha consolidado como un componente transversal de la gestión pública, la comunicación y el acceso a servicios esenciales. En el ámbito estatal, su incorporación ha sido justificada bajo criterios de eficiencia, modernización y celeridad administrativa. Sin embargo, tal como ha sido advertido desde una perspectiva crítica de derechos humanos, el desarrollo tecnológico no es axiológicamente neutro y puede convertirse en un instrumento de afectación a derechos fundamentales cuando carece de límites normativos claros y de controles democráticos efectivos (Pérez Cobo et al., 2024).

En este sentido, el acelerado avance de la inteligencia artificial (IA) y el tratamiento automatizado de datos han generado una creciente preocupación social en torno a derechos como la privacidad, la intimidad y la autonomía individual. Este fenómeno ha sido conceptualizado por la doctrina contemporánea como parte de un modelo de capitalismo de vigilancia, en el que el uso intensivo de tecnologías de identificación tiende a configurar escenarios de supervisión permanente y asimetrías de poder que colocan a las personas en situación de vulnerabilidad frente al Estado y a actores privados (Carbonell, 2009; Pérez Cobo et al., 2024).

No obstante, un enfoque constitucional y garantista desaconseja adoptar una postura tecnofóbica. Desde el pensamiento jurídico iberoamericano se ha sostenido que la tecnología no debe rechazarse en sí misma, sino someterse a una adecuada orientación normativa, de modo que su uso contribuya a la protección y efectividad de los derechos humanos, en lugar de propiciar su debilitamiento (Ferrajoli, 2006; De Sousa Santos, 2010). Las herramientas tecnológicas pueden convertirse en mecanismos legítimos de inclusión jurídica cuando se utilizan con una finalidad legítima, bajo criterios de proporcionalidad, legalidad y control institucional, especialmente en contextos donde existen barreras estructurales que impiden el ejercicio efectivo de derechos.

En esta lógica argumentativa es menester señalar que, Ecuador se ha consolidado en los últimos años como un país de destino para personas que migran en búsqueda de mejores condiciones de vida, seguridad y oportunidades de desarrollo (Banco Mundial, 2020). Sin embargo, una parte importante de esta población enfrenta serias dificultades para regularizar su situación migratoria, no necesariamente por la existencia de antecedentes penales, sino por la ausencia de coordinación efectiva entre las instituciones del Estado ecuatoriano y las de los países de origen (Bastidas, 2020).

Esta desarticulación institucional prolonga los trámites administrativos y sitúa a las personas en movilidad humana en una condición de vulnerabilidad jurídica que limita el acceso efectivo a derechos fundamentales como el trabajo, la salud, la educación y la seguridad social, en contravención de los estándares interamericanos de derechos humanos (Aguilar Cavallo, 2016).

En este contexto, el análisis del uso de datos biométricos se plantea como un mecanismo técnico-jurídico que, debidamente regulado, puede contribuir a la celeridad administrativa, a la cooperación regional y a la garantía efectiva de los derechos humanos de las personas en situación de movilidad humana. De este modo, el artículo se inserta en la línea crítica que reconoce los riesgos del uso tecnológico, pero que, al mismo tiempo, propone alternativas normativamente responsables para su utilización en beneficio de las personas.

Desde esta perspectiva, el presente artículo científico se centra en analizar la viabilidad jurídica del uso de datos biométricos, en particular del reconocimiento facial, como herramienta de apoyo en los procesos de regularización migratoria en Ecuador. A diferencia de los enfoques propios del capitalismo de vigilancia, la propuesta aquí desarrollada se inscribe en una lógica de garantía de derechos, orientada a reducir la dilación administrativa y a superar la fragmentación institucional que actualmente afecta los procesos de regularización migratoria.

METODOLOGÍA

El estudio se configuró como un artículo de reflexión jurídica y posición argumentada, desarrollado mediante un enfoque cualitativo, un diseño documental y un alcance analítico-propositivo. La investigación adoptó una revisión integrativa de carácter crítico, modalidad que permite articular fuentes de distinta naturaleza con el propósito de identificar conceptos, tensiones, vacíos y perspectivas divergentes, así como formular una interpretación teórica o normativa propia (Snyder, 2019; Torracó, 2005).

El corpus de análisis estuvo integrado por fuentes secundarias, donde se consideró la normativa constitucional y legal ecuatoriana, las disposiciones relacionadas con la movilidad humana, la protección de datos personales y la actuación administrativa, así como la jurisprudencia y los documentos oficiales pertinentes. También se analizaron artículos científicos y libros especializados, vinculados con la biometría, el reconocimiento facial, la IA, la protección de datos, la discriminación algorítmica y la regularización migratoria.

