Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), julio-agosto 2025,
Volumen 9, Número 4.

https://doi.org/10.37811/cl_rcm.v9i2

FRONTERAS DIGITALES EN LA ERA GLOBAL: UN ANÁLISIS COMPARATIVO ENTRE ESTADOS UNIDOS-MÉXICO Y TURQUÍA-ASIA

DIGITAL FRONTIERS IN THE GLOBAL ERA: A COMPARATIVE ANALYSIS OF THE UNITED STATES-MEXICO AND TÜRKIYE-ASIA REGIONS

María de los Angeles Blandón Salinas
CISAN-Universidad Autónoma de México, México

DOI: https://doi.org/10.37811/cl_rcm.v9i4.20041

Fronteras Digitales en la Era Global: Un Análisis Comparativo entre Estados Unidos-México y Turquía-Asia

María de los Angeles Blandón Salinas[1]
angeles2013@gmail.com[2]
https://orcid.org/0000-0002-7578-4650
CISAN-Universidad Autónoma de Mexico
Ciudad de México-México

RESUMEN

El artículo Fronteras Digitales en la era Global: Un Análisis Comparativo entre Estados Unidos-México y Turquía-Asia examina el papel de las tecnologías digitales en la configuración de fronteras contemporáneas, entendidas no solo como límites territoriales, sino como dispositivos de vigilancia, control y securitización. El objetivo central es analizar críticamente cómo se despliegan y articulan los mecanismos digitales de control fronterizo en ambos escenarios, a fin de identificar sus convergencias, divergencias e implicaciones para la movilidad humana y la seguridad regional. Metodológicamente, se desarrolló un enfoque cualitativo de carácter exploratorio y descriptivo, sustentado en un diseño documental y comparativo, que incluyó la revisión de informes gubernamentales, bases de datos oficiales, reportes de organismos internacionales, literatura académica y análisis crítico de discurso. Los resultados evidencian que, mientras Estados Unidos–México constituye un laboratorio de securitización tecnológica con fuerte participación de la industria privada y un modelo de *muro virtual*, Turquía–Asia se posiciona como un nodo estratégico en la gestión migratoria europea, donde las tecnologías digitales se emplean como instrumentos de contención y negociación política. Se concluye que ambos casos reflejan la consolidación de un paradigma global de frontera digital caracterizado por la vigilancia biométrica, la cooperación transnacional y la creciente opacidad en torno al uso de datos, lo que plantea riesgos éticos y retos urgentes para los derechos humanos.

***Palabras clave*:** fronteras digitales, gubernamentalidad algorítmica, vigilancia transnacional, control migratorio, violencia estructural

[1]UNAM, Programa de Becas Posdoctorales en la UNAM. Becaria del Centro de Investigaciones sobre América del Norte (CISAN), asesorada por el Dr. Juan Carlos Barrón Pastor.

[2] Autor principal. Correspondencia: angeles2013@gmail.com. Miembro del Proyecto PAPIIT IN302324, Comunicación y diplomacia de las diásporas. Perspectivas desde los contextos de recepción en las Américas, Europa y Asia.

Digital Frontiers in the Global Era: A Comparative Analysis of the United States-Mexico and Türkiye-Asia Regions

ABSTRACT

The article Digital Borders in the Global Era: A Comparative Analysis between the United States–Mexico and Turkey–Asia examines the role of digital technologies in shaping contemporary borders, understood not only as territorial limits but also as devices of surveillance, control, and securitization. The main objective is to critically analyze how digital mechanisms of border control are deployed and articulated in both contexts, in order to identify their convergences, divergences, and implications for human mobility and regional security. Methodologically, the study adopts a qualitative, exploratory, and descriptive approach, based on a documentary and comparative design that included the review of governmental reports, official databases, international organizations' publications, academic literature, and critical discourse analysis. The findings reveal that while the United States–Mexico border functions as a laboratory of technological securitization, heavily influenced by private industry and the development of a *virtual wall,* the Turkey–Asia border emerges as a strategic node in European migration management, where digital technologies operate as instruments of containment and political negotiation. The study concludes that both cases reflect the consolidation of a global paradigm of digital borders characterized by biometric surveillance, transnational cooperation, and increasing opacity in data use, raising ethical concerns and urgent challenges for human rights.

***Keywords*:** digital bordering, algorithmic governmentality, transnational surveillance, migration control, structural violence

Artículo recibido 04 Agosto 2025
Aceptado para publicación: 29 Agosto 2025

INTRODUCCIÓN

En la era global contemporánea, las fronteras han dejado de ser únicamente líneas físicas que separan territorios nacionales para convertirse en espacios complejos donde lo digital desempeña un papel central. La digitalización de las fronteras, a través de tecnologías biométricas, sistemas algorítmicos de vigilancia e infraestructuras de datos, redefine los modos de control, seguridad y movilidad. El presente artículo aborda de manera comparativa los casos de la frontera Estados Unidos–México y la frontera Turquía–Asia, dos escenarios que, aunque situados en contextos geopolíticos distintos, muestran procesos convergentes de securitización tecnológica.

