Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), Noviembre-Diciembre 2025,
Volumen 9, Número 6.

https://doi.org/10.37811/cl_rcm.v9i6

IDENTIDADES DISPUTADAS Y EXTRACTIVISMO DE DATOS: LOS LÍMITES CONSTITUCIONALES DE LA TECNOLOGÍA BIOMÉTRICA EN EL INM

CONTESTED IDENTITIES AND DATA EXTRACTIVISM: THE CONSTITUTIONAL LIMITS OF BIOMETRIC TECHNOLOGY AT THE INM

Jesús Antonio Ramos Ferrer
Universidad Juárez Autónoma de Tabasco, México

Arturo Enrique Jasso Rodríguez
Universidad Juárez Autónoma de Tabasco, México

DOI: https://doi.org/10.37811/cl_rcm.v9i6.22082

Identidades Disputadas y Extractivismo de Datos: Los Límites Constitucionales de la Tecnología Biométrica en el INM

Jesús Antonio Ramos Ferrer[1]
jesus.ramos@ujat.mx
https://orcid.org/0000-0003-3893-9083
División Académica Multidisciplinaria de los Ríos
Universidad Juárez Autónoma de Tabasco.
Tenosique, Tabasco
México

Arturo Enrique Jasso Rodríguez
arturo.jasso@ujat.mx
https://orcid.org/0000-0002-9643-7826
División Académica Multidisciplinaria de los Ríos de la
Universidad Juárez Autónoma de Tabasco
Tenosique, Tabasco - México
México

RESUMEN

El presente artículo tiene como objetivo analizar los retos jurídicos y de seguridad técnica que subyacen a la implementación de sistemas biométricos por parte del Instituto Nacional de Migración (INM), identificando las brechas estructurales que comprometen la protección de datos personales de la población migrante en México. La investigación se inscribe en un enfoque cualitativo de carácter descriptivo y analítico, empleando el método dogmático-jurídico y la técnica de análisis documental para evaluar la coherencia de la normativa vigente frente a los estándares internacionales de derechos humanos. Los principales hallazgos revelan que, si bien la biometría es una herramienta idónea para la identificación migratoria, su aplicación en el contexto mexicano carece de salvaguardas legales suficientes para superar un examen de proporcionalidad integral. Se evidencia una insuficiencia normativa en el artículo 20 de la Ley de Migración y una vulnerabilidad sistémica frente al extractivismo de datos y la suplantación de identidad. Se concluye que es imperativo transitar hacia una gobernanza migratoria ética que garantice la soberanía de los datos y el derecho a la autodeterminación informativa, evitando que la digitalización de la frontera se traduzca en mecanismos de exclusión o deshumanización del sujeto en movilidad.

***Palabras clave*:** datos biométricos, INM, proporcionalidad, seguridad digital, extractivismo de datos

[1] Autor principal
Correspondencia: jesus.ramos@ujat.mx

Contested Identities and Data Extractivism: The Constitutional Limits of Biometric Technology at the INM

ABSTRACT

This article aims to analyze the legal and technical security challenges underlying the implementation of biometric systems by the National Institute of Migration (INM), identifying structural gaps that compromise the protection of personal data of the migrant population in Mexico. The research follows a qualitative approach of a descriptive and analytical nature, using the dogmatic-legal method and documentary analysis techniques to assess the consistency of current regulations with international human rights standards. The main findings reveal that, although biometrics is an adequate tool for migration identification, its application in the Mexican context lacks sufficient legal safeguards to pass a comprehensive proportionality test. There is evidence of regulatory insufficiency in Article 20 of the Migration Law and of systemic vulnerability to data extractivism and identity theft. It is concluded that it is essential to move towards ethical migration governance that guarantees data sovereignty and the right to informational self-determination, preventing the digitization of the border from translating into mechanisms of exclusion or dehumanization of individuals in mobility.

***Keywords*:** biometric data, INM, proportionality, digital security, data extraction

Artículo recibido 10 diciembre 2025
Aceptado para publicación: 10 enero 2026

INTRODUCCIÓN

La conceptualización de los datos biométricos ha evolucionado de una descripción técnica a una categoría jurídica fundamental. Según el Diccionario Panhispánico del Español Jurídico (2025), estos se definen como la información física, fisiológica o conductual que permite la identificación única de un individuo. Más allá de su definición, su operatividad reside en ser un sistema de reconocimiento de patrones que contrasta datos adquiridos con plantillas almacenadas en bases de datos (Ruíz et al., 2022). Esta arquitectura técnica ha permitido que los Estados adopten la biometría como un pilar fundamental de la seguridad nacional; sin embargo, como señalan Simón Castellano y Dorado Ferrer (2022), la implementación de estos sistemas no es neutra, sino que requiere un tratamiento técnico y jurídico específico para que la identificación sea inequívoca y no vulnere las garantías constitucionales. En este sentido, la eficacia de la tecnología biométrica en el control fronterizo debe estar supeditada a un marco de protección de datos que mitigue los riesgos intrínsecos de la vigilancia digital y asegure el respeto a la identidad de las personas migrantes.

