

# La frontera omnipresente

La infraestructura digital de control migratorio en las Américas



*Mizue Aizeki, Laura Bingham y Santiago Narv ez*

TRADUCCI N AL ESPA OL POR NURIA DEL VISO PAB N

ILUSTRACI N DE ZORAN SVILAR



En 2021, José Eusebio Asegurado, agricultor de El Salvador, fue detenido por la Policía Nacional Civil salvadoreña por «promover la trata de personas». La base de la detención fue un chat de grupo de WhatsApp que Asegurado y otros migrantes utilizaban para coordinar una caravana, en la que se había infiltrado un agente de policía. Según las capturas de pantalla utilizadas para incriminarle, la única participación de Asegurado en el chat fue responder “OK” al mensaje de un migrante que le decía que estaría en un punto de encuentro sobre las cinco. La policía detuvo a Asegurado en el punto de encuentro, diciéndole que estaba “fichado” como organizador de la caravana (Cáceres y Gressier, 2021).

El mismo día, la policía salvadoreña también acusó a Fátima Pérez, cocinera, y a Juan Rufino Ramírez, guardia de seguridad privada, de promover la “trata de personas” basándose en los mensajes de un grupo de WhatsApp que habían creado para coordinar una caravana. En las capturas de pantalla del caso de Ramírez se le ve dando instrucciones al grupo de 55 miembros para reunirse en la estación de autobuses, así como los precios de los billetes a Guatemala. La policía detuvo a Ramírez y a Pérez la mañana en que planeaban partir.

Estas tres detenciones se produjeron en un lapso de cuatro horas. La entonces embajadora de Estados Unidos en El Salvador, Katherine Dueholm, felicitó rápidamente a la Fiscalía General y declaró: “Aplaudo a las autoridades salvadoreñas que están tomando medidas contra aquellos que quieren engañar a la ciudadanía con caravanas y falsas promesas. Solo promueven #UnViajeEnVano” (Johnson, 2021).

Las detenciones y los elogios de la embajadora Dueholm reflejan el papel fundamental que desempeñan la vigilancia encubierta y las tecnologías *inteligentes* basadas en datos en las prácticas estadounidenses de control migratorio que operan en países situados fuera de Estados

Unidos. En los últimos veinte años, Estados Unidos (y otros países ricos) han hecho grandes esfuerzos por externalizar los regímenes de control de fronteras más allá de su propio territorio. Esto implica a menudo la participación efectiva de organismos de otros países en la vigilancia, el control policial y la exclusión de los inmigrantes.

Sin embargo, la nueva infraestructura digital que permite la externalización de las fronteras es poco conocida. Esta infraestructura digital se basa tanto en la tecnología de grado militar construida por los principales fabricantes de armas como en la innovación de Silicon Valley: bases de datos interoperables que comparten huellas dactilares sin problemas entre los organismos policiales a través de las fronteras; dispositivos de recogida biométrica utilizados por las autoridades de detención mexicanas para rastrear a los migrantes para la Oficina de Aduanas y Protección Fronteriza de Estados Unidos (CBP); aplicaciones de medios sociales que sirven como redes de comunicación críticas para los migrantes y herramientas de vigilancia para la policía; sistemas de identificación digital que permiten el acceso a los servicios esenciales, pero también como dispositivos de seguimiento.

Las infraestructuras –digitales o materiales– tienen un verdadero poder de adhesión; de eso se trata. Una vez que una autopista parte una comunidad por la mitad, una nueva permanencia sofoca el estruendo de las protestas y la gente sigue adelante. Utilizamos el término *infraestructura digital* para describir el establecimiento de una base que será fundamental para la forma en que las potencias mundiales practicarán el control de la migración; y, a medida que se implante, cada vez más allá del desafío: una intervención estratégica unificada de los países poderosos, con Estados Unidos en la vanguardia. Aunque pueda parecer un experimento tecnológico (como los perros-robot dotados de inteligencia artificial en la frontera) o una captura de datos puntual y oportunista (como las redes de acuerdos internacionales de intercambio de datos), el crecimiento de la infraestructura fronteriza digital es *por diseño*. Esto es posible gracias a las tecnologías digitales integradas que se asientan en el tipo de permanencia rígida y *sin motivo* que se concede a otras infraestructuras, como los cables

de comunicaciones submarinos, los protocolos y los servidores que hacen funcionar Internet, una red eléctrica o una superautopista (De Goede y Westermeier, 2022).

Las profundas implicaciones de las nuevas infraestructuras persisten mucho tiempo después de su creación, como es el caso de la infraestructura digital desplegada para vigilar a los inmigrantes en el llamado *patio trasero* de Estados Unidos. Con frecuencia, sus repercusiones resultan invisibles. Los gobiernos promueven las tecnologías de vigilancia fronteriza como fundamentalmente seguras, humanas y no violentas, mientras que los defensores de los inmigrantes luchan por hacer visible la violencia al otro lado de estos *circuitos fronterizos invisibles*.<sup>1</sup>

Las implicaciones van desde la violencia desencadenada digitalmente y los asesinatos cometidos por la policía local en Centroamérica hasta las acciones de Estados Unidos, sus aliados y competidores en las contiendas geopolíticas por el control de la seguridad mundial. El gobierno estadounidense y la industria privada se han embarcado en un frenesí empresarial, en gran medida encubierto, para poseer y controlar la interfaz de vigilancia de la migración del futuro. Las capacidades de vigilancia y control –una parte rutinaria y de larga data de los paquetes de ayuda de Estados Unidos para luchar contra el crimen organizado– amplían el espionaje interno de los gobiernos socios para sus propios fines y sirven a los intereses de externalización fronteriza de Estados Unidos en el control del movimiento de personas y su desvío fuera de la frontera territorial estadounidense.

Este ensayo se centra principalmente en cómo la infraestructura digital sirve a los intereses estadounidenses. ¿Qué sabemos sobre esta estrategia y cómo está afectando ya a la movilidad y los derechos humanos en la región? ¿cuáles son sus fundamentos históricos? ¿qué

<sup>1</sup> Ver Muñoz, Ana (2022). *Borderland Circuitry: Immigration surveillance in the United States and beyond*. Oakland: University of California Press; ver también Mijente, Immigrant Defense Project, NIPNLG (2018). Who's behind ICE. [https://mijente.net/wp-content/uploads/2023/02/Who-is-Behind-ICE-The-Tech-and-Data-Companies-Fueling-Deportations\\_v4.pdf](https://mijente.net/wp-content/uploads/2023/02/Who-is-Behind-ICE-The-Tech-and-Data-Companies-Fueling-Deportations_v4.pdf)

retos nos aguardan? Es imposible responder a estas preguntas simplemente diseccionando la crudeza o la procedencia de una única tecnología, sistema o actor. Primero tenemos que entender las motivaciones transnacionales que impulsan estas dinámicas en ascenso, más observables, sobre el terreno. En otras palabras, debemos hacer visible la infraestructura digital invisible.