El problema de investigación que guía este estudio surge de un vacío en la literatura académica: mientras que la frontera Estados Unidos–México ha sido objeto de múltiples investigaciones en torno a la militarización y digitalización del control migratorio, existe una menor atención en torno a Turquía como espacio donde se articulan la vigilancia digital, la externalización de fronteras europeas y la contención de refugiados procedentes de guerras regionales. El contraste entre ambos casos permite indagar cómo las fronteras digitales operan bajo lógicas globales, pero se adaptan a realidades políticas y geográficas específicas.

La relevancia de este tema radica en su impacto en tres dimensiones centrales. En primer lugar, revela cómo las tecnologías digitales reconfiguran la noción de soberanía y seguridad, desplazando las prácticas fronterizas tradicionales hacia un ámbito de control de datos y vigilancia remota. En segundo lugar, pone de manifiesto la creciente participación de corporaciones privadas en tareas de seguridad, lo que evidencia una transformación en la gobernanza de las fronteras. Finalmente, subraya los desafíos éticos y legales que estas prácticas imponen sobre los derechos humanos de migrantes y refugiados, quienes se convierten en sujetos privilegiados de experimentación tecnológica y control algorítmico.

El análisis se sostiene en un marco teórico interdisciplinario que articula conceptos de la biopolítica de Michel Foucault (2007), útil para comprender la gestión de poblaciones a través de dispositivos de seguridad; la gubernamentalidad algorítmica de Antoinette Rouvroy y Thomas Berns (2013), que permite examinar cómo los algoritmos clasifican y jerarquizan cuerpos en función de riesgos; y el enfoque de border as method de Sandro Mezzadra y Brett Neilson (2013), que concibe las fronteras como dispositivos de producción de desigualdades.

Asimismo, se incorporan aportes de los estudios críticos de seguridad (Buzan, Wæver y de Wilde, 1998), que cuestionan las narrativas de amenaza como justificación de medidas extraordinarias.

Los antecedentes académicos ofrecen bases importantes. Investigaciones como las de Louise Amoore (2020) han explorado las implicaciones éticas de los algoritmos en la seguridad; Didier Bigo (2002) ha analizado la intersección entre migración y vigilancia; y Nicholas De Genova (2017) ha estudiado las fronteras europeas como espacios de tensión y control. En el caso estadounidense, Todd Miller (2019) ha documentado el desarrollo del muro virtual, mientras que en el caso turco destacan estudios sobre su rol como socio de la Unión Europea en la externalización de fronteras (Kaslı & Parla, 2019). No obstante, aún son escasos los trabajos que articulen ambos contextos bajo una perspectiva comparativa, lo que constituye la principal contribución de este estudio.

El contexto en el que se sitúa la investigación está marcado, en el caso de Estados Unidos–México, por una larga trayectoria de políticas migratorias restrictivas, reforzadas tras los atentados del 11 de septiembre de 2001, que incrementaron las inversiones en drones, sensores y bases de datos biométricos. En Turquía, el detonante ha sido la guerra en Siria y la llegada masiva de refugiados desde 2011, que posicionaron al país como un actor central en la contención migratoria, especialmente tras los acuerdos firmados con la Unión Europea. Estos escenarios, aunque distantes, comparten la tendencia a fortalecer las fronteras mediante la incorporación de tecnologías digitales avanzadas.

En este marco, el artículo parte de la hipótesis de que la digitalización de las fronteras en Estados Unidos–México y Turquía–Asia responde a una lógica común de securitización global basada en tecnologías biométricas y algoritmos de vigilancia, aunque se adapte a contextos históricos y geopolíticos distintos.

El objetivo general es analizar comparativamente los procesos de digitalización fronteriza en ambos casos, identificando similitudes, diferencias e implicaciones. Para alcanzarlo, se plantean cuatro objetivos específicos: describir las tecnologías implementadas, examinar el papel de las corporaciones privadas en su desarrollo, evaluar los efectos sobre los derechos humanos y reconocer patrones comunes y divergentes en la securitización digital.

METODOLOGIA

El presente estudio se enmarca en un enfoque cualitativo de carácter comparativo, cuyo objetivo es explorar críticamente las configuraciones de las fronteras digitales en dos escenarios geopolíticos distintos: la frontera Estados Unidos–México y la de Turquía con Asia. Este diseño se justifica porque la investigación busca comprender procesos complejos vinculados a la gobernanza tecnológica, la soberanía digital y los impactos en derechos humanos, más que medir variables cuantitativas.

Además, este tipo de análisis es particularmente útil para estudiar fenómenos transnacionales, como la digitalización de fronteras, que involucran actores estatales y no estatales, así como múltiples escalas de gobernanza (Ragin, 2014).

El tipo de investigación es de carácter exploratorio y descriptivo, puesto que examina realidades en la literatura comparativa sobre fronteras digitales, y a la vez se orienta a describir las particularidades de cada caso en su especificidad histórica y política. Asimismo, se sostiene una perspectiva relacional, en tanto interesa identificar los puntos de convergencia y divergencia entre los modelos de control digital desplegados en ambos escenarios.