En México, esta implementación se operativiza a través de los Lineamientos para trámites y procedimientos migratorios (2019), los cuales facultan al Instituto Nacional de Migración (en adelante INM) para la recolección de estos datos. No obstante, el despliegue de dichos sistemas se enfrenta a una paradoja estructural: mientras se exige una mayor captura de información sensible, la infraestructura digital del Estado ha demostrado vulnerabilidades críticas. Un antecedente ineludible es la vulneración masiva a los servidores de la Secretaría de la Defensa Nacional en 2022, conocida como 'Guacamaya Leaks', la cual expuso la fragilidad de los protocolos de ciberseguridad en instituciones de alto nivel (Red en Defensa de los Derechos Digitales [R3D], 2022). Lo anterior conlleva a cuestionar si el INM cuenta con los protocolos de seguridad técnica y la robustez de software necesarios para garantizar que la información sensible de las personas en movilidad no sea vulnerada, tal como ocurrió con las instituciones castrenses.

La relevancia de esta investigación radica en la naturaleza excepcional de los datos biométricos. A diferencia de los sistemas de autenticación tradicionales basados en conocimientos (contraseñas) o posesiones (tarjetas), la biometría se vincula a rasgos biológicos permanentes.

Como señala la Agencia Española de Protección de Datos (AEPD, 2023), la pérdida o filtración de estos datos conlleva un riesgo de 'suplantación de identidad de carácter irreversible', puesto que el titular no puede modificar sus rasgos físicos tras una vulneración técnica. En el contexto de la migración en México, este riesgo se potencia debido a la condición de vulnerabilidad de los sujetos, quienes, al encontrarse en tránsito, carecen de mecanismos de defensa jurídica efectivos ante un posible uso indebido de su información por parte de grupos delictivos o autoridades transfronterizas. Por tanto, analizar la capacidad de resguardo del INM no es solo un ejercicio técnico, sino un imperativo de protección a los derechos humanos.

En este entorno de vulnerabilidad digital que se ha descrito, el presente trabajo tiene como propósito analizar los retos jurídicos y de seguridad técnica que subyacen a la implementación de sistemas biométricos por parte del Instituto Nacional de Migración (INM), con el fin de identificar las brechas estructurales que comprometen la protección de datos personales de la población migrante en México.

Para alcanzar esta meta, la investigación se articula a través de tres ejes fundamentales u objetivos específicos. En primer lugar, se busca identificar el marco legal y los protocolos vigentes que regulan la recolección de estos datos en las estaciones migratorias, evaluando su alineación con los estándares internacionales de privacidad. En segundo lugar, se pretende examinar los riesgos de seguridad digital derivados de la centralización de información sensible, tomando como punto de contraste las recientes vulneraciones a instituciones de seguridad nacional en el país. Finalmente, se aspira a evaluar las implicaciones éticas y de derechos humanos respecto a la posible suplantación de identidad y el uso indebido de perfiles biométricos, considerando la condición especial de vulnerabilidad de las personas en situación de movilidad.

METODOLOGÍA

La presente investigación se inscribe en un enfoque cualitativo de carácter descriptivo y analítico, el cual, según Bernal (2023), es pertinente cuando el investigador busca comprender fenómenos complejos a través de la interpretación de textos y contextos específicos (p. 210). En concordancia con este enfoque, se aplica el método dogmático-jurídico que, en palabras de Ponce de León Armenta (2023), permite el estudio sistemático de las estructuras normativas para determinar su coherencia y suficiencia ante problemas sociales emergentes, como lo es la seguridad digital (p. 112). Bajo esta premisa

epistemológica, la investigación jurídica trasciende el análisis exegético para adoptar, como sugiere Cáceres Nieto (2020), un modelo que interprete la norma en relación con su eficacia técnica y su impacto en los derechos fundamentales (p. 45).

Para la ejecución del estudio se empleó la técnica de análisis documental, definida por Salinas Ramos (2021) como el procedimiento sistemático para organizar y evaluar evidencia científica, garantizando que los hallazgos sean verificables y objetivos. El proceso se desarrolló inicialmente mediante una fase normativa en la que se realizó una revisión exhaustiva de la Ley de Migración y los Lineamientos para trámites migratorios (2019), contrastando estas facultades con las obligaciones de resguardo técnico establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Posteriormente, se integró una fase de análisis técnico-seguridad en la que se examinaron informes de vulnerabilidades en la infraestructura digital del Estado mexicano, tomando como eje los antecedentes de filtraciones masivas de datos ocurridos en el periodo 2022-2024. Finalmente, el estudio concluye con una fase crítica orientada a evaluar la eficacia de los protocolos de resguardo biométrico del Instituto Nacional de Migración frente a los estándares internacionales de derechos humanos, permitiendo así la síntesis de propuestas de fortalecimiento institucional.

RESULTADOS Y DISCUSIÓN

Fundamentación Constitucional y Convencional.