Los documentos seleccionados fueron examinados mediante análisis cualitativo de contenido. En la primera se efectuó una lectura exploratoria destinada a identificar los conceptos recurrentes y los principales problemas jurídicos asociados con el uso del reconocimiento facial. En la segunda se elaboró una matriz documental en la que se registraron la naturaleza de la fuente, el ámbito territorial, el problema analizado, la tesis principal, los derechos involucrados, los riesgos identificados y las salvaguardas propuestas. En la tercera etapa se realizó una codificación temática mediante categorías inicialmente deductivas, derivadas del marco constitucional

y de derechos humanos, que fueron posteriormente ajustadas a partir de los contenidos emergentes de las fuentes.

RESULTADOS Y DISCUSIÓN

Reconocimiento facial como tecnología emergente y límites desde los derechos humanos

A medida que avanza el tiempo, también avanza la tecnología, fenómeno que puede considerarse como “preocupante” debido a que, en repetidas ocasiones, se la ha dado un mal uso. No obstante, no es correcto catalogar a todo el avance tecnológico como dañino, ya que también ha logrado convertirse en una ayuda o facilidad para el ser humano.

Este planteamiento se encuentra alineado con la doctrina crítica contemporánea que advierte que la tecnología no es intrínsecamente perjudicial, sino que su impacto depende de los usos sociales, políticos y jurídicos que se le asignen. De Sousa Santos (2010) sostiene que los riesgos tecnológicos emergen cuando el desarrollo científico se desvincula de controles éticos y normativos, mientras que Carbonell (2019) subraya que el desafío del constitucionalismo contemporáneo consiste precisamente en reencauzar la innovación tecnológica dentro de un marco garantista, evitando respuestas de rechazo absoluto que impidan aprovechar sus beneficios sociales.

La doctrina especializada en protección de datos ha advertido que los riesgos asociados al uso indebido de tecnologías digitales no se limitan a escenarios hipotéticos, sino que se manifiestan de manera concreta en fenómenos como la apropiación indebida de información personal, la vigilancia excesiva y la pérdida de control de los individuos sobre sus propios datos. Murillo de la Cueva (2018) señala que la expansión de sistemas automatizados de tratamiento de datos exige una respuesta jurídica reforzada, particularmente cuando se trata de información sensible, ya que su uso inadecuado puede generar daños irreversibles a la privacidad, la identidad y la autonomía personal.

En consecuencia, la reflexión sobre los avances tecnológicos debe situarse en un punto de equilibrio que permita reconocer tanto sus beneficios como sus riesgos. Asumir una postura acrítica frente a la tecnología puede conducir a escenarios de abuso y vulneración de derechos. Uno de los avances tecnológicos más destacados es el desarrollo de softwares que permiten el reconocimiento facial, mediante el cual, incluso por una foto publicada en las redes sociales, se puede reconocer rápidamente a una persona para ser utilizado mayormente como un sistema de control de seguridad.

Es así como el reconocimiento facial constituye una de las aplicaciones más complejas y sensibles de la inteligencia artificial, en tanto se basa en el procesamiento automatizado de datos biométricos que permiten identificar de manera unívoca a una persona.

Desde el punto de vista jurídico, este tipo de tecnología plantea un desafío particular, debido a que involucra información que no solo identifica al individuo, sino que forma parte de su esfera más íntima e irrepetible. En consonancia con lo dispuesto, Rodríguez-Piñero Royo (2019) sostiene que los datos biométricos requieren una protección reforzada, precisamente porque su uso indebido puede generar afectaciones graves y difícilmente reversibles a los derechos fundamentales.

Desde una perspectiva constitucional, la utilización del reconocimiento facial por parte del Estado debe ser examinada bajo los principios de legalidad, necesidad y proporcionalidad. Carbonell (2019), explica que la mera invocación de fines de seguridad o eficiencia administrativa no resulta suficiente para legitimar el uso de tecnologías intrusivas, si estas no se encuentran claramente reguladas y sujetas a mecanismos efectivos de control. En ausencia de tales límites, el reconocimiento facial puede convertirse en una forma de vigilancia permanente incompatible con el derecho a la privacidad y con el principio de autodeterminación informativa.

En el ámbito latinoamericano, la doctrina ha señalado que el uso de tecnologías de identificación masiva corre el riesgo de reproducir prácticas de control selectivo y discriminación estructural. Particularmente, Aguilar Cavallo (2016) destaca que las medidas tecnológicas aplicadas sin un enfoque de derechos humanos suelen impactar de manera desproporcionada sobre grupos en situación de vulnerabilidad, como migrantes, personas empobrecidas o colectivos históricamente estigmatizados, es en estos casos donde la tecnología deja de operar como un instrumento neutral y pasa a reforzar desigualdades preexistentes.

