



**National Security Technologies on the US-Mexico Digital
Border: Tijuana, Case Study.**

**Tecnologías de Seguridad Nacional en la Frontera Digital
EUA-México: Tijuana, Estudio de Caso.**

Para citar este trabajo:

Blandón Salinas, M. de los A. . (2025). Tecnologías de Seguridad Nacional en la Frontera Digital EUA-México: Tijuana, Estudio de Caso. *Multidisciplinary Journal of Sciences, Discoveries, and Society*, 2(4), 1-15.
https://estrellaediciones.com/index.php/sciences_discoveries_and_society/article/view/295

Autores:

María de los Angeles Blandón Salinas¹

Centro de Investigaciones sobre América del Norte (CISAN-UNAM).

Ciudad de México-México.

angeles2013@gmail.com

<https://orcid.org/0000-0002-7578-4650>

Autor de Correspondencia: María de los Angeles Blandón Salinas, angeles2013@gmail.com

RECIBIDO: 29-Junio-2025

ACEPTADO: 13-Julio-2025

PUBLICADO: 27-Julio-2025

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.



Resumen

El artículo examina la incorporación de tecnologías de seguridad nacional en la frontera digital entre Estados Unidos y México, tomando como caso de análisis la ciudad de Tijuana. Se analiza el crecimiento del denominado “muro virtual”, compuesto por datos biométricos, drones, sensores, cámaras de alta resolución y globos aerostáticos, orientados al control migratorio y la protección de la seguridad nacional. El objetivo principal consiste en analizar la contribución de estas tecnologías a los procesos de securitización fronteriza y sus repercusiones en el ámbito local, con particular énfasis en la interacción entre instancias gubernamentales, corporaciones privadas y comunidades afectadas. La metodología empleada integra la revisión de literatura académica, el análisis de fuentes oficiales y bases de datos gubernamentales, así como entrevistas semiestructuradas desarrolladas durante el trabajo de campo en Tijuana. Los hallazgos señalan que la frontera digital reproduce desigualdades sociales, refuerza dinámicas de exclusión y plantea retos significativos en materia de derechos humanos de personas migrantes. Asimismo, se observa la consolidación de un complejo industrial de seguridad y vigilancia que redefine los conceptos de soberanía y espacio fronterizo en el siglo XXI. En conclusión, el estudio identifica a Tijuana como un espacio experimental de securitización tecnológica que transforman de manera sustantiva tanto el control territorial como las relaciones socioeconómicas y políticas de la zona fronteriza EUA y México.

Palabras clave: frontera digital; Tijuana; seguridad nacional; derechos humanos; migración.

Abstract

This article examines the incorporation of national security technologies at the digital border between the United States and Mexico, using the city of Tijuana as a case study. It analyzes the growth of the so-called "virtual wall," composed of biometric data, drones, sensors, high-resolution cameras, and hot-air balloons, aimed at immigration control and the protection of national security. The main objective is to analyze the contribution of these technologies to border securitization processes and their impact at the local level, with particular emphasis on the interaction between government agencies, private corporations, and affected communities. The methodology used integrates a review of academic literature, an analysis of official sources and government databases, as well as semi-structured interviews conducted during fieldwork in Tijuana. The findings indicate that the digital border reproduces social inequalities, reinforces dynamics of exclusion, and poses significant challenges to the human rights of migrants. It also observes the consolidation of a security and surveillance industrial complex that redefines the concepts of sovereignty and border space in the 21st century. In conclusion, the study identifies Tijuana as an experimental space for technological securitization that substantially transforms both territorial control and the socioeconomic and political relations in the US-Mexico border region.

Keywords: digital border; Tijuana; national security; human rights; migration.

1. Introducción

En las dos últimas décadas, la frontera entre Estados Unidos y México ha experimentado un proceso acelerado de digitalización. Esta transformación se refleja en el despliegue de tecnologías de vigilancia y control conocidas colectivamente como “muro virtual”, que incluyen sensores terrestres, cámaras automatizadas, drones, globos aerostáticos, datos biométricos e inteligencia artificial (Ghaffary, 2020; Electronic Frontier Foundation, 2023). A diferencia del muro físico, esta arquitectura digital extiende la vigilancia hacia entornos remotos, el espacio aéreo y el



ámbito informático, incrementando la capacidad de control del territorio y de las personas que lo transitan.

Tijuana, por su ubicación estratégica y su papel como uno de los principales puntos de cruce fronterizo, constituye un espacio de experimentación clave para estas tecnologías. En esta ciudad convergen dispositivos de última generación destinados a la gestión migratoria, la seguridad nacional y el control territorial. Sin embargo, el debate académico sobre sus impactos sociales, políticos y éticos sigue siendo limitado, con un énfasis predominante en el análisis técnico de la infraestructura o en sus implicaciones legales (Heyman, 2008; Boyce et al., 2019). Son escasos los estudios que integran una perspectiva situada que considere las experiencias de comunidades locales, migrantes y otros actores afectados directamente por esta transformación.

La importancia de abordar este fenómeno radica en que la digitalización fronteriza no solo busca reforzar el control migratorio, sino que también genera efectos colaterales sobre la movilidad, los derechos fundamentales y la configuración del espacio social. La securitización tecnológica en Tijuana se inserta en una tendencia global de expansión del complejo industrial de seguridad y vigilancia, que involucra a gobiernos, corporaciones privadas y desarrolladores tecnológicos (Amoore, 2020; Feldman, 2021). Este proceso plantea tensiones significativas entre eficiencia operativa, privacidad, derechos humanos y soberanía. Al analizar cómo estas dinámicas se materializan en Tijuana, este estudio contribuye a un campo de investigación aún en desarrollo, que examina las fronteras no solo como líneas geográficas, sino como espacios tecnológicos, políticos y sociales.