En cuanto al diseño de investigación, se adoptó un diseño documental, transversal y de corte interpretativo, fundamentado en la revisión crítica de fuentes secundarias: informes oficiales de organismos internacionales, reportes de ONG dedicadas a la defensa de derechos humanos, bases de datos gubernamentales, legislación nacional, notas periodísticas y literatura académica especializada. Este diseño permite examinar cómo los discursos de seguridad y las tecnologías de vigilancia se articulan en distintos espacios fronterizos, sin que ello implique la aplicación de experimentos o estudios longitudinales.

La población de estudio no se refiere a sujetos individuales, sino a los discursos, marcos normativos y tecnologías empleadas en el control fronterizo. Se tomaron como informantes clave los documentos estratégicos de agencias como la U.S. Customs and Border Protection (CBP), el Ministerio del Interior de Turquía y reportes de empresas privadas de tecnología de seguridad. Para garantizar una selección coherente de materiales, se empleó un muestreo teórico y de conveniencia, en el que se priorizaron fuentes que ofrecieran datos relevantes sobre vigilancia digital, securitización migratoria y cooperación transnacional en ambos casos de estudio.

En cuanto a las técnicas de recolección de datos, se utilizó principalmente la revisión documental y el análisis crítico de discurso, apoyados con una matriz analítica que permitió organizar y sistematizar la información recabada de manera comparativa. En relación con las consideraciones éticas, se respetó la confidencialidad de las fuentes y se adoptó un enfoque crítico que busca problematizar las asimetrías de poder en el uso de tecnologías digitales, reconociendo el sesgo estructural que atraviesa los discursos de seguridad.

Finalmente, las limitaciones del estudio se vinculan a la disponibilidad de información oficial, ya que no incluye entrevistas con actores clave ni observación directa de los sistemas tecnológicos. Asimismo, algunos documentos oficiales no ofrecen información completa sobre la arquitectura técnica de las soluciones utilizadas, debido a restricciones de seguridad nacional. Estas limitaciones son comunes en investigaciones sobre tecnologías de seguridad, pero se mitigaron mediante el uso de múltiples fuentes y la triangulación de datos.

RESULTADOS Y DISCUSIÓN

El análisis comparativo evidencia que las fronteras contemporáneas operan cada vez más como dispositivos digitales de control y securitización, articulando tecnología, instituciones y normativas de manera integral. En el caso de la frontera Estados Unidos–México, la frontera entre Estados Unidos y México, con 3,169 kilómetros de extensión, ha sido objeto de una creciente securitización desde la década de 1990, cuando la Operación Guardián (*Operation Gatekeeper*) marcó el inicio del despliegue intensivo de infraestructura física y vigilancia en zonas urbanas fronterizas (Nevins, 2010). Este enfoque se intensificó tras los atentados del 11 de septiembre de 2001, con la promulgación del *USA PATRIOT Act* y la creación del Departamento de Seguridad Nacional (DHS), que consolidó la agenda de control fronterizo bajo un marco de seguridad nacional (Andreas, 2009).

En 2005, el Congreso de Estados Unidos aprobó el *Secure Fence Act*, que destinó más de 2.3 mil millones de dólares a la construcción de cercas y sistemas de vigilancia (Rosenblum, 2021). Sin embargo, a partir de 2017, el énfasis comenzó a trasladarse hacia soluciones tecnológicas, dando lugar al llamado *muro virtual* (*Virtual Border Wall*), cuyo costo se estima en más de 1.2 mil millones de dólares en contratos tecnológicos adjudicados entre 2018 y 2023 (Tech Inquiry, 2025).

El modelo estadounidense combina múltiples capas tecnológicas. Una de las piezas centrales es el uso de torres de vigilancia autónomas diseñadas por Anduril Industries, equipadas con sensores ópticos, cámaras de alta resolución y radares de largo alcance, capaces de operar de manera autónoma y transmitir datos en tiempo real a centros de comando (Anduril Industries, 2022). Estas torres utilizan inteligencia artificial para diferenciar entre humanos, animales y vehículos, reduciendo la dependencia del patrullaje humano (Rosenblum, 2021).

Además, la Patrulla Fronteriza de Estados Unidos (CBP) emplea drones MQ-9 Reaper, fabricados por General Atomics, para la vigilancia aérea de áreas remotas. Cada dron tiene un costo aproximado de 30 millones de dólares y está equipado con sensores infrarrojos y de movimiento (GAO, 2021). En 2022, la flota de drones de la CBP realizó más de 7,500 horas de vuelo en la frontera sur (CBP, 2023).

La recopilación y análisis de datos es gestionada por Palantir Technologies, que provee software de análisis predictivo utilizado para crear mapas de riesgo, evaluar patrones migratorios y generar alertas automatizadas (Tech Inquiry, 2025).

Estos sistemas permiten a los agentes fronterizos anticipar movimientos migratorios y optimizar despliegues de recursos, pero generan preocupaciones sobre vigilancia masiva y uso de perfiles de riesgo basados en criterios opacos (Privacy International, 2024).