En armonía con este planteamiento, Ferrajoli (2006) ha advertido que el incremento de las capacidades técnicas del poder estatal debe ir acompañado de un fortalecimiento correlativo de las garantías, ya que, de lo contrario, se produce una expansión ilegítima del control sobre las personas. Aplicado al reconocimiento facial, esta tesis implica que su utilización solo resulta compatible con un Estado constitucional de derechos cuando se encuentra estrictamente delimitada por la ley, responde a una finalidad legítima y se encuentra sujeta a supervisión judicial o administrativa independiente.

Una óptica crítica sobre la tecnología aparece en el artículo de Pérez Cobo et al. (2024), quienes exponen los peligros de los sistemas de reconocimiento facial ya que pueden integrarse fácilmente en lógicas de vigilancia digital si no se establecen salvaguardas claras en materia de protección de datos y transparencia. En particular,

advierten que la recolección y almacenamiento masivo de información biométrica sin consentimiento informado ni control ciudadano constituye una amenaza directa a la dignidad humana, al reducir a la persona a un objeto de identificación y monitoreo constante.

Reconocimiento facial, antecedentes penales y riesgo de discriminación

Entre los años 2019 y 2026, Ecuador consolidó una infraestructura migratoria y de identidad cada vez más biometrizada: procesos extraordinarios de regularización para población venezolana, registro de permanencia con captura presencial de fotografía y huellas, servicios de verificación “demográfico más biométrico” del Registro Civil, puertas biométricas en el aeropuerto de Quito y videovigilancia con analítica y reconocimiento facial en Rumichaca. En al menos un flujo oficial de visado de excepción, la documentación pública llegó a exigir expresamente “realizar el reconocimiento facial en el sistema”; en la documentación pública más reciente de e-VISAS, ese paso ya no aparece descrito con la misma claridad (Ministerio de Relaciones Exteriores y Movilidad Humana, 2023).

Es importante mencionar que el reconocimiento facial, como una de las principales ramas de la IA, presenta novedades como el reconocimiento de perfiles de personas que tengan antecedentes penales. Subrayamos que, en su mayoría, esta herramienta ha sido utilizada como un mecanismo de control dentro de los espacios públicos, donde las cámaras de seguridad tienen instalado un sistema de reconocimiento facial con el objetivo de poder detectar posibles amenazas dentro de dichos espacios. No obstante, su uso ha llegado a cuestionarse por considerarlo en algunos casos discriminatorio, lo que nos enfrenta con otra arista del problema, como lo es el Derecho Penal de Autor, que taxativamente está proscrito en el Código Orgánico Integral Penal de Ecuador (COIP, 2014).

En consideración a lo expresado por Zaffaroni (1999) que la “pretensión de aprehender normativamente, no ya conductas sino personalidades, sosteniendo que a cada tipo normativo corresponde un tipo de personalidad. No es la conducta la que el tipo encierra, sino que encierra la personalidad del autor de esa conducta” (p. 27). Este planteamiento resulta especialmente relevante en el contexto del uso de tecnologías de reconocimiento facial vinculadas a bases de datos de antecedentes penales, ya que pone de relieve el riesgo de transitar desde un derecho penal del acto hacia un derecho penal de autor, incompatible con los principios básicos del Estado de derecho. En efecto, cuando la tecnología permite identificar y clasificar personas en función de su historial penal previo, existe el peligro de que el control estatal se oriente no a conductas actuales, sino a la condición personal del individuo, erosionando el principio de culpabilidad y la presunción de inocencia.

Por su parte, Ferrajoli (2006) ha sostenido que toda forma de control que anticipe juicios de reproche sobre la persona, sin la existencia de una conducta concreta y actual, constituye una violación directa a las garantías penales y procesales. Aplicado al reconocimiento facial, este razonamiento permite advertir que la asociación automática entre identidad biométrica y antecedentes penales puede derivar en prácticas de vigilancia selectiva, donde ciertos sujetos son considerados permanentemente sospechosos, aun cuando se encuentren realizando actividades lícitas y cotidianas.

En el ámbito de los derechos humanos, esta problemática adquiere una dimensión aún más sensible cuando afecta a colectivos históricamente vulnerables. Aguilar Cavallo (2016) señala que las tecnologías de control aplicadas sin salvaguardas suficientes tienden a producir discriminaciones indirectas, en tanto su impacto no se distribuye de manera equitativa, sino que recae con mayor intensidad sobre personas migrantes, empobrecidas o estigmatizadas socialmente. En estos casos, el uso del reconocimiento facial asociado a antecedentes penales puede reforzar prejuicios estructurales y prácticas de exclusión incompatibles con el principio de igualdad y no discriminación.