Desde un punto de vista teórico, el análisis se fundamenta en la perspectiva de la securitización (Buzan, et al., 1998) y en los conceptos foucaultianos de biopolítica y gubernamentalidad (Foucault, 2008), los cuales permiten comprender la frontera como un dispositivo de poder orientado a la gestión de poblaciones y a la regulación de flujos migratorios. A ello se suma la noción de gubernamentalidad algorítmica (Rouvroy & Berns, 2013), útil para examinar cómo la integración de inteligencia artificial y procedimientos predictivos genera nuevas formas de clasificación, discriminación y control social.

El contexto de Tijuana resulta particularmente relevante debido a su condición de nodo estratégico del corredor migratorio y comercial del noroeste de México. Se trata de un espacio urbano caracterizado por una alta movilidad de personas migrantes, solicitantes de asilo, residentes transfronterizos y población deportada, lo que lo convierte en un escenario privilegiado para observar las implicaciones sociales de la frontera digital (Murià & Chávez, 2021; Correa-Cabrera, 2023). En este entorno, el “laboratorio tecnológico de Tijuana” no solo redefine las formas de control territorial, sino que también transforma las relaciones sociales, económicas y políticas.

Por lo tanto, partiendo de la premisa de que el despliegue de tecnologías de seguridad en la frontera digital reproduce desigualdades estructurales y genera nuevas formas de exclusión social, esta investigación busca analizar de manera integral la relación entre tecnología, poder y seguridad en el contexto fronterizo de Tijuana. El objetivo general es examinar el papel de estas tecnologías en los procesos de securitización y sus impactos locales, con especial énfasis en las comunidades migrantes y residentes. Entre los objetivos específicos se encuentran: identificar los actores privados involucrados en el diseño y la operación de estas tecnologías; analizar sus efectos sociales y políticos en la movilidad y la vida cotidiana de la población; y evaluar los discursos oficiales que justifican su adopción frente a las percepciones y experiencias de quienes viven sus consecuencias.



En suma, este estudio se sitúa en la intersección entre estudios fronterizos, tecnologías emergentes y derechos humanos, y busca aportar evidencia empírica y análisis teórico a un debate cada vez más urgente: el de las implicaciones de la digitalización fronteriza en un mundo donde la seguridad y el control de la movilidad están cada vez más mediados por algoritmos, datos y artefactos tecnológicos.

Aportes teóricos sobre las tecnologías de Seguridad Nacional en la Frontera Digital

1. Securitización y frontera digital

La noción de securitización, desarrollada principalmente por Buzan, Wæver y de Wilde (1998), constituye un marco analítico útil para comprender la transformación de la frontera México-Estados Unidos en un espacio altamente tecnologizado. Según la Escuela de Copenhague, un tema se securitiza cuando es presentado como una amenaza existencial que justifica la adopción de medidas extraordinarias, incluso fuera de la lógica política habitual. En el contexto fronterizo, la migración ha sido históricamente construida como un problema de seguridad nacional, especialmente desde el 11 de septiembre de 2001, lo que habilitó la expansión de infraestructuras de vigilancia, control y militarización de la frontera (Nevins, 2010; Walters, 2011).

En este marco, la frontera digital puede interpretarse como una extensión de la securitización clásica, pero con características novedosas: no se trata únicamente de un espacio físico reforzado con muros y personal de seguridad, sino de una arquitectura de control que opera mediante redes de sensores, drones, algoritmos de reconocimiento facial y análisis predictivo. Mezzadra y Neilson (2013) sostienen que las fronteras contemporáneas son “zonas de fricción” que no delimitan únicamente territorios, sino que regulan la movilidad de cuerpos, información y capital. En ese sentido, la frontera digital encarna un mecanismo de gestión diferenciado de flujos humanos, donde los datos biométricos y la inteligencia artificial desempeñan un papel central en la definición de quién puede moverse, bajo qué condiciones y con qué derechos.

Este proceso de securitización tecnológica tiene dos efectos principales: por un lado, amplía la capacidad del Estado de vigilar y clasificar a personas consideradas “riesgosas”; por otro, genera un espacio de excepción donde se suspenden garantías de privacidad y derechos humanos bajo el argumento de la seguridad (Walters, 2011). Así, el estudio de la frontera digital requiere analizar cómo estas tecnologías redefinen la noción de frontera, no solo como línea geográfica, sino como un conjunto distribuido de prácticas de control que trascienden el espacio físico y se extienden hacia el ciberespacio y la infraestructura de datos.

2. Derecho, algoritmo y seguridad nacional

La incorporación de tecnologías algorítmicas en la gestión de fronteras plantea tensiones significativas entre seguridad nacional, derechos fundamentales y gobernanza de datos. Foucault (2008) ya había anticipado que el poder moderno opera no solo mediante el control físico de los cuerpos, sino también mediante la regulación de los flujos y la normalización de conductas. En la actualidad, esa lógica se ve amplificada por algoritmos capaces de procesar grandes volúmenes de información para clasificar individuos, predecir comportamientos y tomar decisiones automatizadas con impacto directo sobre la movilidad humana (Rouvroy & Berns, 2013).