El despliegue de tecnologías biométricas en el control migratorio mexicano no puede ser analizado como un acto administrativo aislado, sino que debe examinarse bajo el prisma del bloque de constitucionalidad. El artículo 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos (2025) establece el mandato imperativo de proteger los datos personales, otorgando a los individuos el poder de disposición y control sobre su información sensible. No obstante, en la praxis del Instituto Nacional de Migración, este derecho fundamental entra en colisión con la facultad estatal de control fronterizo. Al respecto, la Suprema Corte de Justicia de la Nación, en la jurisprudencia 1a./J. 115/2012 (10a.), ha establecido que el derecho a la inviolabilidad de las comunicaciones privadas se extiende a la protección de los datos almacenados en dispositivos tecnológicos. Este criterio es fundamental en el contexto migratorio, pues implica que la información digital y biométrica de la persona constituye un ámbito reservado frente a intrusiones de la autoridad administrativa; por tanto,

cualquier acceso o recolección de dichos datos debe estar estrictamente justificado y observar las garantías constitucionales de legalidad y control judicial (SCJN, 2013).Esta protección constitucional no debe entenderse de manera aislada, sino en estrecha relación con el principio de autodeterminación informativa. De acuerdo con la doctrina del Instituto Nacional de Acceso a la Información (INAI) y los criterios más recientes en materia de transparencia, el control sobre el dato biométrico es una facultad indisponible del Estado; es decir, la autoridad migratoria no se convierte en dueña de la información, sino en una mera depositaria temporal. La falta de claridad en los tiempos de almacenamiento y las condiciones de cancelación de estos datos en los sistemas del INM genera una zona de penumbra jurídica que contraviene el espíritu garantista del artículo 16. Por ende, la seguridad nacional, si bien es un fin legítimo, no puede operar como una excepción absoluta que anule el núcleo esencial del derecho a la privacidad del migrante.

Esta exigencia de legitimidad nos conduce necesariamente al test de proporcionalidad, criterio sostenido indirectamente por el alto tribunal en la tesis 1ª. CCLXIII/2014 (10ª) en la que si bien concierne a la niñez y adolescencia que ha sufrido algún delito y considerando directrices del Fondo de las Naciones Unidas para la Infancia (UNICEF) así como del Consejo Económico y Social de las Naciones Unidas, retomados por la Suprema Corte de Justicia de la Nación en el Protocolo de Actuación para quienes imparten justicia en casos que involucren Niñas, Niños y Adolescentes enfocándose en los casos de realizarles las entrevistas. Según este estándar, puede obtenerse que para que el INM recoja rasgos físicos inalterables como el iris o la huella dactilar, la medida no sólo debe ser legal sino idónea, necesaria y proporcional en sentido estricto.

De igual manera, como puede apreciarse en el criterio aislado IV.1o.A.11 A (11a.) emitido por la propia Corte Mexicana, se establece la siguiente obligación para el actuar administrativo:

> Todas las autoridades tienen la obligación de atender y defender los derechos humanos y la prohibición de interpretar en el sentido de permitir suprimir el goce y ejercicio de los derechos y libertades reconocidos o limitarlos en mayor medida que la prevista en ellas. (SCJN, 2022)

Si bien este criterio emana de la protección a la infancia, su lógica de proporcionalidad es perfectamente analógica para el migrante en situación de vulnerabilidad extrema.

En este punto, el Derecho comparado ofrece una perspectiva crítica: mientras que en México la recolección suele ser generalizada, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y las directrices de la Agencia Española de Protección de Datos (2023) exigen que el tratamiento de categorías especiales de datos sea excepcional y esté sujeto a una evaluación de impacto previa. Por tanto, la falta de protocolos de ciberseguridad robustos en México -evidenciada en vulneraciones previas- sugiere que el Estado podría estar incumpliendo con el principio de proporcionalidad, al recolectar datos cuya integridad no es capaz de garantizar plenamente.

La recolección de datos biométricos por parte del Instituto Nacional de Migración (INM) no debe entenderse como una facultad discrecional, sino como una actividad de alto riesgo que obliga al Estado a una tutela reforzada. Al respecto, el Poder Judicial de la Federación ha determinado que el deber del Estado de salvaguardar el derecho humano a la protección de datos personales debe potencializarse ante el uso de nuevas herramientas tecnológicas, debido a los riesgos que estas representan por sus características intrínsecas (SCJN, 2019). Bajo este criterio, la implementación de sistemas de identificación biométrica en el control migratorio no puede ser entendida como una facultad discrecional, sino como una actividad sujeta a una tutela reforzada, dado que la naturaleza de estas tecnologías exige que el Estado maximice las garantías para prevenir injerencias arbitrarias en la identidad y privacidad de las personas. Esta protección es fundamental porque el derecho a la protección de datos no es una prerrogativa aislada. Según ha determinado el Poder Judicial de la Federación, este constituye un derecho vinculado directamente con la salvaguarda de otros derechos fundamentales inherentes al ser humano, funcionando como un presupuesto necesario para el ejercicio de la libertad y la integridad (SCJN, 2019).

Bajo esta premisa, cualquier actuación del Estado, incluyendo el INM y el propio órgano garante de la transparencia, está obligada a interpretar el orden jurídico favoreciendo en todo tiempo la protección más amplia a las personas (SCJN, 2014a). En consecuencia, el titular de la información conserva en todo momento un interés jurídico para reclamar mediante el juicio de amparo cualquier determinación que ordene la elaboración de versiones públicas que puedan comprometer sus datos personales o sensibles (SCJN, 2014b).