Asimismo, Pérez Cobo et al. (2024) advierten que los sistemas automatizados de identificación pueden generar una forma de “etiquetamiento digital” que reduce a la persona a un conjunto de datos, invisibilizando su condición de sujeto de derechos. Esta lógica resulta particularmente peligrosa cuando se integra en espacios públicos, donde el individuo se encuentra expuesto a mecanismos de control que operan sin su conocimiento ni consentimiento, y donde la posibilidad de cuestionar o impugnar las decisiones tecnológicas resulta limitada.

Respecto a lo señalado, el uso del reconocimiento facial con fines de identificación penal debe ser analizado con especial cautela, pues, si bien puede responder a objetivos legítimos de seguridad, también puede derivar en prácticas de control preventivo basadas en la identidad y no en la conducta. Es en este contexto donde Carbonell (2019) enfatiza que el constitucionalismo contemporáneo exige que toda medida restrictiva de derechos supere una prueba estricta de proporcionalidad, evitando que la eficiencia tecnológica se imponga sobre la dignidad humana y las garantías fundamentales.

Así, el reconocimiento facial aplicado a la identificación de personas con antecedentes penales plantea un dilema jurídico central, mientras su uso indiscriminado puede reproducir esquemas propios del derecho penal de autor y generar discriminación, su implementación limitada, regulada y orientada a fines administrativos legítimos podría evitar tales riesgos. De allí la necesidad de distinguir claramente entre un uso con fines de seguridad y estigmatizante de esta tecnología y su posible utilización garantista, orientada a facilitar procedimientos administrativos sin prejuzgar a la persona por su pasado.

Reconocimiento facial y juicios arbitrarios sobre la persona en Ecuador

El reconocimiento facial puede propiciar juicios arbitrarios y prácticas discriminatorias cuando la persona es valorada por su identidad o por sus antecedentes, en lugar de por la conducta concreta que realiza. Así, una persona con antecedentes penales que desarrolla una actividad cotidiana y legítima en un espacio público podría ser sometida a sospecha, vigilancia o intervención injustificada si el sistema vincula automáticamente su identificación biométrica con registros penales previos.

Es particularmente este planteamiento el que evidencia uno de los principales riesgos asociados al uso de tecnologías de identificación biométrica en espacios públicos, es decir, la sustitución del juicio por una presunción tecnológica basada en datos previos. Ferrajoli (2006) advierte que cualquier forma de imputación que no se funde en una conducta concreta y actual vulnera el principio de presunción de inocencia, el cual constituye una garantía estructural del Estado constitucional de derechos. Cuando el reconocimiento facial se utiliza para identificar a una persona por su pasado penal, se corre el riesgo de transformar dicha garantía en una ficción, desplazando el análisis del hecho hacia la identidad del sujeto.

Desde la teoría constitucional, Carbonell (2019) sostiene que los sistemas tecnológicos aplicados por el Estado no pueden operar como mecanismos automáticos de sospecha, ya que ello implica una inversión inadmisible de la carga de la prueba. En efecto, someter a una persona a un escrutinio reforzado por el solo hecho de poseer antecedentes penales supone tratarla como permanentemente peligrosa, desconociendo que la responsabilidad penal se agota con el cumplimiento de la sanción y que el individuo conserva íntegramente su condición de sujeto de derechos.

En el ámbito de los derechos humanos, esta problemática se agrava cuando se considera el impacto que tales prácticas pueden tener sobre la dignidad humana. Ávila Santamaría (2012) afirma que la dignidad implica el derecho de toda persona a no ser reducida a una categoría, etiqueta o condición previa, especialmente cuando dicha categorización genera exclusión o trato desigual. En este sentido, el uso del reconocimiento facial para identificar antecedentes penales en espacios públicos puede producir una forma de estigmatización tecnológica, donde la persona es juzgada no por lo que hace, sino por lo que fue.

Asimismo, Aguilar Cavallo (2016) señala que las tecnologías de control aplicadas sin salvaguardas suficientes suelen generar discriminaciones indirectas, ya que, aunque se presenten como neutrales, producen efectos diferenciados sobre determinados grupos sociales. En el caso de las personas migrantes o en situación de movilidad humana, este riesgo es aún mayor, pues la combinación de condición migratoria, antecedentes penales y tecnologías de identificación puede derivar en prácticas de control selectivo incompatibles con el principio de igualdad y no discriminación.