Desde 2019, el programa Biometric Entry-Exit del DHS ha implementado sistemas de reconocimiento facial en 238 aeropuertos y 32 puntos fronterizos terrestres, con el objetivo de verificar la identidad de viajeros y detectar posibles cruces no autorizados (DHS, 2023). Este sistema, desarrollado con tecnología de la empresa IDEMIA, ya ha escaneado a más de 200 millones de personas, con un presupuesto de 430 millones de dólares (GAO, 2021).

En paralelo, el proyecto Integrated Fixed Towers (IFT), que sustituyó parcialmente al fallido SBInet, integra torres fijas con cámaras térmicas y radares de vigilancia perimetral, con contratos por 700 millones de dólares adjudicados principalmente a la empresa Elbit Systems of America, filial de la empresa israelí Elbit (Rosenblum, 2021). Estas torres permiten un monitoreo continuo, incluso en zonas de difícil acceso, complementando la presencia de agentes fronterizos.

La combinación de estas tecnologías con algoritmos de aprendizaje automático permite realizar un control fronterizo predictivo, orientado no solo a registrar cruces, sino a anticipar comportamientos considerados riesgosos. Este modelo, sin embargo, enfrenta críticas por su opacidad y la posibilidad de replicar sesgos raciales o geográficos en la toma de decisiones (Koubi, 2021).

La digitalización de la frontera sur de Estados Unidos ha generado un mercado multimillonario de seguridad fronteriza. Solo entre 2018 y 2023, el DHS adjudicó contratos tecnológicos por más de 4.5 mil millones de dólares, de los cuales Anduril Industries recibió aproximadamente 250 millones para el desarrollo de torres autónomas, mientras que Palantir Technologies obtuvo 180 millones para plataformas de análisis de datos (Tech Inquiry, 2025).

Empresas como General Dynamics, Lockheed Martin y Northrop Grumman también participan en la provisión de radares, sensores y servicios de integración tecnológica (Surveillance Watch, 2025). Este entramado evidencia un proceso de privatización de la gestión fronteriza, donde empresas con fines de lucro influyen en decisiones de seguridad y política migratoria, desplazando parcialmente las funciones tradicionales del Estado (Benítez Manaut, 2021).

Sin embargo, el despliegue de estas tecnologías tiene un impacto directo en las personas migrantes. Organizaciones de derechos humanos han documentado un aumento en la mortalidad de migrantes, ya que el uso de vigilancia avanzada obliga a las personas a tomar rutas más peligrosas a través del desierto. Además, el uso de biometría sin consentimiento y de algoritmos de perfilamiento plantea riesgos de discriminación y violaciones a la privacidad (European Council on Refugees, 2024).

El Comité de Derechos Humanos de la ONU ha advertido que las políticas que priorizan el control tecnológico sobre la protección humanitaria pueden vulnerar el derecho a solicitar asilo y el principio de no devolución (*non-refoulement*) (United Nations, 2022). En el caso estadounidense, la ausencia de una ley federal integral de protección de datos aumenta la vulnerabilidad de la información personal recopilada (Privacy International, 2024).

En síntesis, el modelo de frontera digital Estados Unidos–México se ha consolidado como un modelo conocido como muro virtual, que permite la monitorización en tiempo real de movimientos migratorios, la predicción de rutas de tránsito y la priorización de zonas de alto riesgo mediante algoritmos de inteligencia artificial (GAO, 2020; Chishti & Hipsman, 2021).

Es una industria multimillonaria, fuertemente impulsada por tecnologías de inteligencia artificial, aprendizaje automático y sistemas autónomos. Según la Electronic Frontier Foundation (EFF, 2025), más de 230 proveedores tecnológicos participan en la provisión de equipos y servicios para el Departamento de Seguridad Nacional (DHS), incluyendo empresas reconocidas como Anduril Industries y Elbit Systems, así como contratistas menos visibles. Estos proveedores suministran desde sistemas de vigilancia, radares y sensores, hasta plataformas de análisis de datos y soluciones biométricas, abasteciendo no solo a la Patrulla Fronteriza (CBP) y al Servicio de Inmigración y Control de Aduanas (ICE), sino también a otras agencias federales. El estudio evidencia la opacidad del sector, la concentración del mercado y la creciente interdependencia entre empresas privadas y el Estado, revelando cómo la gestión fronteriza se ha privatizado y mercantilizado.

Este entramado corporativo no solo refuerza la eficiencia del control fronterizo, sino que también plantea desafíos significativos en términos de privacidad, ética y derechos humanos, al priorizar la seguridad y la rentabilidad sobre la protección de las personas migrantes.

En contraste, la frontera Turquía–Asia presenta un modelo híbrido donde la tecnología se emplea principalmente para gestionar flujos migratorios hacia Europa, más que para bloquear físicamente el tránsito. Lo anterior se debe a que, tras la crisis migratoria de 2015, la UE reforzó la vigilancia y control fronterizo mediante la creación de Frontex, la Agencia Europea de la Guardia de Fronteras y Costas, que ha experimentado una expansión significativa en funciones y presupuesto, pasando de 143 millones de euros en 2015 a más de 460 millones en 2023 (Frontex, 2023).