Por lo tanto, el INM no puede omitir la implementación de protocolos de ciberseguridad robustos, que ya la vulneración de estos datos inalterables representaría un daño irreparable a la esfera jurídica del migrante.

Vulnerabilidades Sistémicas y Riesgos de Ciberseguridad en el Control Migratorio

La sofisticación de las amenazas digitales contemporáneas exige un cambio de paradigmas en la protección de las fronteras. De acuerdo con Li y Liu (2021), la evolución de los ciberataques ha pasado de simples intrusiones a operaciones complejas que explotan vulnerabilidades en infraestructuras críticas, lo que obliga al Estado a adoptar una 'Inteligencia sobre amenazas cibernéticas' (CTI) capaz de procesar datos masivos de manera sistemática. Al respecto, Cascavilla et al. (2021) sostienen que esta inteligencia no debe ser estática, sino que requiere una revisión multivocal y constante para anticipar vectores de ataque, que en el contexto del control migratorio, podrían dirigirse específicamente a la exfiltración de registros biométricos con fines de seguridad nacional o exploración ilícita.

Esta vulnerabilidad se acentúa drásticamente con la integración de la Inteligencia Artificial (IA) en el ecosistema delictivo. Caldwell et al. (2020) advierten que el 'crimen futuro' habilitado por la IA permitirá automatizar el robo de identidad a una escala sin precedentes, facilitando la creación de perfiles falsos que pueden burlar los controles fronterizos actuales. Esta preocupación es profundizada por Blauth et al. (2022) quienes subrayan que el abuso malicioso de la IA no solo pone en riesgo la privacidad individual, sino la integridad misma del sistema de control estatal. Para el migrante, esto significa que una vez que su rasgo biométrico es comprometido, queda en un estado de desprotección jurídica permanente, dado que la información biológica es inalterable y difícilmente recuperable tras un ataque.

Ante la incapacidad institucional de garantizar una seguridad robusta, surge la necesidad de implementar técnicas situacionales de prevención del delito (SCP) que controlen el entorno digital. Ho et al. (2022) sostienen que la prevención situacional reduce las oportunidades delictivas al aumentar el esfuerzo y el riesgo percibido por el atacante. Sin embargo, mientras el Estado no logre integrar estas técnicas de infraestructuras clave con las de transporte – donde la privacidad es ya un eslabón crítico conforme a López-Aguilar et al. (2022)-, el individuo queda expuesto a una pérdida total de control sobre su información.

Como indican Mcgregor et al. (2023), aunque existen opciones paliativas como el seguro cibernético personal, estas no sustituyen la obligación soberana de proteger el ciberespacio migratorio, dejando a los extranjeros en tránsito en una situación de riesgo sistémico e indefensión.

La identificación de las vulnerabilidades sistemáticas en el control migratorio no debe interpretarse como una crítica a la intención modernizadora del Estado, sino como un diagnóstico necesario para alcanzar una resiliencia institucional efectiva. Bajo esta perspectiva constructiva, el principal reto que enfrenta la implementación de datos biométricos en México es la transición de una visión estrictamente administrativa hacia una cultura de gestión integral de riesgos. Como se ha analizado a través de la taxonomía de Sánchez-García et al. (2023) la eficacia de cualquier sistema de ciberdefensa en el INM depende de un equilibrio simbiótico entre la infraestructura técnica y el fortalecimiento de las dimensiones organizacionales y humanas. Sin este mapeo sistemático de contramedidas, el esfuerzo por recolectar información de alto valor – como el iris o las huellas dactilares- podría generar una asimetría entre la capacidad de captación del dato y la capacidad soberana para garantizar su integridad a largo plazo.

Por consiguiente, el robustecimiento de los protocolos migratorios ante las amenazas de la inteligencia artificial y el ciberdelito situacional, advertidos por autores como Blauth et al. (2022) y Ho et al. (2022), constituye una oportunidad para que el Instituto Nacional de Migración se posicione como un referente regional en la protección de infraestructuras críticas. Este fortalecimiento no solo minimiza los riesgos de identidades sintéticas o exfiltración de información, sino que dota al actuar administrativo de una base técnica que justifica la intervención estatal sobre la privacidad del extranjero. En última instancia, reconocer la precariedad de los sistemas heredados y la obsolescencia técnica es el primer paso para proponer una gobernanza de datos que trascienda la reacción inmediata y se convierta en una política de Estado proactiva, transparente y, sobre todo, segura para el individuo en tránsito. Esta necesidad de seguridad técnica es precisamente, al que obliga a someter la práctica biométrica a un análisis jurídico superior para determinar si el riesgo detectado es proporcional al beneficio de seguridad perseguido.

En este contexto, resulta imperativo analizar la insuficiencia normativa del artículo 20 de la Ley de Migración. Si bien dicho precepto otorga al INM la facultad de recolectar información para el registro de extranjeros, su redacción es peligrosamente ambigua respecto a los estándares de ciberseguridad

exigibles. La ley se limita a autorizar la captación del dato, pero omite establecer las especificaciones técnicas de cifrado o los protocolos de respuesta ante incidentes como los analizados por Sánchez-García et al. (2023). Esta omisión legislativa crea un riesgo legal donde el actuar administrativo carece de un límite claro, permitiendo que la discrecionalidad técnica del Instituto prevalezca sobre el mandato constitucional de seguridad digital.