El uso de algoritmos en la frontera responde a una narrativa legal que enmarca la vigilancia digital como un mecanismo legítimo de protección frente a amenazas a la seguridad nacional. Sin embargo, este marco jurídico suele otorgar amplias facultades al Estado para recolectar, almacenar y analizar datos biométricos sin mecanismos de control efectivos ni garantías plenas de consentimiento (Amoore, 2020). De hecho, se observa una tendencia hacia la creación de

“zonas de excepción algorítmica”. Estas zonas pueden entenderse como espacios en los que el despliegue de tecnologías de vigilancia y control –como cámaras de reconocimiento facial, autónomas y análisis predictivo– se legitima bajo el argumento de la urgencia de seguridad, la protección fronteriza o la gestión de riesgos extremos. En estos espacios, el uso de datos biométricos, inteligencia artificial y de monitoreo masivo se implementa con estándares reducidos de transparencia y rendición de cuentas, creando un régimen en el que los derechos fundamentales quedan subordinados a la lógica de la seguridad (Zuboff, 2019).

En el caso de Tijuana, esta lógica se expresa en la creciente integración de cámaras de reconocimiento facial, predictivas y análisis de big data, cuyo funcionamiento se encuentra protegido por regímenes jurídicos de excepción orientados a la seguridad. Un ejemplo de estos dispositivos son las cámaras Buckeye, utilizadas para la vigilancia remota en zonas de difícil acceso, camufladas en el entorno natural y diseñadas para operar de manera autónoma, capturando imágenes y transmitiendo datos en tiempo real a centros de control (Electronic Frontier Foundation, 2023) (véase **Figura 1. Cámara de vigilancia tipo Buckeye**).

Figura 1. Cámara de vigilancia tipo Buckeye.



Características de la Tecnología

- Agencia: Aduanas y Protección de Fronteras, Servicio de Inmigración y Control de Aduanas, varios sheriffs de Arizona.
- Capacidades: Cámaras activadas por movimiento, transmisión en tiempo real.
- Proveedor: Buckeye.
- Ubicaciones: A lo largo de la frontera EUA-caso Tijuana-México.

Fuente: Electronic Frontier Foundation, 2023. Las Buckeye Cameras se diseñaron originalmente para captar la vida salvaje, pero se han reconvertido para la vigilancia de fronteras, las cuales almacenan los datos durante 15 años, y ahora se comercializan directamente en ese sector.

Este tipo de artefacto tecnológico ha planteado interrogantes sobre el derecho a la privacidad, el uso ético de la inteligencia artificial y la protección de datos personales, cuestiones que hoy se discuten intensamente en foros internacionales (United Nations, 2021). Desde el marco conceptual de “derecho, algoritmo y seguridad nacional” permite problematizar a la frontera digital no solo como un espacio de control físico, sino como una infraestructura tecnológica que redefine la relación entre seguridad y tecnología por cuanto traslada las prácticas de excesivo control fronterizo al ámbito de los datos, y plantea dilemas sobre el alcance de los derechos humanos, la privacidad y la autonomía de las personas frente a procedimientos automatizados.



3. Complejo industrial de seguridad

El concepto de “complejo industrial de seguridad” resulta clave para comprender el papel de los actores corporativos en la frontera digital. Inspirado en la noción del complejo militar-industrial, este término describe la interacción entre el sector privado, las agencias gubernamentales y los intereses políticos que promueven la adopción de tecnologías de vigilancia y control (Feldman, 2021). Según Amoores (2020), la securitización contemporánea depende en gran medida de infraestructuras tecnológicas desarrolladas y gestionadas por empresas privadas, cuyas innovaciones responden tanto a necesidades gubernamentales como a lógicas de mercado.

En la frontera México-Estados Unidos, esta dinámica se observa en la creciente participación de empresas como Anduril Industries, Palantir Technologies o Elbit Systems, responsables de proveer soluciones que van desde sensores de movimiento hasta plataformas algorítmicas de análisis de riesgo migratorio. Este ecosistema empresarial no solo produce tecnologías, sino también marcos discursivos que legitiman su implementación, apelando a valores como la eficiencia, la seguridad y la innovación (Amoores, 2020).

El problema radica en que esta externalización de funciones críticas de vigilancia genera dependencias estructurales: el Estado delega competencias soberanas a corporaciones cuyo objetivo principal no es la protección de derechos, sino la generación de beneficios económicos. De este modo, la frontera digital se convierte en un laboratorio donde confluyen intereses tecnológicos, políticos y económicos que configuran un modelo de control híbrido, sustentado tanto por actores públicos como privados (Mezzadra & Neilson, 2013).

En este sentido, la frontera digital debe analizarse también desde el prisma de la data vigilancia, entendida como la recolección y el uso de información personal mediante dispositivos tecnológicos interconectados con fines de control social y securitización. Como señala Meneses Gutiérrez (2023), el estudio de la frontera desde esta perspectiva permite comprender cómo la vigilancia digital transforma no solo los dispositivos de control, sino también las relaciones de poder y la experiencia migratoria en puntos fronterizos como Tijuana.

Por su parte, al incorporar los conceptos anteriores —securitización, derecho y algoritmo, e incluso complejo industrial de seguridad— permite analizar más específicamente el caso de Tijuana, donde se observa con claridad la convergencia de estas dinámicas: un discurso político de amenaza, un marco jurídico que habilita la vigilancia digital y un ecosistema empresarial que opera como catalizador del proceso que influye directamente en la formulación de políticas públicas y en la propia definición de las prioridades en materia de control fronterizo.