En cualquier caso, es clave comprender lo señalado por Pérez Cobo et al. (2024) sobre los sistemas de vigilancia basados en datos biométricos ya que estos tienden a normalizar la supervisión constante, erosionando progresivamente la libertad individual. Cuando estas tecnologías se utilizan para anticipar juicios o decisiones sobre las personas, se configura un escenario en el que el individuo pierde control de su propia imagen y sobre la información que define su interacción con el espacio público.

De allí que, el reconocimiento facial, cuando se vincula de manera directa a la identificación de antecedentes penales, debe ser objeto de una regulación particularmente estricta, ya que su uso indiscriminado puede dar lugar a juicios arbitrarios que lesionan derechos fundamentales como la presunción de inocencia, la igualdad y la dignidad humana, en tal circunstancia, resulta imprescindible distinguir entre un uso legítimo, limitado y garantista de esta tecnología, y aquellas prácticas que, bajo el pretexto de la seguridad, reproducen lógicas de exclusión y control incompatibles con un Estado constitucional de derechos.

Datos biométricos: definición, alcance y tipologías

El sistema analizado en esta investigación emplea datos biométricos, entendidos como datos personales obtenidos mediante un tratamiento técnico específico de características físicas, fisiológicas o conductuales que permiten identificar o verificar de manera unívoca a una persona. Entre los identificadores biométricos de carácter físico o fisiológico se encuentran las huellas dactilares, los rasgos faciales, el iris y determinados patrones de la voz; mientras que los biométricos conductuales comprenden, entre otros, la dinámica de la escritura, la firma manuscrita, la forma de caminar o ciertos patrones de interacción. Debido a su capacidad identificadora y a la dificultad de sustituirlos en caso de uso indebido, estos datos requieren un nivel reforzado de protección jurídica y técnica (Rodríguez-Piñero Royo, 2019).

La definición expuesta coincide con la doctrina especializada que distingue los datos biométricos por su capacidad identificadora reforzada, en tanto se encuentran intrínsecamente vinculados a la identidad física o comportamental de la persona. Rodríguez-Piñero Royo (2019) señala que este tipo de datos no solo permiten identificar a un individuo, sino que lo hacen de manera prácticamente irreversible, lo que justifica que reciban un nivel de protección jurídica superior al de otros datos personales. Esta característica convierte a la biometría en una herramienta altamente eficaz, pero también en una fuente potencial de riesgos para los derechos fundamentales.

No en vano Murillo de la Cueva (2018) advierte que el tratamiento de datos biométricos implica una afectación directa al derecho a la privacidad y a la autodeterminación informativa, razón por la cual su utilización debe encontrarse sujeta a principios estrictos de legalidad, finalidad específica y minimización de datos. En este sentido, no basta con que el Estado alegue una finalidad legítima para justificar su uso, sino que resulta indispensable demostrar que no existen medios menos invasivos para alcanzar el mismo objetivo.

En correspondencia, Ávila Santamaría (2012) ha sostenido que la protección de los datos personales forma parte del contenido esencial del derecho a la dignidad humana, en tanto garantiza a la persona el control sobre la información que la identifica y la define frente a terceros. Aplicado a los datos biométricos, este planteamiento implica reconocer que su uso indebido puede generar formas de dominación o control incompatibles con un Estado constitucional de derechos, especialmente cuando se trata de poblaciones en situación de vulnerabilidad.

Asimismo, Ferrajoli (2006) enfatiza que todo incremento en las capacidades técnicas del poder estatal debe ir acompañado de un fortalecimiento correlativo de las garantías jurídicas. En el caso de los datos biométricos, ello supone establecer límites claros respecto a su recolección, almacenamiento, acceso y uso, así como mecanismos efectivos de supervisión y responsabilidad. De lo contrario, la biometría puede convertirse en un instrumento de control masivo que exceda los fines para los cuales fue originalmente concebida.

Reconocimiento facial y eficiencia administrativa

Ahora bien, no todo es negativo, ya que el reconocimiento facial ha permitido lograr la identificación de las personas de una manera mucho más rápida incluso por medio de la comparación de imágenes de una persona determinada. Esto representa un beneficio para la administración pública de un país ya que va a permitir la celeridad de los procesos aumentando la efectividad de dicha administración.

El planteamiento anterior pone de relieve una de las principales ventajas del reconocimiento facial desde la óptica de la gestión pública relacionada con su capacidad para optimizar los procedimientos administrativos, reduciendo tiempos, costos y márgenes de error asociados a la verificación manual de la identidad.

Desde el derecho administrativo contemporáneo, Esteve Pardo (2015) sostiene que la incorporación de tecnologías digitales puede contribuir significativamente a la eficacia y eficiencia de la administración pública, siempre que su uso se encuentre orientado a mejorar la prestación de los servicios y no a sustituir indebidamente el juicio humano.