El Examen de Proporcionalidad de la Recolección Biométrica en el INM

Desde una perspectiva operativa y técnica, la biometría se presenta como una herramienta idónea porque, a diferencia de los documentos físicos, los rasgos biológicos son difícilmente transferibles o falsificables, lo que reduce drásticamente el error en la identificación. Aquí, la argumentación debe centrarse en que el Estado no busca "vigilar" por el simple hecho de hacerlo, sino de 'identificar para proteger', garantizando que la persona que solicita un trámite o refugio sea realmente quien dice ser, evitando así la suplantación de identidad que vulnera tanto al sistema como al propio migrante.

Análisis de Idoneidad y Necesidad

El análisis de idoneidad en el uso de herramientas biométricas por parte del Instituto Nacional de Migración (INM) no debe limitarse a una evaluación de su eficacia técnica, sino que debe considerar las implicaciones éticas de lo que se denomina la 'política epidérmica'.

Como argumentan Glouftsios et al. (2022), la digitalización de las fronteras conlleva el riesgo de que las infraestructuras de datos estigmatice a ciertos grupos, convirtiendo el rasgo biológico en una marca de control, en este sentido, para que la medida sea idónea en el contexto mexicano, la implementación debe trascender la simple vigilancia y orientarse hacia un modelo de gobernanza híbrido que, en palabras de Järv (2025), equilibre la eficiencia tecnológica con salvaguardas sólidas de derechos humanos y valores humanitarios fundamentales.

Por otro lado, la transición hacia un 'ensamblaje biométrico' plantea interrogantes críticos sobre la transparencia y la vulnerabilidad de los sujetos en tránsito. La investigación de Madianou (2019) advierte que el uso de estas tecnologías en sectores humanitarios y migratorios a menudo carece de regulaciones específicas, lo que podría afianzar desigualdades globales. En el caso de México, el reto de la 'idoneidad' radica en asegurar que la recolección de datos no se convierta en una forma de

‘extractivismo de datos’ (Poyares, 2025) donde la dignidad humana se ve desplazada por una lógica de predicción contractual y perfilamiento racial que desposee al migrante de su autonomía jurídica.

Así mismo, la implementación de inteligencia artificial en la gestión de asilo y refugio, aunque prometedora en términos de operatividad, exige un examen de necesidad exhaustivo.

Nalbandian (2022) señala que, si bien estas herramientas pueden aumentar la eficiencia administrativa, su uso suele poner en peligro la transparencia del proceso. Para el control migratorio mexicano, esto implica que la tecnología no debe sustituir el juicio humano, sino complementarlo dentro de un marco de identificación objetiva que reconozca, como sugieren Grünenberg et al. (2020), que la biometría está siempre sujeta a la interpretación humana y a contextos sociales específicos.

Finalmente, el cumplimiento de los principios de necesidad y proporcionalidad en las bases de datos a gran escala requiere evitar la toma de decisiones automatizada que resulta discriminatoria. Brouwer (2020) sostiene que la legitimidad de estos sistemas se fundamenta en la limitación de propósitos y el respeto a la privacidad. Por lo tanto, el reto para el Estado Mexicano consiste en construir una arquitectura de seguridad que no reduzca al migrante a una simple ‘amenaza para la seguridad´ (Madianou et al., 2020), sino que se utilice la biometría como un puente para garantizar la identidad legal y el acceso a derechos, transformado el control fronterizo en un espacio de certidumbre jurídica y no de exclusión.

Al analizar el subexamen de necesidad, resulta imperativo cuestionar si la implementación de sistemas biométricos no excede los límites de la intervención estatal. Siguiendo el planteamiento de Singler (2021), este tipo de arquitecturas tecnológicas a menudo funcionan como una afirmación del poder soberano, donde el sistema identifica al migrante como un sujeto de riesgo para justificar intervenciones basadas en un ‘solucionismo tecnológico’ (p. 17). Bajo esta lógica, el reto para el INM no es solo la identificación técnica, sino evitar que la tecnología se convierta en una herramienta de estigmatización del individuo.

En este mismo sentido, la preocupación ética sobre la medición de los cuerpos se intensifica cuando el despliegue de estas herramientas ocurre sin salvaguardas legales suficientes. En concordancia con lo expuesto por Madianou (2019), el ensamblaje biométrico en el sector humanitario y migratorio genera inquietudes legítimas sobre el sesgo y las prácticas de intercambio de datos, factores que podrían

profundizar las desigualdades en contextos globales (p. 2). Por lo tanto, la proporcionalidad en sentido estricto exige que el Estado Mexicano no solo demuestre la utilidad del dato, sino que garantice que su tratamiento no perpetúe vulnerabilidades sociales o discriminación automatizada.