El acuerdo migratorio UE-Turquía de 2016 estableció un mecanismo de externalización de control migratorio, mediante el cual Turquía actúa como frontera proxy para la UE, recibiendo apoyo financiero y tecnológico para gestionar flujos migratorios y prevenir cruces irregulares (Lazaridis & Campani, 2017). Esta estrategia se complementa con la implementación de sistemas digitales avanzados en el espacio Schengen y sus fronteras exteriores, extendiendo el control fronterizo más allá del territorio europeo.

Frontex ha implementado una plataforma tecnológica integrada llamada EUROSUR (Sistema Europeo de Vigilancia de Fronteras), que combina vigilancia por satélite, drones, radares y sistemas de inteligencia artificial para monitorear las fronteras marítimas y terrestres (Frontex, 2023).

El presupuesto destinado a EUROSUR ascendió a aproximadamente 170 millones de euros desde 2016 (European Commission, 2021).

Empresas como Thales Group, Airbus Defence and Space y Leonardo son proveedores clave de tecnologías de vigilancia para la UE. Por ejemplo, Thales provee soluciones de reconocimiento facial y biometría desplegadas en puntos de entrada, mientras Airbus suministra servicios satelitales para la detección remota (European Commission, 2021).

En Turquía, la firma local HAVELSAN coopera con la UE y Frontex para implementar sistemas de vigilancia fronteriza que incluyen torres con cámaras térmicas, sensores acústicos y drones para patrullaje en la frontera con Siria e Irán (HAVELSAN, 2022). El presupuesto turco para tecnología fronteriza, con aportes europeos, supera los 250 millones de euros desde 2017 (Lazaridis & Campani, 2017).

Además, la UE ha desarrollado bases de datos biométricos como Eurodac, que contiene huellas dactilares de solicitantes de asilo, y el sistema ETIAS (Sistema Europeo de Información y Autorización de Viajes), previsto para implementarse completamente en 2024, que funcionará como un sistema de pre-autorización similar a ESTA estadounidense (European Commission, 2023).Una característica central del modelo europeo es la externalización de funciones de control migratorio a países terceros, especialmente Turquía, pero también a países asiáticos que actúan como puntos de tránsito y filtros para flujos migratorios hacia Europa (Guild, 2021). Esta estrategia implica transferencia tecnológica, financiera y de capacidades de vigilancia a estados que operan con estándares legales y de derechos humanos menos estrictos.

Este modelo genera una red compleja de gobernanza transnacional, donde los datos biométricos y perfiles migratorios se comparten y gestionan a través de múltiples jurisdicciones, dificultando el acceso a recursos legales para los migrantes y dificultando la supervisión democrática (Molnar, 2020).Incluso, permite identificar que, mientras la frontera estadounidense enfatiza la prevención y control físico-virtual, la turca opera estratégicamente en la mediación política y la gestión masiva de personas migrantes afectado otros aspectos de la movilidad humana (Veáse Cuadro 1. Variables de comparación entre casos de frontera digital).

Cuadro 1. Variables de comparación entre casos de frontera digital

Variable	EUA-México	Europa-Turquía-Asia
Modelo de control	Muro virtual + biometría + IA	Externalización + biometría + preautorizaciones
Actores clave	CBP, DHS, Palantir, Anduril	Frontex, Estados miembros, Turquía, Thales
Marco normativo	Seguridad Nacional (Patriot Act)	GDPR + Acuerdo con Turquía 2016
Tecnologías clave	Torres de vigilancia, drones, IA predictiva	Eurosur, Eurodac, ETIAS
Enfoque en derechos	Bajo, centrado en seguridad	Críticas por externalización y limitación de asilo

Fuente: Elaboración propia, 2025. En este cuadro se puede observar como en la frontera Estados Unidos-México, empresas como Anduril Industries y Palantir Technologies diseñan y operan sistemas de inteligencia artificial para la detección de cruces no autorizados, mientras que en Europa empresas como Thales y Airbus Defence proporcionan plataformas de monitoreo remoto. Esta privatización plantea desafíos en términos de transparencia, rendición de cuentas y control democrático, ya que las decisiones sobre seguridad fronteriza se encuentran parcialmente delegadas a actores no estatales

No obstante, un rasgo común en los dos casos es la creciente participación de empresas privadas en la provisión de tecnologías y servicios de vigilancia fronteriza, fenómeno que implica la mercantilización de la soberanía y la seguridad (Benítez Manaut, 2021). En Estados Unidos, empresas como Anduril y Palantir no solo suministran tecnología, sino que influyen en la definición de políticas y en el diseño de algoritmos que determinan quién representa un riesgo (Privacy International, 2024). Este proceso genera tensiones entre intereses económicos y derechos humanos, con escasa transparencia y supervisión efectiva.

La UE presenta una red aún más compleja, pues las tecnologías se implementan a través de acuerdos multilaterales con países terceros, extendiendo la privatización y externalización de la seguridad a niveles internacionales (Lazaridis & Campani, 2017).

La biopolítica y la gubernamentalidad algorítmica en la frontera digital

Siguiendo a Foucault (2007), la frontera digital se configura como un espacio donde la biopolítica se materializa en prácticas de vigilancia y control poblacional, mediadas por tecnologías algorítmicas que segmentan y clasifican a las personas migrantes según categorías de riesgo. La gubernamentalidad algorítmica, que combina datos biométricos, inteligencia artificial y bases de datos masivas, opera en

estos espacios para optimizar la gestión migratoria, pero también reproduce desigualdades estructurales y exclusiones (Dijstelbloem & Meijer, 2021).