### **La infraestructura digital es clave para la externalización de fronteras y el aumento de la violencia irresponsable**

Entender la externalización de las fronteras a través de la lente de la infraestructura digital capta la verdadera escala de las prácticas fronterizas previstas por Estados Unidos (y sus competidores y aliados), así como su permanencia prevista en el futuro orden mundial. La infraestructura fronteriza digital se alimenta de historias de dominación, control y atrocidades en nombre de proyectos transnacionales de *lucha contra el crimen*, preparando el terreno para unos elevados costes sociales.

En primer lugar, en lo que respecta a la escala, estamos asistiendo a una escalada del imperialismo fronterizo estadounidense y de la violencia en las fronteras, tanto en términos de alcance geográfico en territorios nacionales como de la ampliación de la *capacidad policial* a un número cada vez mayor de individuos y grupos a través de esta infraestructura digital.<sup>2</sup> Esto incluye a cualquier persona que un

<sup>2</sup> Esta lente también nos permite hacer hincapié en la conexión con antecedentes históricos como los proyectos de *modernización* de las infraestructuras físicas de tránsito y comercio, donde el vínculo con la violencia estatal es indiscutible (por ejemplo, los proyectos de construcción de ferrocarriles y el genocidio de los pueblos indígenas en Sonora entre 1880 y 1900). Ver Guidotti-Hernández, N. (2011). *Unspeakable Violence: remapping U.S. and Mexican national imaginaries*. Londres: Duke University Press. Insistimos en que esta escala no se aleja de las lógicas racializadas que han definido las prácticas fronterizas en esta región durante décadas. Ver Rosas, G. (2006). The managed violences of the borderlands: treacherous geographies, policeability, and the politics of race. *Latino Studies*, 4(4), 401–418. <https://doi.org/10.1057/palgrave.lst.8600221>

algoritmo considere *peligrosa*, a quienes puedan emigrar, así como a los agentes humanitarios, los grupos de defensa de los inmigrantes y las organizaciones de ayuda. La escalabilidad y el rápido crecimiento que engendra es una propiedad por excelencia de las tecnologías digitales, independientemente de su origen o aplicación. Los desplazamientos hacia nuevos objetivos en el marco de la infraestructura digital carecen de fricciones en comparación con las anteriores tácticas analógicas de vigilancia fronteriza. Asegurado, el agricultor que ayudaba a los inmigrantes en El Salvador, se vio envuelto en la red de externalización fronteriza de Estados Unidos con un simple “OK” en un chat de WhatsApp.

En segundo lugar, en cuanto a la permanencia, los defensores de las fronteras digitales en las capitales nacionales, la industria y las agencias de desarrollo adoptan el término *infraestructura pública digital* como una marca, para otorgar confianza (no merecida), normalización y la inevitabilidad de herramientas digitales cuestionadas como las identificaciones biométricas y los sistemas de pago.<sup>3</sup> Ceder el privilegio de definir la *infraestructura digital* a actores con intereses creados en las actuales prácticas de control de la migración es imprudente. Sin una contranarrativa que articule su disposición violenta, las herramientas digitales de externalización de fronteras –incluida la recogida generalizada de datos biométricos, la recopilación de datos de transacciones en tiempo real en los sistemas de pago y la confiscación de

<sup>3</sup> Ver, por ejemplo, Shivkumar, G., O’Neil, K. y Nordhaug, L. (30 agosto de 2021). How to bring digital inclusion to the people who need it most. <https://www.weforum.org/agenda/2021/08/4-reasons-you-should-care-about-digital-public-infrastructure/> (“[Digital Public Infrastructure (DPI)] se refiere a soluciones digitales que permiten funciones básicas esenciales para la prestación de servicios públicos y privados, es decir, colaboración, comercio y gobernanza. Piénsese en nuestras actuales infraestructuras públicas compartidas, como carreteras y educación, pero en línea: eso es la DPI en pocas palabras”; Masiero, Silvia y Arvidsson, Viktor (2021). Degenerative outcomes of digital identity platforms for development. *Information Systems Journal*, 31(6), 903–928. <https://doi.org/10.1111/isj.12351>; Massally, K. y Frankenhauser, C. (3 agosto de 2022). The right way to build digital public infrastructure: 5 insights. <https://www.weforum.org/agenda/2022/08/digital-public-infrastructure/>

teléfonos inteligentes en la frontera– pueden normalizarse fácilmente como *infraestructura pública digital*, en lugar de resistirse a ellas.

La escala y el impacto duradero del rápido endurecimiento de la infraestructura digital que alimenta la externalización fronteriza exigen una coordinación transnacional urgente. Como escritores y activistas, nos hemos unido para resistir el uso de la infraestructura digital en la política estadounidense de control migratorio en México, Centroamérica, Sudamérica y el Caribe. Solo tenemos rastros y no la imagen completa. Basándonos en el trabajo de otros, entretejemos todo esto para mostrar cómo la fusión del poder estatal y digital para construir una infraestructura fronteriza digital no es ni humana ni segura: más bien, está incrementando formas de violencia irresponsables.

### **Convergencia: guerra contra las drogas, externalización de fronteras, infraestructura digital y militarización de las regiones vecinas de EE.UU.**

Desde la década del setenta, las iniciativas económicas y políticas han impulsado sin tregua las inversiones estadounidenses en prácticas de control de la inmigración más militarizadas, criminalizadoras y digitalizadas. Desde el 11 de septiembre, la convergencia estadounidense de la *seguridad nacional* con la migración no autorizada ha impulsado un régimen de externalización de fronteras cada vez más amplio –actualmente hay 23 oficinas de la CBP y 48 oficinas del ICE en todo el mundo–(Aizeki et al., 2021) y, en consecuencia, ha proporcionado un mercado especialmente lucrativo para las empresas de vigilancia digital.<sup>4</sup> A través de programas como la Iniciativa Mérida y la Iniciativa de Seguridad Regional Centroamericana, Estados Unidos ha vinculado

<sup>4</sup> Andersson, Ruben (2018). *Illegality, Inc.: clandestine migration and the business of bordering Europe*. Oakland: University of California Press; Miller, Todd (2019). *Empire of Borders: The Expansion of the U.S. Border around the World*. Londres, Nueva York: Verso.; Akkerman, Mark (2021). *Border Wars*. Amsterdam: Transnational Institute



la ayuda a países como México, El Salvador, Guatemala y Honduras al aumento de la militarización, la vigilancia policial, el encarcelamiento y el control de la migración.