Hacia la Necesidad y Proporcionalidad

La evaluación del subexamen de necesidad requiere determinar si el Estado dispone de alternativas menos lesivas para alcanzar el mismo nivel de eficacia en la identificación. Al respecto, la experiencia en el cono sur ofrece un contraste relevante; Aravena Flores et al. (2025) señalan que en Chile, aunque la tecnología biométrica ha optimizado el control y la seguridad, la ausencia de una regulación específica y el riesgo de un uso indebido de los datos personales representan una frontera crítica para los derechos de los migrantes (p. 5). Esta observación sugiere que, en el caso mexicano, la 'necesidad' de la biometría debe estar indisolublemente ligada a un marco normativo robusto que impida que la eficiencia administrativa se traduzca en una vulneración de la privacidad.

En el contexto de la frontera norte, la presión tecnológica se intensifica. Murrugarra (2024) advierte que el uso intensivo de biometría en la zona fronteriza entre México y Estados Unidos podría comprometer significativamente derechos fundamentales sino existen mecanismos de transparencia claros. Por lo tanto, la proporcionalidad en la recolección de estos datos por el INM no solo depende de la herramienta en si, sino de la implementación de protocolos ciberdefensa que aseguren que el 'extractivismo de datos' no se convierta en una práctica institucionalizada, garantizando así que la digitalización de la frontera sea un proceso de protección y no solo de vigilancia.

Al profundizar en el análisis de la proporcionalidad en sentido estricto, es fundamental considerar la naturaleza del dato biométrico no solo como un recurso técnico, sino también como una extensión de la identidad del individuo. En este sentido, Bescherer (2025) argumenta que la implementación de infraestructuras digitales en la gestión migratoria da lugar a 'identidades disputadas', donde el registro tecnológico a menudo prevalece sobre la narrativa personal del migrante. Para el INM, este hallazgo es crucial: la digitalización de la frontera no debe simplificar la identidad del sujeto a un mero conjunto de algoritmos, pues esto podría derivar en una deshumanización del proceso administrativo y en una vulneración de la dignidad humana.

Complementando esta visión, el fenómeno de la recolección masiva de datos plantea interrogantes sobre el uso posterior de dicha información. Poyares (2025) introduce el concepto de 'extractivismo de datos' en el contexto fronterizo, describiéndolo como una práctica donde la tecnología biométrica se utiliza para capturar información vital de poblaciones vulnerables que, en muchas ocasiones, carecen de mecanismos reales para dar un consentimiento informado (p. 14). Bajo esta premisa, la proporcionalidad exige que el Estado mexicano implemente protocolos de seguridad que garanticen que la información recopilada por el INM sea utilizada exclusivamente para los fines de control migratorio previstos por la ley, evitando que el migrante se convierta en un 'recurso de datos' para otros fines no autorizados.

DISCUSIÓN

Como corolario del análisis de proporcionalidad y los riesgos de extractivismo de datos expuesto, la transición hacia una gobernanza migratoria ética en México no puede postergarse. Resulta imperativo que el marco normativo del INM evolucione de una visión puramente securitaria hacia una protección integral de la identidad digital. En este sentido, la propuesta de reforma debe articularse sobre tres ejes fundamentales. Primero, la positivización del principio de finalidad, que restringe el uso de los datos biométricos exclusivamente a los objetivos migratorios originales, mitigando así el riesgo de uso indebido señalado por Poyares (2025).

Segundo, es indispensable la implementación de mecanismos de transparencia algorítmica y el reconocimiento del 'derecho al olvido' biométrico, permitiendo que la digitalización de la frontera no se traduzca en una vigilancia perpetua. Estas medidas, lejos de debilitar el control estatal, fortalecen la legitimidad de las instituciones al alinearlas con los estándares internacionales de derechos humanos y la protección de datos personales en contextos de vulnerabilidad.

Más allá de la reforma legal, el reto subyacente para el Estado mexicano es la construcción de una verdadera soberanía de datos migratorios. Esto implica que el INM no solo debe ser capaz de proteger la información frente a ciberataques externos, sino también de garantizar que el procesamiento de los biométricos sea auditable y soberano, evitando la dependencia tecnológica de proveedores externos que podrían replicar los sesgos algorítmicos advertidos por la literatura internacional.

La justicia migratoria en la era digital depende de que el algoritmo no sea una 'caja negra' inaccesible para el derecho, sino un proceso transparente sujeto al escrutinio judicial.

CONCLUSIONES

En conclusión, la integración de tecnologías biométricas en el Instituto Nacional de Migración representa un avance técnico innegable, pero su validez constitucional depende de un equilibrio entre la eficacia administrativa y la dignidad humana. A lo largo de esta investigación, se ha demostrado que, si bien la biometría es una herramienta idónea para la identificación, su aplicación actual en México carece de las salvaguardas legales suficientes para superar el examen de proporcionalidad. La existencia de 'identidades disputadas' y la vulnerabilidad ante el extractivismo de datos, como advierten Bescherer (2025) y Poyares (2025), obligan a replantear el papel del Estado no como un simple recolector de información corporal, sino como un custodio de derechos fundamentales.

Finalmente, el éxito de una política migratoria moderna no debe medirse por la cantidad de datos almacenados, sino por la capacidad de procesarlos bajo principios de transparencia y justicia. Solo mediante una reforma que garantice la seguridad jurídica y el control sobre la propia identidad digital, México podrá asegurar que la tecnología en sus fronteras sea un instrumento de orden y no un mecanismo de exclusión o estigmatización automatizada.