En Estados Unidos, la IA utilizada para predecir movimientos migratorios contribuye a una política de riesgo que estigmatiza principalmente a comunidades latinas y centroamericanas (Koubi, 2021). En Canadá, pese a mayores controles, los algoritmos pueden sesgar las decisiones, afectando a migrantes de países con menor representación en el sistema de evaluación (Molnar & Gill, 2018). La UE, al operar con datos compartidos y externalizados, enfrenta dificultades para garantizar el cumplimiento de derechos fundamentales, ya que la transferencia a terceros limita la supervisión y el acceso a recursos legales (European Council on Refugees, 2024).

Impactos en la movilidad y seguridad humana

El despliegue de tecnologías de frontera tiene consecuencias directas sobre la movilidad de las personas y su seguridad. En el contexto Estados Unidos–México, la vigilancia digital intensiva genera efectos diferenciados entre distintos grupos de migrantes. La priorización de rutas y zonas mediante algoritmos reproduce desigualdades estructurales, limitando el acceso de personas en condiciones más vulnerables y exacerbando la exposición a riesgos físicos y legales. Esta dinámica refleja un patrón de gubernamentalidad algorítmica, en el que los migrantes son clasificados, monitoreados y gestionados como objetos de control más que como sujetos de derechos (Foucault, 2007; Amoore, 2020).

Por su parte, la frontera Turquía–Asia presenta un impacto distinto: la gestión tecnológica permite la coordinación masiva de flujos migratorios y la implementación de políticas de contención que afectan la movilidad de forma indirecta. El uso de sistemas biométricos y plataformas de seguimiento facilita la toma de decisiones administrativas y la selección de beneficiarios de protección internacional, pero también introduce opacidad y riesgos para los derechos humanos, dado que los datos personales se manejan en gran medida sin mecanismos claros de supervisión (Kaya, 2021; UNHCR, 2022).

En ambos escenarios, los resultados evidencian que la tecnología no es neutral; actúa como mediadora de exclusión y control, generando efectos diferenciados según la nacionalidad, el estatus migratorio, el género y la edad de las personas migrantes. Por otra parte, un hallazgo central es la importancia de la cooperación internacional y de actores privados en la consolidación de las fronteras digitales.

En el caso estadounidense, empresas de seguridad tecnológica colaboran estrechamente con agencias gubernamentales, desarrollando sistemas que optimizan la vigilancia y predicción de flujos migratorios (Chishti & Hipsman, 2021). Turquía, en cambio, participa en acuerdos de cooperación con la Unión Europea, recibiendo asistencia técnica y financiera para gestionar la migración hacia el continente, integrando plataformas digitales y protocolos de monitoreo que permiten compartir información entre países y agencias (Kaya, 2021).

Esta cooperación transnacional evidencia que la frontera digital no es un fenómeno exclusivamente nacional, sino un paradigma global de control migratorio. Al mismo tiempo, reproduce asimetrías de poder y dependencia tecnológica, en las cuales los países receptores o actores privados ejercen influencia sobre los estados fronterizos en términos de implementación tecnológica y estrategias de securitización.

En sintesis, los resultados permiten sustentar que estamos frente a un modelo global de frontera digital, caracterizado por la integración de tecnología avanzada, cooperación internacional y prácticas de vigilancia biométrica. Tanto Estados Unidos como Turquía aplican sistemas que convierten a los migrantes en sujetos de predicción, clasificación y control, lo que refleja la consolidación de la gubernamentalidad algorítmica y la extensión de la biopolítica al ámbito digital (Foucault, 2007; Lyon, 2018). Este paradigma combina tres elementos centrales: 1) la vigilancia masiva mediante tecnologías digitales; 2) la cooperación transnacional y el rol de actores privados; y 3) la opacidad en torno al uso de datos y algoritmos de predicción. Juntos, configuran fronteras que no solo delimitan territorios, sino que modulan la vida, la movilidad y la seguridad de los migrantes, transformando los desplazamientos en procesos gestionados, monitoreados y, en muchos casos, restringidos.

En cuanto al tema de la Ética, derechos humanos y transparencia, la a discusión ética emerge como un eje central. En Estados Unidos, la discriminación algorítmica se traduce en perfiles de riesgo que afectan a grupos específicos, mientras que en Turquía la opacidad administrativa limita la rendición de cuentas frente a decisiones que condicionan la movilidad y el acceso a protección internacional. Ambos casos serán analizandos mas a fondo a continuación .

Implicaciones para los derechos humanos y la soberanía digital

Los dos modelos evidencian tensiones significativas entre la soberanía estatal en el control fronterizo y la protección de derechos humanos, particularmente el derecho al asilo, la privacidad y la no discriminación (United Nations, 2022). La digitalización y automatización de fronteras, si bien incrementan la eficiencia, también generan nuevas formas de exclusión y violencia estructural, que requieren un enfoque crítico basado en el respeto a estándares internacionales.