En el mismo sentido, la doctrina ha destacado que la celeridad constituye un principio esencial del procedimiento administrativo moderno. García de Enterría & Fernández (2017) señalan que la administración está obligada a adoptar los medios técnicos disponibles para garantizar respuestas oportunas y efectivas a los ciudadanos, evitando dilaciones indebidas que afecten el ejercicio de derechos. En este contexto, el reconocimiento facial puede configurarse como una herramienta legítima para agilizar trámites que, por su naturaleza masiva, suelen verse afectados por retrasos estructurales.

Carbonell (2019) advierte que la eficiencia administrativa no puede concebirse como un valor absoluto, sino que debe armonizarse con la protección de los derechos fundamentales. No obstante, ello no implica rechazar el uso de tecnologías avanzadas, sino someterlas a un marco regulatorio que asegure su compatibilidad con los principios de legalidad, proporcionalidad y debido proceso. Bajo esta lógica, la eficiencia tecnológica resulta constitucionalmente admisible cuando se orienta a facilitar el acceso a derechos y no a restringirlos.

Asimismo, Ávila Santamaría (2012) sostiene que el principio de eficiencia estatal debe interpretarse a la luz del principio de dignidad humana, lo que implica que toda innovación tecnológica debe evaluarse en función de su impacto real sobre las personas. En este sentido, el reconocimiento facial, cuando se emplea para simplificar trámites y reducir cargas burocráticas, puede constituir un mecanismo que fortalezca la relación entre el Estado y los administrados, siempre que se garantice la protección de los datos personales y el respeto a la privacidad.

En estos términos, el reconocimiento facial puede ser concebido como una herramienta idónea para mejorar la eficiencia administrativa y la celeridad de los procesos, particularmente en ámbitos donde la verificación de identidad resulta un requisito indispensable. No obstante, su legitimidad depende de que su implementación se encuentre claramente regulada, limitada a fines administrativos específicos y acompañada de garantías efectivas que eviten su utilización como un mecanismo de vigilancia o control incompatible con los derechos humanos.

Reconocimiento facial y regularización de personas en situación de movilidad humana en Ecuador

La posibilidad de emplear tecnologías biométricas para agilizar procesos de regularización migratoria se inscribe en una concepción de administración pública orientada a la garantía de derechos, particularmente relevante en contextos de alta demanda y limitaciones institucionales. Ecuador ha sido utilizado como país de tránsito por las migrantes décadas atrás, no obstante, en estos últimos años, el mismo se convirtió en un

país de destino para las personas que buscan mejorar sus condiciones de vida, especialmente, las personas de nacionalidad venezolana. La gran mayoría de personas migrantes se encuentran en una condición de “irregulares”, es decir, que su estatus migratorio no se encuentra regularizado en el país por lo que se encuentran un poco limitados en el Ecuador con lo que respecta a poder desenvolverse en la sociedad (Banco Mundial, 2020).

En el caso ecuatoriano, la llegada sostenida de población migrante, particularmente de origen venezolano, ha evidenciado las limitaciones estructurales de los procedimientos de regularización y de los mecanismos de identificación exigidos por el Estado. Aguilar Cavallo (2016) advierte que la irregularidad migratoria coloca a las personas en una situación de vulnerabilidad jurídica que restringe el ejercicio efectivo de derechos, aun cuando estos se encuentren formalmente reconocidos en la Constitución. Esta contradicción entre reconocimiento normativo y goce efectivo constituye uno de los principales problemas del enfoque tradicional de la gestión migratoria.

Ahora bien, la falta de regularización prolongada puede derivar en procesos de estigmatización social, donde la persona migrante es percibida como una carga o una amenaza, en lugar de ser reconocida como un sujeto de derechos. De Sousa Santos (2010) precisa que estas narrativas de exclusión suelen intensificarse en contextos de crisis económica o institucional, reforzando prácticas discriminatorias que se traducen en políticas restrictivas o en omisiones estatales.

Queda claro que, el reconocimiento del Ecuador como país de destino migratorio exige un replanteamiento de las estrategias de gestión migratoria, orientándolas hacia un enfoque de derechos humanos y de inclusión social. La incorporación de tecnologías como el reconocimiento facial, analizada en este estudio, debe entenderse como parte de una respuesta estructural destinada a facilitar la regularización, reducir la vulnerabilidad jurídica y garantizar el ejercicio efectivo de los derechos de las personas en situación de movilidad humana.