Declaración de Ética y Uso de Inteligencia Artificial

Transparencia tecnológica: Durante la fase de revisión técnica y refinamiento del manuscrito, el autor empleó herramientas de inteligencia artificial generativa exclusivamente como soporte para el procesamiento de lenguaje natural. Esta asistencia se limitó a la optimización de la fluidez narrativa, la precisión gramatical y la corrección ortotipográfica del documento.

Responsabilidad de autoría e integridad: El uso de estas tecnologías se circunscribió estrictamente a la asistencia editorial y de estilo. La selección de los marcos teóricos (incluyendo conceptos como extractivismo de datos e identidades disputadas de los autores debidamente citados), el desarrollo del análisis dogmático-jurídico, la interpretación de la jurisprudencia y la síntesis de las propuestas finales son resultado de la actividad intelectual del investigador. El autor ha revisado y validado integralmente el contenido final, asumiendo la responsabilidad total por la originalidad del análisis, la correcta atribución de fuentes y el cumplimiento de las normas de citación APA (ed. 7.ª).

Conflicto de intereses: El autor declara la ausencia de conflictos de intereses personales o financieros en la realización de esta investigación.

REFERENCIAS BIBLIOGRAFICAS

Agencia Española de Protección de Datos. (2023). *Guía sobre tratamientos de control de presencia mediante sistemas biométricos*. https://www.aepd.es/

Aravena Flores, M. A., & Brebi Rivera, R. B. (2025). Tecnología biométrica en el ingreso irregular del migrante en Chile ¿protección o control? *Revista de Derecho*, *10*(1). https://doi.org/10.47712/rd.2025.v10i1.302

Bernal, C. A. (2023). *Metodología de la investigación: administración, economía, humanidades y ciencias sociales* (6.ª ed.). Pearson Educación.

Bescherer, P. (2025). *Contested identities: Digital borders and the politics of migration management*. Oxford University Press.

Blauth, T., Gstrein, O., & Zwitter, A. (2022). Artificial Intelligence Crimes: An Overview of Malicious Use and Abuse of AI. *IEEE Access*, *10*, 77110-77122. https://doi.org/10.1109/access.2022.3191790

Brouwer, E. (2020). Large-scale databases and interoperability in migration and border policies: The non-discriminatory approach of data protection. *European Public Law*, *26*(4), 71-92.

Cáceres Nieto, E. (2020). *Metodología de la investigación jurídica y sociojurídica*. Instituto de Investigaciones Jurídicas, UNAM.

Caldwell, M., Andrews, J., Tanay, T., & Griffin, L. (2020). AI-enabled future crime. *Crime Science*, *9*(1), 1-22. https://doi.org/10.1186/s40163-020-00123-8

Cascavilla, G., Tamburri, D., & Heuvel, W. (2021). Cyber threat intelligence: A multivocal systematic literature review. *Computers & Security*, *105*, 102258. https://doi.org/10.1016/j.cose.2021.102258

Constitución Política de los Estados Unidos Mexicanos [CPEUM]. (2025). *Diario Oficial de la Federación*. Última reforma publicada el 20 de diciembre de 2024. http://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Diccionario Panhispánico del Español Jurídico. (2025). Dato biométrico. En *Diccionario Panhispánico del Español Jurídico*. Recuperado el 19 de diciembre de 2025, de https://dpej.rae.es/

Glouftsios, G., & Scheel, S. (2022). Epidermal politics: Control, violence and dissent at the biometric border. *Environment and Planning C: Politics and Space*, *40*(6), 1251-1269.

Grünenberg, K., & Casper, M. (2020). Introduction to the theme: IDentities and Identity: Biometric Technologies, Borders and Migration. *Ethnos*, *85*(3), 381-395.

Ho, H., Ko, R., & Mazerolle, L. (2022). Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review. *Computers & Security*, *115*, 102611. https://doi.org/10.1016/j.cose.2022.102611

Järv, K. (2025). Digital borders and migrants' rights: The clash between technology, international law and humanitarian values. *Proceedings of the International Symposium on Migration and Technology*.

Li, Y., & Liu, Q. (2021). A comprehensive review study on cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

López-Aguilar, P., Batista, E., Martínez-Ballesté, A., & Solanas, A. (2022). Information Security and Privacy in Railway Transportation: A Systematic Review. *Sensors*, *22*(20), 7698. https://doi.org/10.3390/s22207698

Madianou, M. (2019). The biometric assemblage: Surveillance, experimentation, profit and the measuring of refugee bodies. *Television & New Media*, *20*(6), 581-599.

Madianou, M., Dencik, L., Aradau, C., Taylor, L., Metcalfe, P., & Perret, S. (2020). The biometric lives of migrants: Borders, discrimination and (in)justice. *AoIR Selected Papers of Internet Research*. https://doi.org/10.5210/spir.v2020i0.11137

Mcgregor, R., Reaiche, C., Boyle, S., & Zubielqui, G. (2023). Cyberspace and Personal Cyber Insurance: A Systematic Review. *Journal of Computer Information Systems*, *64*(2), 157-171. https://doi.org/10.1080/08874417.2023.2185551

Murrugarra, B. I. (2024). Vigilancia fronteriza: tecnologías biométricas y datos personales en la migración latinoamericana. *Epistemia Revista Científica*, *8*(2), 1-16. https://doi.org/10.26495/erc.2820

Nalbandian, L. (2022). An eye for an 'I': A critical assessment of artificial intelligence tools in migration and asylum management. *Comparative Migration Studies*, *10*(1), 1-22.