El modelo estadounidense destaca por su falta de regulación integral en protección de datos, lo que amplifica los riesgos de violaciones y abusos (Privacy International, 2024). La UE, con un marco fuerte, pero externalización creciente, debe atender las brechas que esta dinámica genera en países terceros (Amnesty International, 2023).

La soberanía digital, entendida como la capacidad del Estado para gestionar la tecnología y los datos en beneficio de su población y en respeto a derechos fundamentales, es un concepto en tensión en los tres casos, debido a la influencia creciente de actores privados y la complejidad de redes transnacionales (Amoore, 2020).

Desafíos y oportunidades para una gobernanza justa de las fronteras digitales

Frente a estos desafíos, es imprescindible promover marcos regulatorios robustos que integren mecanismos de supervisión independiente, auditoría ética de algoritmos y participación ciudadana en la definición de políticas tecnológicas (Booth, Colomb & Williams, 2021). La cooperación internacional debe orientarse no solo a compartir tecnologías, sino también a garantizar estándares comunes de derechos humanos y transparencia (Guild, 2021).

Asimismo, la investigación debe profundizar en la experiencia de las personas migrantes, para comprender el impacto real de estas tecnologías y diseñar respuestas que prioricen la dignidad y la justicia social (Molnar, 2020). La soberanía digital debe redefinirse en clave de democracia tecnológica y soberanía popular, para evitar que la frontera digital se transforme en un espacio de exclusión y control desproporcionado.

Estos hallazgos sugieren múltiples líneas de investigación futura: Análisis crítico de algoritmos de predicción y clasificación migratoria o estudios sobre la interacción entre políticas nacionales, actores privados y organismos internacionales en la gobernanza digital de fronteras.

En síntesis, la investigación demuestra que las fronteras digitales son más que líneas territoriales: constituyen dispositivos complejos de vigilancia, control y poder, que articulan tecnología, política y derechos humanos en un escenario globalizado, marcado por tensiones éticas, desigualdades estructurales y desafíos de gobernanza transnacional. Esta configuración plantea nuevas preguntas sobre *soberanía tecnológica*, entendido como la capacidad de un Estado para mantener control sobre las infraestructuras digitales, los flujos de datos y los algoritmos que sustentan la vigilancia fronteriza (Hofmann, Katzenbach & Gollatz, 2017). Sin embargo, en la práctica, gran parte de la tecnología utilizada en fronteras es provista por empresas privadas con intereses comerciales, lo que genera dependencias y posibles vulnerabilidades estratégicas. Además, la opacidad de los sistemas algorítmicos dificulta la rendición de cuentas: ni los migrantes ni la ciudadanía en general tienen acceso a los criterios de decisión, lo que genera una brecha entre el ejercicio del poder y los mecanismos de control democrático (Molnar, 2020).

CONCLUSIONES

La frontera digital se ha consolidado como un espacio central para el ejercicio contemporáneo de la soberanía estatal y la gestión migratoria, mediado por tecnologías avanzadas de vigilancia, inteligencia artificial y bases de datos biométricos. Este estudio comparativo de los casos Estados Unidos–México, y Europa–Turquía–Asia revela que, aunque existen diferencias significativas en enfoques, inversiones y marcos legales, en todos predomina una tendencia hacia la privatización y tecnificación del control fronterizo, que genera profundos retos éticos, legales y sociales.

En Estados Unidos, la securitización está marcada por un despliegue masivo de tecnologías autónomas y un modelo militarizado donde empresas privadas como Anduril y Palantir desempeñan un papel clave, sin una regulación integral de protección de datos, lo que expone a migrantes a riesgos elevados de vigilancia invasiva y violaciones de derechos humanos (Rosenblum, 2021; Privacy International, 2024).

La Unión Europea y su política de externalización a países terceros como Turquía amplía el espectro del control fronterizo a redes transnacionales, donde la combinación de tecnología avanzada y acuerdos geopolíticos complejos genera un escenario de responsabilidad difusa y opacidad, con cuestionamientos crecientes desde los ámbitos de derechos humanos (Guild, 2021; Amnesty International, 2023).

Estos modelos ponen en evidencia las tensiones entre la soberanía digital y la protección de derechos fundamentales, especialmente en un contexto globalizado donde la movilidad humana desafía las fronteras tradicionales y las capacidades estatales de control (Amoore, 2020). La creciente privatización de tecnologías críticas y la opacidad en el diseño y uso de algoritmos demandan una urgente implementación de marcos regulatorios más democráticos, inclusivos y transparentes, que aseguren el respeto a la dignidad humana y la justicia social en la gobernanza fronteriza.

Finalmente, la frontera digital debe ser entendida no solo como un espacio tecnológico o securitario, sino como un ámbito donde se configuran relaciones de poder, control y resistencia, que requieren un abordaje interdisciplinario y una reflexión crítica permanente para evitar que la innovación tecnológica sirva únicamente a lógicas de exclusión y violencia estructural.

REFERENCIAS BIBLIOGRAFICAS

Amoore, L. (2020). Cloud ethics: Algorithms and the attributes of ourselves and others. Duke University Press.