2. Metodología

La investigación adoptó un enfoque cualitativo con el propósito de comprender, desde una perspectiva integral, la implementación y el impacto de las tecnologías de seguridad nacional en la frontera digital de Tijuana. Este enfoque resulta pertinente para analizar fenómenos complejos que involucran relaciones de poder, seguridad y percepciones sociales, donde la experiencia de los actores y el contexto local desempeñan un papel fundamental (Creswell & Poth, 2018).

El diseño de investigación se estructuró en tres etapas complementarias. En primer lugar, se realizó una revisión documental de fuentes académicas, informes gubernamentales y publicaciones relacionadas con el despliegue tecnológico en la frontera Estados Unidos-México. Este análisis permitió identificar los marcos normativos, las empresas involucradas y las tendencias globales en la digitalización fronteriza (Chacón & Davis, 2022; Electronic Frontier Foundation, 2023).



En segundo lugar, se llevó a cabo un análisis de datos secundarios provenientes de bases públicas de contratos gubernamentales, reportes de adquisiciones tecnológicas y registros de inversión pública en infraestructura de seguridad proporcionado por Electronic Frontier Foundation, 2023. Esta etapa facilitó la identificación de los actores corporativos y estatales participantes, así como la caracterización de las tecnologías desplegadas en el área de Tijuana.

La tercera etapa consistió en un trabajo de campo desarrollado entre julio y agosto de 2025, que incluyó la realización de 5 entrevistas semiestructuradas con funcionarios, académicos, migrantes y residentes de zonas cercanas a la infraestructura tecnológica. Las entrevistas se diseñaron para explorar percepciones, experiencias y posibles tensiones derivadas del uso de tecnologías de vigilancia, siguiendo protocolos éticos de consentimiento informado y confidencialidad.

Para el tratamiento y análisis de la información, se empleó el método de análisis temático, el cual permite identificar patrones y categorías significativas en los discursos y documentos revisados. En conjunto, la metodología implementada proporcionó un marco robusto para examinar el papel de la frontera digital en la securitización tecnológica de Tijuana, al integrar dimensiones normativas, técnicas y sociales, y al priorizar la voz de los actores locales frente a procesos de vigilancia de alcance global.

3. Resultados

Durante las observaciones realizadas, se pudo constatar una expansión significativa de la infraestructura tecnológica. La instalación de sensores terrestres, drones autónomos y globos aerostáticos equipados con cámaras de alta resolución, junto con procedimientos biométricos para la captura y procesamiento de datos faciales y de huellas digitales, forman un entramado interconectado que permite una vigilancia constante y en tiempo real. También, se evidencia una tendencia hacia la consolidación de una infraestructura tecnológica compleja y, en varios aspectos, experimental, caracterizada por la integración de múltiples sistemas de monitoreo y análisis de datos con fines de control fronterizo. Al mismo tiempo, dicha infraestructura tiene un impacto social diferenciado, generando percepciones ambivalentes entre las comunidades fronterizas, que oscilan entre la expectativa de mayor seguridad y la preocupación por la pérdida de privacidad y el incremento de la vigilancia.

Finalmente, este proceso revela la emergencia de un complejo industrial de seguridad con implicaciones regionales, donde actores privados y públicos articulan intereses económicos, políticos y tecnológicos que extienden la lógica de la securitización más allá del ámbito estrictamente fronterizo.

1. Consolidación de una infraestructura tecnológica compleja y experimental

La revisión de fuentes oficiales y académicas, así como el análisis de contratos públicos y registros de adquisiciones, mostró que el caso de estudio de Tijuana se ha consolidado como un nodo de experimentación tecnológica en el marco del denominado “muro virtual”. Las tecnologías implementadas incluyen cámaras de reconocimiento facial y biométrico en puntos de cruce, drones autónomos de vigilancia aérea, globos aerostáticos para monitoreo persistente y sensores de alta precisión para detección de movimiento en áreas de difícil acceso (véase **Figura 2. Globos aerostáticos, Tijuana**).

Figura 2. Globos aerostáticos Tijuana.



Características de la Tecnología

- Agencia: Aduanas y Protección de Fronteras.
- Capacidades: Radar.
- Contratistas: Altaeros Energies, QinetiQ, C Speed, etc.
- Número de sistemas: 8.

Fuente: Electronic Frontier Foundation, 2023. Estos globos se basan principalmente en el radar y se centran en aeronaves y vehículos terrestres que vuelan bajo. La oficina de Aduanas y Protección Fronteriza, (por siglas en inglés CBP) afirma que puede detectar un avión a 200 millas de distancia.

Asimismo, se identificó la integración de torres de vigilancia de análisis predictivo basadas en inteligencia artificial, diseñadas para anticipar flujos migratorios y detectar patrones considerados “anómalos” por las autoridades fronterizas (Electronic Frontier Foundation, 2023; Chacón & Davis, 2022).

Un funcionario (bajo condición de anonimato) afirmó: “La tecnología actual nos permite anticiparnos a los movimientos, identificar patrones y actuar preventivamente. Antes la frontera era física, ahora es digital y mucho más eficaz.” (Entrevista #1, autoridad local, Tijuana, 2025).