Sin embargo, los patrones migratorios hacia Estados Unidos desde México, América Central y el Caribe no pueden disociarse de las prácticas y políticas que Estados Unidos ha empleado durante más de un siglo para dominar a los países de estas regiones. Décadas de prácticas y políticas estadounidenses han alimentado la inestabilidad económica, política y medioambiental, factores clave que impulsan la migración a Estados Unidos. En los últimos veinte años, el número de personas que emigran desde Centroamérica se ha más que duplicado, y los mayores aumentos se han producido en Guatemala, Honduras y México. La *guerra contra el narcotráfico* respaldada por Estados Unidos en México y Centroamérica ha aumentado drásticamente la violencia y la inestabilidad (Paley, 2014). En México, la lucha contra el crimen organizado ha provocado 350 mil muertes y más de 72 mil desapariciones entre 2006 y 2021. Según el Banco Mundial, el 60 % de la población rural centroamericana vive en la pobreza. Aunque los mayores contribuyentes a la crisis climática son los países ricos, estas poblaciones ya empobrecidas sufren los impactos más agudos del cambio climático. Durante décadas, las sequías prolongadas junto con catástrofes naturales como huracanes e inundaciones han afectado profundamente a Centroamérica. El número de personas que se enfrentan la inseguridad alimentaria se triplicó entre 2019 y 2021, afectando a 6,4 millones de personas. Asegurado, Pérez y Ramírez –como muchos otros– buscan alternativas a esta situación intolerable.

En lugar de reconocer estas causas subyacentes, la respuesta de Estados Unidos ha sido ampliar aún más su frontera. El general John Kelly, ex secretario del Departamento de Seguridad Nacional de Estados Unidos (DHS), declaró: “Creo que la defensa de la frontera suroeste comienza a 1.500 millas al sur”. México ha sido durante mucho tiempo fundamental en el régimen de externalización de fronteras de EE.UU., y la infraestructura digital desempeña un papel cada vez más crítico. Tony Crowder, ex director de Operaciones Aéreas y Marítimas

de la CBP, compartía la opinión de Kelly: «Hemos enseñado a pescar a los mexicanos... [pero] aunque tenemos toda esta capacidad de vigilancia, no tenemos suficiente, necesitamos más» (Miller, 2019).

Aunque forma parte de los esfuerzos continuados de Estados Unidos por reclutar a México en apoyo de sus objetivos regionales, esta *asociación para la seguridad y el Estado de derecho* se aceleró tras el 11 de septiembre. En 2007, Estados Unidos desplazó el foco de su guerra contra las drogas de Colombia a México, América Central y el Caribe. En este marco de securitización, la guerra contra las drogas se fusionó con el régimen de control de la inmigración. En 2008, se puso en marcha la Iniciativa Mérida, una asociación bilateral entre Estados Unidos y México en nombre de la guerra estadounidense contra las drogas. Inicialmente proporcionó financiación para que México adquiriera equipamiento para sus fuerzas militares y policiales y para la recopilación de información de inteligencia. En 2013, Mérida fue renovada para incluir cuatro pilares, incorporando la creación de una “frontera estadounidense-mexicana del siglo XXI, mejorando al mismo tiempo la aplicación de las leyes de inmigración en México y la seguridad a lo largo de las fronteras meridionales de México”. Desde 2008, unos 3.500 millones de dólares, prolongación de la política estadounidense, han contribuido a dar forma a la agenda de control migratorio de México.

En 2014, el Programa Frontera Sur reforzó aún más la seguridad de la frontera sur de México mediante el aumento de la policía de migración y el aparato de deportación. En consecuencia, México cuenta ahora con uno de los mayores sistemas de detención de inmigrantes del mundo. Entre 2014 y 2017, México deportó a más centroamericanos que la Patrulla Fronteriza de Estados Unidos. Doris Meissner, ex comisionada del Servicio de Inmigración y Naturalización (INS, el predecesor de ICE y CBP), subrayó la importancia del control migratorio mexicano, explicando en 2017 la necesidad de examinar tanto los datos estadounidenses como los mexicanos para evaluar la eficacia de la aplicación de la ley en la frontera estadounidense (Miller, 2019, p. 177).

En el marco de estos acuerdos, el Departamento de Defensa de EE.UU. ha proporcionado formación y ha vendido millones en equipamiento militar a México, incluida una serie de tecnologías de *fronteras inteligentes* proporcionadas por empresas como Dev Technology, General Dynamics, Amazon Web Services y NEC.<sup>5</sup> Un elemento clave del apoyo de EE.UU. a México ha sido el desarrollo de una infraestructura para recopilar y compartir datos –como información biométrica y biográfica, y antecedentes penales– de forma que interactúe sin problemas con las bases de datos estadounidenses.

La infraestructura digital que rastrea y cataloga a los migrantes es fundamental para la política migratoria estadounidense en México. La estrategia del Instituto Nacional de Migración (INM), respaldada por Estados Unidos, se basa en esta infraestructura como principal medio para controlar la migración en lugar de sellar la frontera sur de México con Guatemala. La recogida de datos biométricos es esencial para que los migrantes sean más legibles para el Estado. En 2011, Estados Unidos proporcionó cuatro quioscos biométricos a la frontera sur de México, y 117 escáneres biométricos adicionales al año siguiente. Entre 2018 y la primera mitad de 2022, el gobierno mexicano recopiló y compartió información sobre más de 360 mil migrantes en centros de detención.<sup>6</sup> La información de la CBP revela que las autoridades mexicanas compartieron información de 10 mil solicitudes de visado humanitario ante el DHS. La liberación de aproximadamente 1.800 migrantes no registrados de un albergue en Piedras Negras estaba condicionada al registro de sus datos.<sup>7</sup>