Andreas, P. (2009). Border games: Policing the U.S.-Mexico divide. Cornell University Press.

Amnesty International (2023). EU: Migration Pact agreement will lead to a surge in suffering.

Anduril Industries. (2024). Anduril deploys 300th Autonomous Surveillance Tower (AST), advancing capability for border security. https://www.anduril.com/article/anduril-deploys-300th-autonomous-surveillance-tower-ast-advancing-capability-for-border-security/

Benítez Manaut, R. (2021). La militarización de la frontera sur de México: Implicaciones para la seguridad y los derechos humanos. Revista Mexicana de Política Exterior, 129, 29–50.

Bigo, D. (2002). Security and immigration: Toward a critique of the governmentality of unease. Alternatives, 27(Supplement), 63–92.

Buzan, B., Wæver, O., & De Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.

Booth, R., Colomb, G., & Williams, J. (2021). The craft of research (4th ed.). University of Chicago Press.

CBP. (2023). U.S. Customs and Border Protection: Annual report 2022. U.S. Department of Homeland Security.

Chishti, M., & Hipsman, F. (2021). The U.S.-Mexico border: A history of policy and politics. Migration Policy Institute.

De Genova, N. (2017). The borders of Europe. Duke University Press.

Dijstelbloem, H., & Meijer, A. (Eds.). (2021). Borders as infrastructure: The technopolitics of border control.

DHS. (2023). Biometric Entry-Exit Program: Annual report to Congress 2022. U.S. Department of Homeland Security.

European Commission. (2021). EUROSUR: European Border Surveillance System. European Union.

European Commission. (2023). ETIAS: European Travel Information and Authorization System. European Union.

European Council on Refugees. (2024). Digital borders and the right to asylum: A critical analysis. European Council on Refugees and Exiles.

Electronic Frontier Foundation. (2025). U.S. Border-Homeland Security Technology Vendors Dataset.

Foucault, M. (2007). Seguridad, territorio, población: Curso en el Collège de France (1977–1978). Fondo de Cultura Económica.

Frontex. (2023). Frontex Annual Activity Report 2022. European Border and Coast Guard Agency.

GAO. (2021). DHS: Actions needed to address risks in biometric entry-exit program. U.S. Government Accountability Office.

Guild, E. (2021). Schengen Borders and Multiple National States of Emergency. European Journal of Migration and Law, 23(4), 385–406.

HAVELSAN. (2022). HAVELSAN and EU cooperation on border surveillance technologies.

Hofmann, J., Katzenbach, C., & Gollatz, K. (2017). Data sovereignty: A concept and its implementation in the digital age. Springer.

Kaslı, N., & Parla, A. (2019). Turkey and the European Union: Externalizing borders and the politics of migration. Migration Studies, 7(3), 345–363.

Kaya, C. (2021). Surveil, datafy, publicize: Digital authoritarianism and migration governance in Turkey.

Koubi, V. (2021). Algorithmic governance and border control: Ethical implications. Journal of Borderlands Studies, 36(2), 203–220.

Lazaridis, G., & Campani, G. (2017). The EU-Turkey deal: Implications for migration and border security. European Journal of Migration and Law, 19(3), 267–285.

Lockheed Martin. (2025). Lockheed Martin: Border security solutions. Lockheed Martin Corporation.

Lyon, D. (2018). The culture of surveillance: Watching as a way of life (2nd ed.). Polity Press.

Mezzadra, S., & Neilson, B. (2013). Border as method, or, the multiplication of labor. Duke University Press.

Miller, T. (2019). How Border Patrol occupied the Tohono O'odham Nation. In These Times. Recuperado de Transnational Institute.

Molnar, P. (2020). Transnational governance and the digital border: A critical perspective. Global Policy, 11(4), 482–493.

Molnar, P., & Gill, L. (2018). The borders of algorithmic control: Risk and migration management in Canada. Surveillance & Society, 16(4), 451–469.

Nevins, J. (2010). Operation Gatekeeper and beyond: The war on illegal immigration in border communities. Routledge.

Privacy International. (2024). Privacy implications of biometric border control systems.

Ragin, C. C. (2014). The comparative method: Moving beyond qualitative and quantitative strategies. University of California Press.

Rosenblum, M. R. (2021). The U.S.-Mexico border: A comprehensive analysis of security and migration policies. Migration Policy Institute.

Rouvroy, A., & Berns, T. (2013). Gubernamentalidad algorítmica y perspectivas de emancipación: ¿La disparidad como condición de individuación a través de la relación? Réseaux, 177, 163–196.

Surveillance Watch (2025). Border surveillance technologies market overview. Recuperado de https://www.datainsightsmarket.com/reports/border-surveillance-1396401

Tech Inquiry. (2025). The digital border: A report on U.S. border surveillance technologies.

United Nations. (2022). Report of the Committee on the Elimination of Racial Discrimination: Consideration of reports submitted by States parties under article 9 of the Convention. United Nations.

UNHCR. (2022). Global report 2022. Recuperado de https://www.unhcr.org/sites/default/files/2023-07/2305336E_UNHCR-AR-2022_web_V3.pdf