Este relato refuerza el hallazgo sobre la creciente confianza institucional en el uso de sistemas algorítmicos y predictivos, que sustituyen la noción tradicional de frontera física por una infraestructura virtual con capacidad de anticipación. Por otro lado, revela como ese despliegue tecnológico está acompañado por el uso de la inteligencia artificial que procesa grandes volúmenes de datos para clasificar perfiles de riesgo migratorio, utilizando algoritmos predictivos que asignan niveles de alerta a personas y grupos detectados. Sin embargo, la opacidad en los criterios de clasificación genera incertidumbre y cuestionamientos sobre posibles sesgos discriminatorios.

En consecuencia, la evidencia recopilada muestra que la lógica de operación de estas tecnologías excede el objetivo inicial de control migratorio, abarcando también la gestión de riesgos asociados al comercio transfronterizo y la vigilancia generalizada de espacios públicos en el perímetro urbano de Tijuana. Este carácter experimental se manifiesta en la participación de empresas tecnológicas de vanguardia, como Anduril Industries y Palantir Technologies, contratadas no solo para proveer hardware, sino también para operar y perfeccionar algoritmos de análisis de datos. En conjunto, estas dinámicas evidencian la consolidación de una infraestructura tecnológica compleja que trasciende el ámbito estrictamente fronterizo, generan un impacto social entre las comunidades locales.

2. Impacto social diferenciado y percepciones ambivalentes

Los datos recopilados también evidencian la reproducción de desigualdades y exclusiones mediante la frontera digital. Los algoritmos de reconocimiento facial al operar con bases de datos



parciales y a veces sesgadas, pueden resultar en perfiles discriminatorios basados en origen étnico, nacionalidad o estatus migratorio.

La percepción de las personas migrantes sobre el uso de tecnologías predictivas muestra un alto nivel de desconfianza, especialmente cuando estas prácticas derivan en clasificaciones erróneas que pueden tener consecuencias graves. Un migrante entrevistado bajo condición de anonimato señaló:

“Tengo conocidos que los regresaron a su país de origen porque fueron detectados por la tecnología como personas de riesgo de manera errónea, lo que derivó en detenciones injustificadas o negación de paso” (Entrevista #2, migrante, Tijuana, 2025).

Este testimonio ilustra la preocupación por los posibles errores de clasificación algorítmica y sus efectos directos en la vida de las personas, reforzando la exposición a prácticas discriminatorias y la adopción de rutas de cruce más peligrosas, elevando el riesgo de accidentes y abusos. Incluso, genera un escenario donde la frontera digital actúa como un filtro desigual, incrementando la vulnerabilidad de ciertos grupos y afectando su acceso a derechos fundamentales como el debido proceso y la protección contra tratos arbitrarios.

Para la población tijuana, la implementación de tecnologías es mixtas. Mientras algunos la perciben como una herramienta que incrementa la seguridad y promueve un entorno más controlado respecto a la reducción de delitos transfronterizos y al fortalecimiento de la vigilancia en áreas urbanas sensibles. Otros estacaron total desconocimiento y despreocupación. Y, por último, una vecina comentó: *“Desde que pusieron esos globos y cámaras, uno siente que siempre está siendo observado, como si ya no tuviéramos espacio para estar tranquilos.”* (Entrevista #3, residente de colonia fronteriza, Tijuana, 2025).

En conjunto, los resultados indican que la frontera digital en Tijuana no constituye únicamente una herramienta de control migratorio, sino un espacio experimental de desarrollo tecnológico con implicaciones sociales, políticas y económicas de amplio alcance. Por un lado, estas tecnologías han contribuido a mejorar la capacidad de monitoreo y respuesta de las autoridades, fortaleciendo la percepción de seguridad en algunos sectores de la población. Por otro, generan nuevas formas de exclusión y vigilancia masiva que afectan de manera diferenciada a grupos vulnerables, especialmente a personas migrantes.

Al respecto, estos hallazgos confirman la hipótesis planteada en la investigación: la expansión del “muro virtual” en Tijuana reproduce desigualdades sociales, genera dinámicas de control social más sofisticadas y refuerza la lógica de securitización tecnológica, con impactos que trascienden el ámbito local y se proyectan a escala regional.

3. Emergencia de un complejo industrial de seguridad con implicaciones regionales

Un tercer aspecto identificado por el estudio fue el entramado cada vez más estrecho de colaboración entre el sector público y las corporaciones privadas, lo que consolida lo que algunos autores han denominado un “complejo industrial de seguridad” (Amoore, 2020; Feldman, 2021). Esta dinámica se refleja en el papel protagónico que desempeñan las empresas privadas en el diseño e implementación de artefactos tecnológicos orientados al control y la vigilancia.

Las entrevistas coincidieron en destacar la centralidad de las empresas privadas en estos procesos. Como expresó José García, director del albergue Juventud 2000 en Tijuana, “estas empresas tienen como trabajo proveer soluciones integrales que respondan a las necesidades del cliente, en este caso agencias gubernamentales, sin importar la parte humana” (Entrevista #4, director Albergue Juventud 2000, Tijuana, 2025).



En ese sentido, esta dinámica ha generado una dependencia estructural, en la que el Estado delega funciones clave de seguridad a empresas privadas, lo que plantea desafíos en términos de soberanía y control democrático sobre la información recolectada. Las entrevistas con actores locales evidenciaron, además, que esta dependencia tecnológica tiene un impacto económico ambivalente: por un lado, crea oportunidades laborales vinculadas con la instalación y mantenimiento de infraestructura tecnológica; por otro, refuerza la dependencia de soluciones externas, muchas de ellas desarrolladas fuera del país y sin procesos claros de rendición de cuentas.