La pregunta relevante no es si Ecuador “usa” o “no usa” reconocimiento facial en movilidad humana. La evidencia muestra que el país ya opera dentro de un entorno biométrico migratorio. La cuestión jurídica y política es si ese entorno cumple con el estándar de un Estado constitucional de derechos. A la luz de las fuentes revisadas, la respuesta hoy es parcial e insuficiente. Hay base constitucional y ley general; hay avances regulatorios desde la Superintendencia de Protección de Datos Personales (SPDP); pero persisten opacidad técnica, ausencia de auditorías públicas locales, vacíos de control judicial y riesgo serio de interoperabilidad expansiva.

No obstante, aunque Ecuador tiene base constitucional y una ley general robusta de protección de datos, el principio interamericano exige una regulación suficientemente precisa sobre fines, facultades, autoridades competentes y salvaguardas. En las fuentes públicas revisadas, la regularización migratoria sí está creada por decretos y acuerdos, pero la utilización concreta de reconocimiento facial en ese proceso no aparece desarrollada con el mismo nivel de detalle normativo. Eso deja una zona gris entre “foto obligatoria”, “captura biométrica”, “reconocimiento facial” y “validación biométrica”, con efectos jurídicos distintos.

Desde una perspectiva de derechos humanos, el problema no es solo la existencia de biometría, sino su inserción en trámites de alta dependencia material: para una persona migrante o refugiada, “consentir” el tratamiento de datos sensibles no ocurre en condiciones equivalentes a un servicio opcional, porque la regularización determina acceso a trabajo, salud, educación, movilidad y protección frente a sanciones migratorias.

La Constitución de la República del Ecuador (2008) protege el derecho a migrar, prohíbe la discriminación por condición migratoria y reconoce la protección de datos personales y la intimidad, La Ley Orgánica de Protección de Datos Personales (2021) considera sensibles tanto los datos biométricos como la condición migratoria, exige bases de legitimación, seguridad, análisis de riesgos, protección desde el diseño y evaluaciones de impacto, y reconoce garantías frente a decisiones automatizadas. Sin embargo, no existe una normativa sectorial públicamente visible que regule con precisión y proporcionalidad el uso de reconocimiento facial en regularización migratorio.

La prioridad de corto plazo debería ser reducir dependencia estructural de la biometría facial en decisiones que condicionan estatus jurídico y acceso a derechos. Ecuador puede avanzar hacia un modelo de identidad digital y regularización menos invasivo mediante autenticación multifactor, validación documental reforzada, verificación presencial humana cuando exista falla algorítmica y reglas de exclusión probatoria para coincidencias faciales no auditadas. En paralelo, la Corte Constitucional y la jurisdicción contencioso-administrativa deberían desarrollar jurisprudencia específica sobre biometría estatal, movilidad humana y reparación frente a errores algorítmicos.

CONCLUSIONES

Se evidencia la necesidad de replantear los mecanismos tradicionales de gestión migratoria en el Ecuador y en la región latinoamericana, particularmente en lo que respecta a los procesos de regularización de personas en situación de movilidad humana. En este contexto, resulta pertinente destacar la importancia de impulsar un convenio de cooperación regional, orientado al intercambio de información básica y verificable a través de bases de datos compartidas, que permita mejorar la celeridad y eficacia de los procedimientos administrativos, sin sacrificar las garantías propias de un Estado constitucional de derechos.

Los resultados de investigación evidenciaron que uno de los principales obstáculos para la regularización migratoria no radica exclusivamente en las exigencias del país de destino, sino en la falta de coordinación y comunicación efectiva entre los Estados de origen y de acogida. En numerosos casos, las personas migrantes no logran completar su proceso de regularización debido a la imposibilidad de obtener oportunamente documentos esenciales situación de irregularidad y profundiza su condición de vulnerabilidad jurídica. Esta realidad pone de manifiesto la necesidad de adoptar soluciones estructurales que trasciendan el ámbito nacional y promuevan respuestas regionales articuladas.

En este escenario, el uso de tecnologías como el reconocimiento facial y los datos biométricos, debidamente regulados, se presenta como una alternativa técnica y jurídicamente viable para superar las deficiencias actuales del sistema. Estas herramientas no deben concebirse como mecanismos de control o vigilancia, sino como instrumentos orientados a facilitar los procesos de regulación. La incorporación del reconocimiento facial solo resultará legítima cuando se acompañe de una regulación estricta, y de mecanismos de supervisión que eviten prácticas discriminatorias o estigmatizantes.