Un “entorno de intercambio de información” que incluya sistemas interoperativos de intercambio de datos es fundamental para lograr

<sup>5</sup> Immigrant Defense Project, Mijente, y NIPNLG (2018). Who's Behind ICE: The Tech and Data Companies Fueling Deportations. [https://mijente.net/wp-content/uploads/2023/02/Who-is-Behind-ICE-The-Tech-and-Data-Companies-Fueling-Deportations\\_v4.pdf](https://mijente.net/wp-content/uploads/2023/02/Who-is-Behind-ICE-The-Tech-and-Data-Companies-Fueling-Deportations_v4.pdf)

<sup>6</sup> Ver FOIA: <https://www.foia.gov/>

<sup>7</sup> Watch CBP Intel (2019). Central American Caravans and Migration Crisis Flow - Update 32. *U.S. Customs and Border Protection*. <https://r3d.mx/wp-content/uploads/Central-American-Caravans-and-Migration-Crisis-Flow-Update-32.pdf>.

los objetivos del Estado de seguridad nacional (Meissner et al., 2013). La *interoperabilidad* permite una conectividad sin fisuras entre la policía, las agencias de inmigración, los gobiernos extranjeros, etc.<sup>8</sup> Las principales formas de la infraestructura digital iniciada por Estados Unidos se basan en la recopilación generalizada de información y el intercambio sin fisuras de datos para la vigilancia a través de las fronteras.

Este enorme volumen de recopilación e intercambio de datos se ha visto impulsado por el despliegue del poder del Estado carcelario—incluida la centralidad del “extranjero delincuente”, el “miembro de una banda” y el “narcotraficante” como amenazas para la seguridad nacional— en todos los niveles geográficos del régimen estadounidense de control de inmigrantes. Por ejemplo, el Programa de Alerta Migratoria Transnacional de Identificación Biométrica (BITMAP) permite al DHS y a sus países socios saber dónde y cuándo llega una persona al hemisferio occidental y sus pautas de viaje antes de que llegue a la frontera suroeste de Estados Unidos. El BITMAP está desplegado actualmente en 18 países, incluido México. El DHS también cuenta con un programa de intercambio de información sobre antecedentes penales (CHIS) que permite compartir a escala mundial información biográfica, biométrica y descriptiva sobre las personas expulsadas de Estados Unidos (por ejemplo, presuntos antecedentes de inmigración, laborales, familiares y penales).

La criminalización estructural de la pobreza en ambos países se amplifica con el CHIS. Según la Encuesta Nacional de Población Privada de la Libertad en México, realizada por el Instituto Nacional de Geografía y Estadística (INEGI) en 2021, casi el 44 % de los encuestados declaró haber sido encarcelado por acusaciones o incriminaciones falsas. El 42 % afirmó haber sido obligado a declararse culpable o a incriminar a otra persona. Casi la mitad de las personas encarceladas

<sup>8</sup> Ver Woodward, John (2005). Using biometrics to achieve identity dominance in the Global War on Terrorism. *Military Review*; ver también Jacobsen, Annie (2021). *First Platoon: a story of modern war in the age of identity dominance*. Nueva York: Dutton.

no han sido condenadas (Angel, 2020), y casi la mitad de las condenas son por robos de menos de 100 dólares (Romero, 2014). Este es el tipo de datos que alimenta CHIS.

En otro ejemplo, el DHS está desarrollando el Sistema Avanzado de Tecnología de Reconocimiento Nacional (HART, por sus siglas en inglés) para sustituir a su actual base de datos biométricos centralizada, IDENT, mediante un contrato con Peraton (filial de Veritas Capital, una empresa de capital riesgo). Alojado en Amazon Web Services, HART permitirá al DHS agregar y comparar datos biográficos y biométricos de cientos de millones de personas en todo el mundo. Esto incluye los denominados datos de identificación procedentes de identificaciones policiales, reconocimiento facial, ADN, escáneres de iris e impresiones de voz, normalmente recopilados sin el conocimiento o consentimiento de la persona. La enorme base de datos HART se basa en la recopilación generalizada de datos biométricos en todos los ámbitos, por ejemplo, el desarrollo de bases de datos de ADN integradas en México y Centroamérica por parte del Departamento de Estado de EE.UU. en nombre de la lucha contra el tráfico de personas o la propuesta de un documento de identificación digital biométrica nacional en México. De este modo, se fusionan múltiples iniciativas estatales y crece exponencialmente el poder del Estado para vigilar, rastrear y controlar a los migrantes y a todas las personas bajo su vigilancia.

Aunque la Iniciativa Mérida terminó formalmente en 2019, su enfoque ha sido sostenido por el gobierno mexicano. En 2021, el gobierno mexicano aumentó el ejército en un 46 % y la Guardia Nacional dedicada a detener migrantes en un 300 %. En julio de 2022, el presidente López Obrador comprometió 1.500 millones de dólares en infraestructura fronteriza inteligente durante los próximos dos años.

Para los estados socios de EE.UU., cualquier canal tecnológico y de intercambio de datos que se financie y se exporte a ellos se convierte en un activo, no solo para vigilar a los migrantes, sino para impulsar múltiples agendas de construcción de poder coercitivo. Por tanto, esta infraestructura puede acabar alimentando la violencia

y la criminalización, socavando el derecho de asilo, exacerbando la desigualdad y ampliando el poder de los paramilitares y la policía, al tiempo que privilegia las prerrogativas corporativas y neoliberales securitizadas.

## **La naturaleza geopolítica de la infraestructura digital**

En su investigación sobre los sistemas de pago digitales, Marieke de Goede y Carola Westermeier utilizan el término *geopolítica de infraestructuras* para subrayar la creciente centralidad de las infraestructuras en la geopolítica y el modo en que el poder económico estadounidense está arraigado en las infraestructuras financieras (que, como el control de la migración, se están digitalizando rápidamente) (De Goede y Westermeier, 2022).

La red mundial de mensajería financiera SWIFT es un ejemplo de infraestructura invisible para la mayoría de la gente y que, sin embargo, desempeña un papel fundamental, como describen los autores, en el refuerzo de las relaciones de poder del orden mundial de posguerra en el que surgió. Setenta años después de la Segunda Guerra Mundial y cincuenta desde la creación de SWIFT, las rutas de mensajería bancaria fluyen a través de antiguas capitales coloniales y se sitúan en un *núcleo* de países occidentales, dejando grandes franjas de América Latina, África y Oriente Medio en una periferia económica permanente, pero efectivamente invisible. Del mismo modo, las identificaciones digitales, el seguimiento y la infiltración en las redes sociales y las plataformas de intercambio de datos son esencialmente componentes, nodos o capas parcialmente visibles de proyectos de infraestructura digital geoestratégica más profundos y a más largo plazo.