Además, el caso de Tijuana es una de las ciudades más transitadas del mundo, con más de 40 millones de cruces anuales por los puertos de San Ysidro y Otay Mesa. Esta condición la convierte en un laboratorio para tecnologías de control migratorio. Desde 2006, Tijuana concentra datos biométricos en estaciones migratorias y centros de procesamiento, donde tecnologías de captura facial y huellas son cotidianas. Sin embargo, se detecta la ausencia de mecanismos institucionales robustos para garantizar la transparencia en la gestión de los datos recolectados por estas tecnologías, particularmente en lo relacionado con el uso de algoritmos de reconocimiento facial y análisis predictivo. Este vacío normativo ha generado inquietud sobre el alcance de las capacidades de vigilancia y su posible expansión hacia otros ámbitos de la vida social más allá del control fronterizo.

Algunas de las tecnologías empleadas en la frontera Tijuana, han sido las torres inteligentes (Integrated Fixed Towers) con cámaras infrarrojas y radares que detectan movimientos hasta a 10 km de distancia, enviando alertas automáticas a centros de comando. Estas torres están equipadas con IA para diferenciar animales, humanos y vehículos, priorizando el envío de agentes.

En cuanto al uso de drones y vigilancia aérea, la frontera es patrullada por drones MQ-9 Predator B, equipados con sensores electro-ópticos y radares. Pueden volar durante 20 horas continuas, mapeando rutas migrantes y generando mapas de calor que indican “zonas calientes” de cruce.

Empresas como Palantir proveen bases de datos como IDENT y el FBI Next Generation Identification que analizan datos de redes sociales, transacciones bancarias y patrones de movilidad (véase Tabla 1. Tipo de Tecnologías implementadas en la frontera Tijuana).

Tabla 1. Tipo de Tecnologías implementadas en la frontera Tijuana

Tecnología	Cantidad estimada en Tijuana	Función principal	Empresa proveedora	Año de implementación
Lectores biométricos	100+	Identificación y verificación en garitas y estaciones migratorias	Palantir Technologies	2022
Drones MQ-9	12 vuelos mensuales	Vigilancia aérea	Anduril Industries	2023
Globos aerostáticos (aerostatos)	1	Monitoreo persistente	Elbit Systems	2021



Tecnología	Cantidad estimada en Tijuana	Función principal	Empresa proveedora	Año de implementación
Torres inteligentes (RVSS) y (AST)	35	Equipadas con radar e IA	General Dynamics	2024

Fuente: Elaboración propia, 2025. La Tabla 1 muestra el despliegue tecnológico en Tijuana y su dependencia de corporaciones con fuerte presencia internacional, lo que refuerza la idea hacia una economía de seguridad transfronteriza controlada por el sector privado.

En 2024, al intensificarse la vigilancia en Tijuana-San Diego, un estudio de Chambers y Boyce (2019) mostró que las torres de vigilancia estaban correlacionadas con un aumento del 30% en muertes en el desierto. El doctor Hugo Méndez Fierros, profesor de la Universidad Autónoma de Baja California sintetizó: *“Lo que sucede aquí anticipa modelos que probablemente se expandirán a otras fronteras y contextos. Es crucial estudiar esta experiencia para entender hacia dónde va la gobernanza digital de las fronteras.”* (Entrevista #5, académico, Tijuana, 2025).

4. Discusión

El análisis de la frontera digital de Tijuana muestra que la incorporación de tecnologías de vigilancia –drones, sensores de movimiento, globos aerostáticos, cámaras de reconocimiento facial e inteligencia artificial– no solo responde a una lógica de protección territorial, sino que forma parte de una transformación estructural en la manera en que los Estados gestionan la movilidad y el espacio social. Estas tecnologías, inicialmente diseñadas para optimizar procesos de control, terminan generando un régimen de vigilancia que afecta de manera directa a las comunidades locales, migrantes y residentes transfronterizos.

Este fenómeno no es reciente. Desde finales de la década de los ochenta, Clarke (1988) advirtió que la digitalización de la información y su utilización a futuro con fines de supervisión gubernamental y corporativa conformaría un régimen emergente de data vigilancia, orientado a la recolección, procesamiento y uso masivo de datos personales. En el caso de Tijuana, la infraestructura de frontera digital se materializa precisamente en este tipo de prácticas: bases de datos biométricos, de análisis predictivo y procedimientos algorítmicos de perfilamiento que, aunque actualizados tecnológicamente, responden a la misma lógica de control estructural identificada por Clarke.

La situación se complejiza cuando empresas privadas, como Anduril Industries o Palantir Technologies, participan activamente en la provisión de soluciones tecnológicas, lo que genera dependencias entre el Estado y el sector corporativo. En consecuencia, la frontera digital en el caso de estudio de Tijuana se inscribe en una lógica de control que responde tanto a imperativos estatales como a intereses corporativos, conforme al modelo del complejo industrial de seguridad descrito por Amoore (2020) y Feldman (2021).

Esta convergencia contribuye a la consolidación de un espacio fronterizo hipervigilado que, si bien mejora ciertas capacidades operativas, plantea importantes desafíos para los derechos humanos y las dinámicas sociales locales. Además, la noción de data vigilancia resulta fundamental para entender cómo estas prácticas no solo transforman los dispositivos de control, sino también las relaciones de poder y la experiencia migratoria. Al mismo tiempo, plantea un desafío democrático al operar bajo regímenes jurídicos de excepción que suelen reducir los estándares de transparencia y rendición de cuentas.