Parlamento Europeo y del Consejo. (2016). Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD). *Diario Oficial de la Unión Europea*.

Ponce de León Armenta, L. (2023). *Metodología de la ciencia jurídica* (21.ª ed.). Editorial Porrúa.

Poyares, M. (2025). Migrant data extractivism: Technology and borders at the limits of rights. *International Migration*, *63*(1), 112-128.

Red en Defensa de los Derechos Digitales [R3D]. (2022, 3 de octubre). *Guacamaya Leaks: El hackeo a SEDENA y los riesgos de la militarización digital*. https://r3d.mx/

Ruíz, S., Alvez, C. E., Etchart, G., & Miranda, E. (2022). Hacia la definición de un marco metodológico para el desarrollo de un sistema de reconocimiento biométrico mediante técnicas de Machine Learning. En *XXIV Workshop de Investigadores en Ciencias de la Computación* (WICC 2022, Mendoza).

Salinas Ramos, J. (2021). *Métodos y técnicas de investigación jurídica: Una visión práctica*. Tirant lo Blanch.

Sánchez-García, I., Gilabert, T., & Calvo-Manzano, J. (2023). Contramedidas y sus taxonomías para el tratamiento de riesgos en ciberseguridad: una revisión sistemática de mapeo. *Computers & Security*, *128*, 103170. https://doi.org/10.1016/j.cose.2023.103170

Secretaría de Gobernación. (2019, 30 de diciembre). Lineamientos para trámites y procedimientos migratorios. *Diario Oficial de la Federación*.

Simón Castellano, P., & Dorado Ferrer, X. (2022). Límites y garantías constitucionales frente a la identificación biométrica. *IDP. Revista de Internet, Derecho y Política*, (35), 1-13. https://doi.org/10.7238/idp.v0i35.392324

Singler, S. (2021). Biometric statehood, transnational solutionism and security devices: The performative dimensions of IOM's MIDAS. *Theoretical Criminology*, *25*(3), 440-461.

Suprema Corte de Justicia de la Nación. (2013). Tesis: 1a./J. 115/2012 (10a.). Derecho a la inviolabilidad de las comunicaciones privadas. Su ámbito de protección se extiende a los datos almacenados en el teléfono móvil asegurado a una persona detenida y sujeta a investigación por la posible comisión de un delito. *Semanario Judicial de la Federación y su Gaceta*, Libro XVII, Tomo 1, p. 431. (Registro digital: 2002741).

Suprema Corte de Justicia de la Nación. (2014a). Tesis: 1a. CCLXIII/2014 (10a.). Test de proporcionalidad de las leyes. Pasos a seguir por el juzgador para determinar si una medida legislativa limita un derecho fundamental. *Gaceta del Semanario Judicial de la Federación*, Libro 10, Tomo I, p. 157. (Registro digital: 2007064).

Suprema Corte de Justicia de la Nación. (2014b). Tesis: 2a. CVI/2014 (10a.). Derecho a la información. El titular de ésta tiene interés jurídico para reclamar en amparo... *Gaceta del Semanario Judicial de la Federación*, Libro 11, Tomo I, p. 1093. (Registro digital: 2007730).

Suprema Corte de Justicia de la Nación. (2018). Tesis: 2a. LVI/2018 (10a.). Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Como autoridad del Estado, está obligado a promover, respetar, proteger y garantizar los derechos humanos... *Gaceta del Semanario Judicial de la Federación*, Libro 55, Tomo II, p. 1463. (Registro digital: 2017154).

Suprema Corte de Justicia de la Nación. (2019a). Tesis: I.10o.A.6 CS (10a.). Protección de datos personales. El deber del Estado de salvaguardar el derecho humano relativo debe potencializarse ante las nuevas herramientas tecnológicas, debido a los riesgos que éstas representan por sus características. *Gaceta del Semanario Judicial de la Federación*, Libro 70, Tomo III, p. 2200. (Registro digital: 2020564).

Suprema Corte de Justicia de la Nación. (2019b). Tesis: I.10o.A.5 CS (10a.). Protección de datos personales. Constituye un derecho vinculado con la salvaguarda de otros derechos fundamentales inherentes al ser humano. *Gaceta del Semanario Judicial de la Federación*, Libro 70, Tomo III, p. 2199. (Registro digital: 2020563).

Suprema Corte de Justicia de la Nación. (2022). Tesis: IV.1o.A.11 A (11a.). Migrantes. Privación de la libertad en estaciones migratorias. Debe privilegiarse siempre una medida menos gravosa y estrictamente necesaria para proteger los bienes jurídicos fundamentales de los migrantes, de lo contrario, conduciría al ejercicio abusivo del poder punitivo del Estado. *Gaceta del Semanario Judicial de la Federación*, Libro 19, Tomo IV, p. 3696. (Registro digital: 2025513).