La ampliación de las fronteras mediante infraestructuras digitales sirve a objetivos políticos y económicos de Estados Unidos que van mucho más allá de la vigilancia de la movilidad humana. La lucha geopolítica por el control de las infraestructuras se desarrolla en varios ámbitos. Los organismos militares codician el *dominio de la identidad*,

un objetivo que llevó a las fuerzas estadounidenses a recopilar almacenes masivos de datos biométricos en Afganistán e Irak como arma de guerra.<sup>9</sup> Los gigantes estadounidenses de los servicios digitales como Amazon y Google dominaron la *plataformización* construyendo infraestructuras de comercio electrónico (publicidad digital, búsquedas, redes sociales, etc.) para dominar la economía digital. A menudo convergen los intereses de los sectores público y privado, incluso en forma de asociaciones público-privadas (APP) para construir infraestructuras. En cada caso, la verdadera pugna entre estados y gigantes corporativos se centra en el control de la interfaz, o de los métodos infraestructurales más esenciales e invisibles de comunicación y control digitales. Como explica Michael Kwet, “las corporaciones transnacionales de las ‘grandes tecnologías’ con sede en Estados Unidos han amasado billones de dólares y han adquirido poderes desmesurados para controlarlo todo, desde los negocios y el trabajo hasta los medios sociales y el entretenimiento en el Sur Global. El colonialismo digital se está extendiendo por todo el mundo” (Kwet, 2021). La búsqueda de Estados Unidos de la dominación a través de infraestructuras externalizadas de vigilancia de la migración va de la mano de sus designios geopolíticos y corporativos de poder económico.

Estas formas de poder digital a través de las infraestructuras plantean retos únicos para la documentación y, en última instancia, para cualquier forma de cambio sistémico. Los retos incluyen líneas borrosas de responsabilidad, misión y función; los gobiernos y los actores corporativos son vistos o presentados como conductos pasivos o intermediarios en la infraestructura pública digital; y las infraestructuras pueden aparecer fácilmente como *ahistóricas* y sin motivación. En México y Centroamérica, el control de la migración converge con las operaciones policiales exteriores de Estados Unidos (como la guerra contra las drogas y las guerras entre bandas). Exploramos los diversos

<sup>9</sup> Ver Woodward, John (2005). Using biometrics to achieve identity dominance in the Global War on Terrorism. *Military Review*. <https://www.rand.org/pubs/reprints/RP1194.html>; ver también Jacobsen, 2021.

efectos simultáneos de esta compleja fusión: el giro hacia la infraestructura digital; su relación con la violencia y el sufrimiento humano; y su exclusión de la rendición de cuentas por estos daños.

### **Infraestructura digital de fronteras en su teléfono: las técnicas policiales de las Tecnologías de la Información y la Comunicación (TIC) en las rutas migratorias**

La infraestructura de vigilancia es tangible en los centros físicos de detención de inmigrantes y en las detenciones policiales, con fichas policiales, frotis de mejillas y confiscación del teléfono móvil del detenido, entre otras. La creciente integración de la vida cotidiana, las telecomunicaciones y la informática abre amplias vías para una vigilancia más encubierta y oportunista de las comunicaciones y actividades privadas de los usuarios que recurren a las redes sociales, las comunicaciones móviles y las aplicaciones de mensajería. La vigilancia de los teléfonos móviles y las redes sociales abarca desde la obligación de revelar información para solicitar visados y prestaciones sociales hasta la elaboración de listas y el seguimiento por parte del gobierno de manifestantes y otros actores *indeseables*. La vigilancia de los migrantes está inmersa en estos sistemas de control, en los que la tecnología de vigilancia sirve de herramienta silenciosa para la violencia y la represión gubernamentales.

Esto ha repercutido en la forma en que los migrantes viajan y se mantienen a salvo, por ejemplo, mediante la seguridad en el número. Viajar en caravana se ha convertido, por tanto, en una estrategia tanto de supervivencia como de protesta: fuentes de seguridad tanto física como económica y de oposición a las políticas económicas que contribuyeron a su desplazamiento. Las redes sociales y las aplicaciones de mensajería son herramientas clave para la coordinación de las caravanas y para los migrantes en general. Los migrantes utilizan estas herramientas para identificar rutas, buscar refugio y alimentos, comunicarse con sus redes de apoyo, avisarse mutuamente de los riesgos y



coordinar los viajes. Tanto los gobiernos como la delincuencia organizada entienden esta dinámica y utilizan estas mismas herramientas para vigilar y extorsionar a los migrantes.

El 5 de junio de 2019, Irineo Mújica, de Sin Fronteras –una organización de la sociedad civil dedicada a la protección de los derechos humanos de los migrantes en México y Estados Unidos, y que ha apoyado a múltiples caravanas de migrantes– fue detenido en México, acusado falsamente de tráfico de personas. Mújica apareció en la base de datos de la lista de vigilancia de la CBP publicada en 2019 que contenía fotos, nombres, profesiones y otros detalles de periodistas, activistas y personas influyentes en las redes sociales, tanto de México como de Estados Unidos, con vínculos con la caravana de migrantes.

Un informe de la Oficina del Inspector General (OIG) del DHS sobre la base de datos y otras prácticas de vigilancia descubrió que la CBP estableció alertas electrónicas (vigías) sobre periodistas, abogados y defensores que estaban conectados a través de las redes sociales con las caravanas de migrantes.<sup>10</sup> Las personas etiquetadas por los vigías eran constantemente marcadas para un control secundario al entrar en Estados Unidos, e interrogadas sobre su trabajo, organización, familia, educación e inclinaciones políticas.