Por otra parte, desde la teoría de la securitización (Buzan et al., 1998) muestra cómo la frontera digital es una extensión tecnológica de la construcción discursiva de la migración como amenaza. Esta securitización habilita la justificación política y legal para la adopción de tecnologías que en la práctica generan condiciones de excepción, donde los derechos y garantías fundamentales se ven restringidos en aras de la seguridad nacional. El concepto foucaultiano de biopolítica y gubernamentalidad algorítmica (Foucault, 2008; Rouvroy & Berns, 2013) es útil para entender cómo estas tecnologías no solo controlan movimientos físicos, sino que normativizan y administran la vida misma a través del procesamiento masivo de datos biométricos y conductuales.

No obstante, la incorporación de algoritmos en procesos de vigilancia y control no es neutra ni exenta de riesgos. Como se observó en el trabajo de campo, las tecnologías algorítmicas reproducen sesgos y desigualdades, afectando desproporcionadamente a personas migrantes. Esto es consistente con los argumentos de Zuboff (2019) y Amoore (2020), quienes advierten sobre la “capitalización de la vigilancia” y la creación de “zonas de excepción algorítmica” que erosionan derechos fundamentales.

Además, plantea interrogantes sobre la soberanía tecnológica y la rendición de cuentas. La dependencia del Estado hacia empresas externas puede limitar la transparencia y la supervisión pública, dificultando la evaluación de impactos y la protección efectiva de derechos. Esta situación subraya la necesidad de marcos regulatorios robustos que controlen la utilización de tecnologías de vigilancia y promuevan la responsabilidad social corporativa en el ámbito de la seguridad nacional.

Por otro lado, la experiencia de Tijuana revela cómo la frontera digital traslada la frontera tierra adentro, pues las personas pueden ser detectadas y clasificadas mucho antes de llegar al muro físico. Más bien, refuerza dinámicas coloniales, donde el Norte Global diseña e impone tecnologías de control sobre poblaciones del Sur Global, consolidando un mercado lucrativo que beneficia a corporaciones como Palantir, Anduril, Elbit Systems o General Dynamics, las cuales promueven la perpetuación de la crisis migratoria como oportunidad de negocio.

Por consiguiente, la novedad de este trabajo radica en el análisis situado de un espacio fronterizo concreto, que integra la perspectiva de actores locales con datos de carácter técnico y normativo, ofreciendo una visión holística del fenómeno. Un aspecto controversial identificado es la forma en que las tecnologías generan efectos no previstos: la vigilancia extendida induce a las personas migrantes a buscar rutas más peligrosas, lo que incrementa su vulnerabilidad y, en ocasiones, sus riesgos de muerte. Este hallazgo pone de relieve la paradoja entre los objetivos oficiales de una migración segura, ágil y controlada.

En términos de proyecciones futuras, el modelo de frontera digital implementado en Tijuana se perfila como una plantilla replicable en otros contextos geopolíticos, lo que refuerza la pertinencia de investigaciones críticas orientadas a comprender sus efectos sociales y políticos. Este estudio contribuye a la línea de investigación sobre tecnologías, fronteras y derechos humanos, ofreciendo insumos teóricos y empíricos útiles para debates sobre políticas públicas, regulación tecnológica y ética de la seguridad.

5. Conclusión

El presente trabajo realizado sobre la implementación de tecnologías de seguridad nacional en la frontera digital de Tijuana evidencia que la digitalización de los espacios fronterizos no constituye únicamente un reemplazo de las infraestructuras físicas tradicionales, sino una reconfiguración



integral de los mecanismos de control territorial y social. A partir de la integración de drones, datos biométricos, globos aerostáticos, sensores y torres inteligentes, la frontera se transforma en un laboratorio de innovación tecnológica donde se articulan intereses estatales y corporativos.

Uno de los hallazgos centrales se refiere a la consolidación de un complejo industrial de seguridad compuesto por empresas tecnológicas privadas y agencias gubernamentales, que generan una red de cooperación público-privada para la provisión, operación y mantenimiento de tecnologías de vigilancia. Este fenómeno plantea desafíos importantes en materia de tecnológica, transparencia en la gestión de datos y rendición de cuentas. La dependencia de soluciones tecnológicas desarrolladas y operadas por corporaciones externas puede limitar la capacidad del Estado para controlar plenamente el uso y destino de la información generada, así como los algoritmos que guían las decisiones sobre movilidad y control migratorio.

En el plano social, los resultados indican que la digitalización fronteriza produce impactos diferenciados y, en ocasiones, contradictorios. Por un lado, sectores de la población local perciben un incremento en la seguridad y un reforzamiento de la capacidad de respuesta institucional frente a riesgos reales o percibidos. Por otro lado, las personas migrantes, experimentan un aumento en la vigilancia cotidiana y en la sensación de exclusión social. Además, la presión ejercida por estos dispositivos induce a los migrantes a buscar rutas alternativas más riesgosas, lo que genera consecuencias humanitarias adversas, como el incremento de accidentes y la exposición a redes criminales.

Estos aspectos ponen de relieve una paradoja central: las tecnologías desplegadas en nombre de la seguridad y la protección generan, en la práctica, nuevas vulnerabilidades y reproducen desigualdades estructurales. La frontera digital no es un espacio neutral; está atravesada por relaciones de poder y lógicas económicas que priorizan la eficiencia técnica sobre los derechos humanos. Esta tensión es especialmente relevante en un contexto como el de Tijuana, donde convergen intereses geopolíticos, flujos migratorios complejos y dinámicas socioeconómicas asimétricas.