REFERENCIAS

- Aguilar Cavallo, G. (2016). *Derechos humanos y migraciones internacionales*. Tirant lo Blanch. <https://dialnet.unirioja.es/servlet/autor?codigo=4109550>
- Ávila Santamaría, R. (2012). Los derechos y sus garantías: Ensayos críticos. Corte Constitucional del Ecuador. <https://repositorio.uasb.edu.ec/bitstream/10644/6114/1/Avila,%20R-CON-012-Los%20derechos.PDF>
- Banco Mundial. (2020). *Retos y oportunidades de la migración venezolana en Ecuador*. <https://documents1.worldbank.org/curated/en/453941593004490155/pdf/Retos-y-Oportunidades-de-la-Migracion-Venezolana-en-Ecuador.pdf>
- Bastidas, C. (2020). *Sistematización de estudios sobre la caracterización de la migración venezolana en Ecuador (Quito y Guayaquil)*. Organización Internacional del Trabajo. <http://ecuador.un.org/sites/default/files/remote-resources/5f5ccc4e646c891984d0e560ec63b4cb.pdf>
- Carbonell, M. (2009). ¿Qué es el garantismo? Una nota muy breve. Editorial UNAM. https://gc.scalahed.com/recursos/files/r161r/w23990w/Que_garantismo_S3.pdf
- Carbonell, M. (2019). *Derechos fundamentales y nuevas tecnologías*. Instituto de Investigaciones Jurídicas, UNAM.
- Código Orgánico Integral Penal de Ecuador. [COIP]. (2014, 10 de febrero). Registro Oficial Suplemento 180. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf
- Constitución de la República del Ecuador. (2008, 20 de octubre). Registro Oficial N.º 449. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf
- De Sousa Santos, B. (2010). *Para una revolución democrática de la justicia*. Consejo Latinoamericano de Ciencias Sociales (CLACSO). https://biblioteca.clacso.edu.ar/clacso/se/20181203040213/Antologia_Boaventura_Vol1.pdf
- Esteve Pardo, J. (2015). *La nueva relación entre Estado y sociedad: Aproximación al trasfondo de la crisis*. Marcial Pons. <https://www.marcialpons.es/media/pdf/9788415664505.pdf>
- Ferrajoli, L. (2006). *Sobre los derechos fundamentales*. Trotta. <https://www.riaj.com/sites/default/files/2022-06/Derechos%20Fundamentales.pdf>
- García de Enterría, E., & Fernández, T. R. (2017). *Curso de derecho administrativo* (Vol. I). Civitas. https://www.cortesaragon.es/fileadmin/_DMZMedia/biblioteca/boletinNovedades/201402/04.pdf
- Ley Orgánica de Protección de Datos Personales. (2021, 26 de mayo). Registro Oficial Suplemento 459. http://finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf
- Ministerio de Relaciones Exteriores y Movilidad Humana. (2023). *Emisión de visa de residencia temporal de excepción (virte) para ciudadanos venezolanos*. <http://www.gob.ec/sites/default/files/sign/procedure-14343-2024030306066-16808455-signed.pdf>
- Murillo de la Cueva, P. (2018). *La protección de los datos personales y el derecho a la autodeterminación informativa*. Tecnos. <https://acortar.link/kmPQp7>

- Pérez Cobo, G. B., Vera Mendoza, C., & Valverde Jalca, Y. I. (2024). El capitalismo de vigilancia frente a la protección de los derechos humanos en la era tecnológica. *Revista Científica Panorámica de los DDHH y DIH*, 2(2), 55-69. <https://egradh.edu.do/revista-cientifica-panoramica-ddhh/>
- Rodríguez-Piñero Royo, M. (2019). Las facultades de control de datos biométricos del trabajador. *Temas Laborales: Revista Andaluza de Trabajo y Bienestar Social*, (150), 91-109. <https://idus.us.es/items/2b9a7172-552d-4550-afb4-f3910ce7d815>
- Romero, J. G., Menéndez, F. M., & Chica, T. M. (2019). Migración como fenómeno social y vulnerable y salvaguarda de los derechos humanos. *Revista de Ciencias Sociales*, 281-294. <https://www.redalyc.org/journal/280/28065583018/28065583018.pdf>
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333-339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review*, 4(3), 356-367. <https://doi.org/10.1177/1534484305278283>
- Uprimny, R. (2014). *Migración, derechos humanos y políticas públicas en América Latina*. DeJusticia.
- Zaffaroni, E. R. (1999). *Tratado de derecho penal: Parte general* (Tomo III). Ediar. https://www.salapenaltribunalmedellin.com/images/doctrina/libros01/Tratado_De_Derecho_Penal_-_Parte_General-III.pdf

Conflicts of Interest:

The authors declare no conflicts of interest.

Author Contributions:

The authors were responsible for all aspects of the study, including conceptualization, methodology, analysis, and writing.

Disclaimer/Publisher's Note:

The statements, opinions, and data contained in all publications are solely those of the authors and individual contributors and not of Revista San Gregorio or the editors. Revista San Gregorio and/or the editors disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.