La militarización de esta información tuvo efectos nefastos en el lado mexicano de la frontera. Según Alex Mensing, activista de Sin Fronteras, después de que la CBP compartiera con el Gobierno mexicano la información recabada a través de los vigías, otros miembros de su organización que ayudaron a las caravanas de migrantes en el mismo periodo vieron aumentar el escrutinio fronterizo y las amenazas de muerte. Organizar y apoyar a los migrantes amenaza las operaciones lucrativas que dependen de la criminalización de la migración en toda la región. La ayuda de la sociedad civil hace que los migrantes sean menos propensos al secuestro y la extorsión, lo que por tanto

<sup>10</sup> DHS Office of Inspector General (2021) ‘CBP Targeted Americans Associated with the 2018–2019 Migrant Caravan’. <https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-62-Sep21.pdf>

reduce los ingresos de la delincuencia organizada vinculada a estas actividades y, como efecto dominó, también disminuyen los sobornos a las autoridades, lo que enfrenta los intereses colectivos de estos grupos con los de los activistas y los que prestan ayuda humanitaria.

La vigilancia de cualquier persona que pueda suponer una amenaza para el sistema ha sido durante mucho tiempo una forma generalizada y sistemática de control gubernamental en México. Un documento filtrado de NSO Group, la empresa israelí que creó Pegasus, reveló que 50 mil personas eran posibles objetivos de vigilancia en México. La lista incluía a políticos de la oposición, periodistas que investigaban la corrupción gubernamental y las ejecuciones extrajudiciales, activistas que abogaban por gravar las bebidas azucaradas, jueces, académicos y expertos internacionales que investigaron el caso de la desaparición forzada y ejecución extrajudicial de los 43 estudiantes, entre otros.

En 2022, se descubrió que los teléfonos móviles de dos periodistas y un activista que investigaron los abusos cometidos por el ejército mexicano estaban infectados con el programa malicioso Pegasus. En 2020, el Gobierno mexicano pretendió crear un registro de tarjetas SIM que enlazaría con los datos biométricos y otros datos personales del propietario de la tarjeta. Esto habría intensificado la vigilancia digital del gobierno a través de la infraestructura de las TIC, y contó con la oposición de la sociedad civil.

Documentos internos de la CBP muestran que las agencias gubernamentales a través de la frontera comparten continuamente información sobre la ubicación de los migrantes, su origen y el número de personas en cada grupo, incluso antes de que comiencen a migrar. En 2018, agentes del DHS estadounidense se infiltraron en un grupo de WhatsApp de migrantes hondureños que viajaban en una caravana de unos 4.000. Estas prácticas policiales también están siendo reproducidas por el Gobierno mexicano.<sup>11</sup>

<sup>11</sup> LIS and R3D (2023). Uso de las tecnologías digitales en los contextos migratorios: necesidades, oportunidades y riesgos para el ejercicio de los derechos humanos de las

## **Impacto: violencia infraestructural y déficit de rendición de cuentas en la actuación policial globalizada en materia de migración**

Roberto M., un joven de El Salvador, fue tiroteado y detenido por la policía poco después de ser deportado de Estados Unidos. Los policías rurales que dispararon a Roberto también amenazaron a punta de pistola a un testigo presencial, diciéndole que Roberto era miembro de una banda y que, si revelaba lo que había visto, le ocurriría lo mismo. La policía de El Salvador recibe de Estados Unidos datos sobre la afiliación de los miembros de las bandas, y comparte estas listas con la policía de los barrios donde tienen previsto vivir los deportados. Se ha comprobado que estas bases de datos son problemáticas y poco fiables.<sup>12</sup> Los departamentos de policía confirmaron que esta información se utiliza para perseguir a las personas: “Pensamos que si una persona no era buscada en Estados Unidos, debe ser porque la persona deportada es mala”.

La violencia puede vincularse cada vez más a las tecnologías digitales fronterizas, sobre todo en combinación entre sí y con las realidades físicas y medioambientales que las rodean. Algunos estudios muestran los efectos de la vigilancia integrada por torres fijas en las tasas de mortalidad de los inmigrantes en el Valle de Altar, en Arizona. En este caso, la infraestructura digital se fusiona con la ineficaz, aunque antigua, política de disuasión estadounidense, que hace más peligrosas las rutas migratorias, con la teoría de que los migrantes no se arriesgarían a emprender el viaje. La fusión de tecnología y políticas que infligen un daño deliberado produce estos resultados predecibles del aumento de muertes de inmigrantes (Chambers et al., 2019).

personas migrantes, defensoras y periodistas [en prensa]. [www.r3d.mx/publicaciones](http://www.r3d.mx/publicaciones)  
<sup>12</sup> Open Society Justice Initiative (2019). *Unmaking Americans: insecure citizenship in the United States*. <https://www.justiceinitiative.org/uploads/e05c542e-0db4-40cca3ed-2d73abcf37f/unmaking-americans-insecure-citizenship-in-the-united-states-report-20190916.pdf>

La historia de Roberto M. y del testigo de su tiroteo y desaparición tras la deportación en El Salvador refleja otra pauta de violencia vinculada al intercambio de información a través de infraestructuras digitales. La criminóloga Ana Muñiz documenta un “ciclo de actuación policial violenta, migración, actuación policial más violenta, detención, deportación, actuación policial violenta, migración, y así sucesivamente” (Muñiz, 2022), en el que las propias etiquetas (“extranjero criminal” o “miembro de una banda”) se convierten en vectores ineludibles de precariedad. Tales etiquetas canalizan a los individuos hacia una *especie de apátridas* como chivos expiatorios constantes y cuantificables que proporcionan una distracción fácil para las fuerzas de seguridad del Estado y las corporaciones que producen y perpetúan las “causas estructurales de la violencia” (Rosas, 2006).

La infraestructura digital no se fusiona con un terreno físico, sino con factores sociales y políticos preexistentes que hacen de la violencia una conclusión inevitable. La infraestructura digital polivalente de hoy en día también permite la incorporación eficaz de nuevas categorías criminalizadas indeseables, incluidos los *organizadores de caravanas* o los *promotores de la migración*, como en el intento de El Salvador de reformar su código penal, criminalizando la *promoción de la migración* en las redes sociales.

## Retos y perspectivas

Nos interesa desarrollar un conocimiento más profundo sobre los orígenes políticos de estas infraestructuras para desafiar la violencia de los sistemas globales de control de la migración. Este ensayo solo delimita el campo del objeto de estudio. Se necesita mucho más trabajo colectivo para documentar y diseñar modelos de resistencia que permitan hacer frente a estos desafíos.