En términos teóricos, la investigación confirma que la frontera digital puede analizarse mediante los conceptos de securitización (Buzan et al., 1998), biopolítica y gubernamentalidad algorítmica (Foucault, 2008; Rouvroy & Berns, 2013), los cuales permiten comprender la transición hacia un modelo de control caracterizado por la centralidad de los datos y el uso de procedimientos o métodos predictivos. Este marco conceptual es clave para interpretar cómo las fronteras dejan de ser únicamente espacios físicos para convertirse en arquitecturas digitales.

En cuanto a la relevancia del estudio, sus resultados aportan evidencia empírica sobre un proceso en curso que, aunque intensamente discutido en el plano político, cuenta con escasos análisis situados desde la perspectiva de actores locales y comunidades afectadas. La combinación metodológica empleada —revisión documental, análisis de datos y trabajo de campo— permitió ofrecer una mirada integral que vincula el despliegue tecnológico con sus impactos sociales y políticos.

Al respecto, este estudio sugiere la necesidad de establecer mecanismos robustos de supervisión y transparencia en el uso de tecnologías de vigilancia, desarrollar marcos regulatorios que garanticen la protección de la privacidad y los derechos humanos, así como ampliar el análisis comparativo hacia otros puntos fronterizos donde se estén implementando tecnologías similares, a fin de identificar patrones y particularidades en diferentes contextos geográficos.

Finalmente, los hallazgos confirman la hipótesis central: la frontera digital de Tijuana funciona como un laboratorio de securitización tecnológica con implicaciones que afectan las dinámicas de movilidad humana, y los derechos fundamentales. Comprender este fenómeno resulta crucial en



un mundo donde la seguridad y el control de la movilidad están cada vez más mediados por algoritmos, datos masivos y artefactos digitales.

Referencias Bibliográficas

- Amoore, L. (2020). *Cloud ethics: Algorithms and the attributes of ourselves and others*. Duke University Press.
- Boyce, G., Launius, S., & Lobo, S. (2019). Border militarization and migrant deaths: Consequences of a virtual wall. *Journal of Borderlands Studies*, 34(2), 211–227. <https://doi.org/10.1080/08865655.2018.1480409>
- Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner.
- Braun, V., & Clarke, V. (2013). *Successful qualitative research: A practical guide for beginners*. SAGE.
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE.
- Correa-Cabrera, G. (2023). *Digital borders and security industry growth in the US-Mexico borderlands*. Routledge
- Clarke, R. 1988. Information technology and dataveillance. *Communications of the ACM* 31 (5): 498 – 512. <https://doi.org/10.1145/42411.42413>.
- Chacón, J. M., & Davis, M. (2022). The expansion of border surveillance technologies in North America. *Migration Studies*, 10(3), 457–475. <https://doi.org/10.1093/migration/mnab012>
- Chambers, S. N., & Boyce, G. A. (2019). Mortality, Surveillance and the tertiary “funnel effect” on the U.S.-Mexico border: A geospatial modeling of the geography of deterrence. *Journal on Migration and Human Security*, 7(1). <https://doi.org/10.1080/08865655.2019.1570861>
- Electronic Frontier Foundation. (2023). *Surveillance and the U.S.-Mexico Border: 2023 year in review*. <https://www.eff.org/deeplinks/2023/12/surveillance-and-us-mexico-border-2023-year-review>
- Feldman, I. (2021). Algorithmic governance and human mobility. *Journal of Border Security Studies*, 15(1), 33–52.
- Foucault, M. (2008). *Seguridad, territorio y población*. Fondo de Cultura Económica.
- Ghaffary, S. (2020, febrero 8). The “smarter” wall: How drones, sensors, and AI are patrolling the border. *Vox*. <https://www.vox.com/recode/2019/5/16/18511583/smart-border-wall-drones-sensors-ai>
- Heyman, J. (2008). Constructing a virtual wall: Race and citizenship in US-Mexico border policing. *Journal of Borderlands Studies*, 23(2), 1–18.
- Murià, M., & Chávez, S. (2021). Shopping and working in the borderlands: Enforcement, surveillance and marketing in Tijuana, Mexico. *Surveillance & Society*, 19(3), 332–346. <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/4169>
- Mezzadra, S., & Neilson, B. (2013). *Border as method, or, the multiplication of labor*. Duke University Press.
- Meneses Gutiérrez, M. M. (2023). *Researching the Mexico-US border: A tale of dataveillance*. *Journal of Global Ethics*, 19(3), 347–358. <https://doi.org/10.1080/17449626.2023.2271005>
- Nevins, J. (2010). *Operation Gatekeeper and beyond: The war on “illegals” and the remaking of the U.S.-Mexico boundary*. Routledge.



- Rouvroy, A., & Berns, T. (2013). Algorithmic governmentality and prospects of emancipation. *Réflexions sur la politique des algorithmes*, 1-28.
- United Nations. (2021). *The right to privacy in the digital age*. UN Human Rights Council Report A/HRC/48/31.
- Walters, W. (2011). Foucault and frontiers: Notes on the birth of the humanitarian border. *Governmentality Studies*, 3(1), 138-164.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

Conflicto de Intereses: Los autores declaran que no tienen conflictos de intereses relacionados con este estudio y que todos los procedimientos seguidos cumplen con los estándares éticos establecidos por la revista. Asimismo, confirman que este trabajo es inédito y no ha sido publicado, ni parcial ni totalmente, en ninguna otra publicación.