La naturaleza difusa y estructural del poder que subyace a las características aparentemente ahistóricas y carentes de motivación de las infraestructuras digitales socava los enfoques clásicos de la rendición

de cuentas. Además, las conocidas vías judiciales nacionales e internacionales para responsabilizar a los autores de estas formas de violencia indirecta –por muy imperfectas o ineficaces que puedan ser– son excepcionalmente inadecuados para las condiciones que se dan en el contexto específico del seguimiento policial de la migración, y esto por varias razones.

En primer lugar, las tecnologías en uso, como las bases de datos biométricos, y los medios de utilizar tecnologías civiles como las redes sociales y otras TIC, simplemente no están diseñadas para respetar o someterse al escrutinio democrático; son de corte militar y convertidas para su uso en espacios cuasi-militarizados, por instituciones impregnadas de ideología militar. Casi un tercio del personal de la CBP sirvió anteriormente en el ejército estadounidense. Las tecnologías de vigilancia biométrica avanzaron a pasos de gigante en las operaciones militares estadounidenses antes de integrarse en la vigilancia fronteriza *civil*. Los contratistas militares del sector privado desempeñan un papel integral en esta transición.

Como documenta la periodista Annie Jacobsen, en el marco de la recopilación de datos biométricos por parte del ejército estadounidense en Afganistán, Palantir Technologies sirvió de enlace fundamental entre las operaciones de inteligencia estadounidenses para rastrear y matar a objetivos militares y las operaciones policiales cuasi civiles, como la prueba piloto de muestras rápidas de ADN de familias migrantes en la frontera estadounidense en 2019 (Jacobsen, 2020). Hoy en día, los kits biométricos utilizados en Afganistán, algunos de los cuales aún almacenan datos biométricos recopilados en el campo de batalla, están a la venta en eBay.

En segundo lugar, los organismos de justicia y supervisión están mal equipados para cumplir la función que les corresponde en este ecosistema. En los procedimientos e investigaciones penales, el uso de tecnologías que capturan y registran pruebas de actividades supuestamente delictivas o que pretenden cotejar biométricamente los registros son extremadamente difíciles de impugnar debido a su barniz científico y a la opacidad de sus métodos de recopilación y análisis

de datos, lo que no deja margen práctico para impugnar o excluir tales pruebas. El diseño de tecnologías que predeterminan factores de riesgo relacionados con conductas delictivas, incluida la migración, contraviene la presunción de inocencia. En el contexto civil, los mecanismos de justicia de ámbito nacional niegan la legitimación activa a los no nacionales situados fuera de Estados Unidos que son víctimas de violaciones vinculadas a la vigilancia digital.

Por último, existen enormes incentivos para que tanto el Estado como el poder empresarial oculten la violencia. El posicionamiento político de las *fronteras inteligentes* como más *humanas* oculta el papel del Estado en la violencia y aísla a las corporaciones de las relaciones públicas negativas o de las restricciones por participar en mercados repugnantes. Su tarea se ve facilitada por la abstracción del dolor físico en lugar de afectar a seres humanos reales (Guidotti-Hernandez, 2011; Woodward, 2005), y por características de la economía de datos como la forma en que las empresas han ayudado al movimiento hacia la gestión de las funciones gubernamentales como plataformas digitales privadas.

Las herramientas de *evaluación de riesgos* de mitigación, como la protección de datos o las evaluaciones de impacto sobre los derechos humanos proporcionan cobertura, favoreciendo la continuación de estas prácticas empresariales porque las empresas las llevan a cabo voluntariamente y se enfrentan a pocas o ninguna consecuencia por una mala evaluación de riesgos. Como era de esperar, estas herramientas dirigidas por la industria a menudo no proporcionan un medio real para la rendición de cuentas; revelan escasa información que sería procesable si y cuando los productos causan daño; y la carga de probar las violaciones de derechos y encontrar un remedio eficaz después de los hechos es asumida enteramente por las víctimas. Los intereses de actores poderosos convergen en torno a una red de intereses financieros en el sistema, lo que conduce al acoso agresivo y al posible silenciamiento de activistas, como ilustra el caso de Irineo Mújica y Sin Fronteras.

Necesitamos herramientas y métodos de cooperación transnacional para documentar, recopilar y compartir información de forma segura, y organizarnos. La fusión de nuevos conocimientos sobre cómo funciona el poder digital dentro de los movimientos de resistencia transnacionales existentes ofrece la posibilidad de cuestionar la infraestructura digital de la externalización de fronteras.

Estamos en las fases iniciales de nuestro esfuerzo colectivo por comprender y sacar a la luz esta infraestructura digital. A través de este análisis, podemos empezar a identificar las intervenciones para empezar a desmantelarla y romperla. La organización transnacional contra las corporaciones tecnológicas ofrece oportunidades para un entendimiento compartido y una solidaridad significativa. Este año, organizaciones de Francia y Kenia, con el apoyo de actores de otros países, demandaron al gigante de la biometría IDEMIA por no cumplir ni siquiera las normas mínimas de diligencia debida en materia de derechos humanos, ya que cosecha miles de millones en ventas secretas de tecnología de seguridad fronteriza a países de renta baja y media. Esta iniciativa surgió de la colaboración en la recopilación de pruebas y la organización transfronteriza.

Como reconoció el estamento militar estadounidense hace décadas: “quien domina el campo de las fronteras externalizadas define ‘amigo y enemigo’ en todas partes” (Woodward, 2005). Cuanto más rápido establezca Estados Unidos el dominio económico y político sobre la infraestructura digital de control de la migración, mayor será su seguridad para mantener el poder digital global. La infraestructura digital sirve a múltiples propósitos a la vez, pero la función geopolítica última es el poder bruto y generalizado sobre los asuntos mundiales. Las herramientas examinadas aquí *contendrán* la vida humana dentro de espacios de violencia catastrófica, por diseño (Muñiz, 2022; Rosas, 2006; Khan, 2019). Este efecto específico traiciona los compromisos más fundamentales de los derechos humanos internacionales y el derecho humanitario ante los desafíos sin precedentes para la supervivencia humana en la mayor parte del mundo. Pero este efecto pernicioso tampoco viene al caso.

En realidad, como facetas del poder infraestructural, las tecnologías que fijan el “cálculo de quién debe vivir y quién debe morir” (Rosas, 2006) no lo hacen como un fin en sí mismo, sino al servicio del poder y de su reproducción en esta era digital (McCoy, 2017). De este modo, la complicidad de los actores estatales y corporativos en la producción de violencia se pone de manifiesto con la mayor crudeza. Este análisis geopolítico es nuestro punto de partida para construir la resistencia y promover la transformación.

## Bibliografía

Aizeki, Mizue et al. (2021). *Smart Borders or A Humane World*. <https://www.tni.org/en/publication/smart-borders-or-a-humane-world>

Akkerman, Mark (2021). *Border Wars*. Amsterdam: Transnational Institute.

Andersson, Ruben (2018). *Illegality, Inc.: clandestine migration and the business of bordering Europe*. Oakland: University of California Press.

Angel, Arturo (15 de diciembre de 2020). Población en cárceles crece a ritmo récord en 2020: hay 14 mil reos más que al inicio del año. *Animal Político*. <https://www.animalpolitico.com/2020/12/poblacion-carceles-crece-record-2020#:~:text=Mientras%20que%20en%20diciembre%20de,de%20que%20cometieron%20un%20delito>

Cáceres, Gabriela y Gressier, Roman (14 de mayo de 2021). Sting operation against migrant caravan arrests working-class migrants as human traffickers. *El Faro*.



[https://elfaro.net/en/202105/el\\_salvador/25479/Sting-Operation-against-Migrant-Caravan-Arrests-Working](https://elfaro.net/en/202105/el_salvador/25479/Sting-Operation-against-Migrant-Caravan-Arrests-Working)

Chambers, Samuel et al. (2019). 'Mortality, surveillance and the tertiary "funnel effect" on the U.S.-Mexico border: a geospatial modeling of the geography of deterrence'. *Journal of Borderlands Studies*, 36(3), 443–468. <https://doi.org/10.1080/08865655.2019.157086>

De Goede, Marieke y Westermeier, Carola (2022). Infrastructural geopolitics. *International Studies Quarterly*, 66(3), 1–12. <http://dx.doi.org/10.1093/isq/sqac033>

DHS Office of Inspector General (2021). CBP Targeted Americans Associated with the 2018–2019 Migrant Caravan. <https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-62-Sep21.pdf>

Guidotti-Hernández, Nicole (2011). *Unspeakable Violence: remapping U.S. and Mexican national imaginaries*. Londres: Duke University Press

Immigrant Defense Project, Mijente, y NIPNLG (2018). Who's Behind ICE: The Tech and Data Companies Fueling Deportations. [https://mijente.net/wp-content/uploads/2023/02/Who-is-Behind-ICE-The-Tech-and-Data-Companies-Fueling-Deportations\\_v4.pdf](https://mijente.net/wp-content/uploads/2023/02/Who-is-Behind-ICE-The-Tech-and-Data-Companies-Fueling-Deportations_v4.pdf)

Jacobsen, Annie (2021). *First Platoon: a story of modern war in the age of identity dominance*. Nueva York: Dutton.

Johnson, R. [@USAmbSV] (15 enero de 2021). Aplaudo a las autoridades salvadoreñas que están tomando acción contra quienes quieren engañar a los ciudadanos con caravanas y promesas falsas Solo promueven #UnViajeEnVano [Twit]. *Twitter*. [https://twitter.com/FGR\\_SV/status/1350133335549501443](https://twitter.com/FGR_SV/status/1350133335549501443)

Khan, Jeffrey (2019). *Islands of Sovereignty: Haitian migration and the borders of empire*. Chicago: University of Chicago Press.

Kwet, Michael (2021). Digital Colonialism. <https://longreads.tni.org/digital-colonialism-the-evolution-of-us-empire>

Masiero, Silvia y Arvidsson, Viktor (2021). Degenerative outcomes of digital identity platforms for development. *Information Systems Journal*, 31(6), 903–928. <https://doi.org/10.1111/isj.12351>

Massally, K. y Frankenhauser, C. (3 agosto de 2022). The right way to build digital public infrastructure: 5 insights. <https://www.weforum.org/agenda/2022/08/digital-public-infrastructure/>

McCoy, Alfred (2017). *In the Shadows of the American Century: The Rise and Decline of US Global Power*. Chicago: Haymarket Books.

Meissner, Doris et al. (2013). *Immigration Enforcement in The United States: a formidable machinery*. Washington, DC: Migration Policy Institute. <https://www.migrationpolicy.org/pubs/enforcementpillars.pdf>.

Mijente, Immigrant Defense Project, NIPNLG (2018). Who's behind ICE. [https://mijente.net/wp-content/uploads/2023/02/Who-is-Behind-ICE-The-Tech-and-Data-Companies-Fueling-Deportations\\_v4.pdf](https://mijente.net/wp-content/uploads/2023/02/Who-is-Behind-ICE-The-Tech-and-Data-Companies-Fueling-Deportations_v4.pdf)

Miller, Todd (2019). *Empire of Borders: The Expansion of the U.S. Border around the World*. Londres, Nueva York: Verso.

Muñiz, Ana (2022). *Borderland Circuitry: Immigration surveillance in the United States and beyond*. Oakland: University of California Press

Open Society Justice Initiative (2019). Unmaking Americans: insecure citizenship in the United States. <https://www.justiceinitiative.org/uploads/e05c542e-0db4-40cc-a3ed-2d73abcf37f/unmaking-americans-insecure-citizenship-in-the-united-states-report-20190916.pdf>

Paley, Dawn (2014). *Drug War Capitalism*. Oakland, CA: AK Press.

Romero, Oscar A. (10 de febrero de 2014). La criminalización de la pobreza y el sistema de justicia penal. *Información Sididh*. [http://centroprodh.org.mx/sididh\\_2\\_0\\_alfa/?p=31418](http://centroprodh.org.mx/sididh_2_0_alfa/?p=31418)

Rosas, Gilberto (2006). The managed violences of the borderlands: treacherous geographies, policeability, and the politics of race. *Latino Studies*, 4(4), 401–418. <https://doi.org/10.1057/palgrave.lst.8600221>

Shivkumar, G., O’Neil, K. y Nordhaug, L. (30 agosto de 2021). How to bring digital inclusion to the people who need it most. <https://www.weforum.org/agenda/2021/08/4-reasons-you-should-care-about-digital-public-infrastructure/>

Watch CBP Intel (2019). Central American Caravans and Migration Crisis Flow - Update 32. *U.S. Customs and Border Protection*. <https://r3d.mx/wp-content/uploads/Central-American-Caravans-and-Migration-Crisis-Flow-Update-32.pdf>.

Woodward, John (2005). Using biometrics to achieve identity dominance in the Global War on Terrorism. *Military Review*.

