Fronteras "inteligentes", democracias negligentes

Un análisis del uso de la inteligencia artificial y otras formas de tecnología en las políticas de control migratorio

Enero de 2026

Autores: **Martyna A. Wierzbicka, Luisa Forjaz de Lacerda, José Bautista, Noemí Mena y Gonzalo Fanjul.**

Los autores agradecen las contribuciones de Lucila Rodríguez-Alarcón y Cristina Fuentes Lara.

porCausa
Investigación, periodismo y migraciones

CENTRE DELÀS D'ESTUDIS PER LA PAU

Con el apoyo de:

Generalitat de Catalunya

ACCD Agència Catalana de Cooperació al Desenvolupament

Índice

Glosario de tecnicismos y eufemismos

Algoritmo: Secuencia de instrucciones matemáticas que permiten procesar datos y tomar decisiones automáticas. En el ámbito migratorio, su uso plantea riesgos de sesgo, opacidad y ausencia de control humano.

Biometría: Sistema de identificación de personas basado en rasgos físicos o comportamentales —huellas, rostro, iris, voz—. Su uso en fronteras ha generado debate sobre privacidad, discriminación y tratamiento masivo de datos sensibles.

Despersonalización de la decisión pública: Proceso por el cual decisiones antes tomadas por personas pasan a ser ejecutadas por sistemas automáticos, reduciendo la rendición de cuentas y la dimensión ética del poder.

Discriminación algorítmica: Reproducción de prejuicios o desigualdades sociales dentro de sistemas automatizados, consecuencia del sesgo en los datos de entrenamiento o en el diseño de los modelos.

Externalización del control migratorio: Delegación de funciones de control y vigilancia a países de tránsito o empresas privadas, desplazando las fronteras más allá del territorio europeo y diluyendo la responsabilidad estatal.

Fetichismo tecnológico: Fe irracional en la neutralidad y superioridad de la tecnología como solución política o moral. Justifica la delegación de poder en sistemas opacos y descontextualizados.

Frontera inteligente: Conjunto de tecnologías —sensores, drones, biometría, inteligencia artificial— aplicadas al control migratorio con el fin de vigilar, clasificar y restringir la movilidad. Representa el paso de la frontera física a una infraestructura de datos y algoritmos.

Fronteras verticales: La verticalización de la frontera es un proceso dinámico por el cual la línea fronteriza deja de ser una línea física para desplazar sus límites cada vez más al Sur, bloqueando o paralizando la migración hacia el Norte global.

Gobernanza algorítmica: Modelo de administración pública en el que la toma de decisiones depende de procesos automatizados y flujos de datos, reduciendo el espacio para la deliberación democrática.

Industria del Control Migratorio: todas las interacciones económicas destinadas a controlar los flujos migratorios, y en las que no solo participan la industria de seguridad y defensa, sino otros actores económicos que incluyen empresas de otros sectores, ONG y organismos oficiales intermediarios.

Inteligencia artificial (IA): Tecnología capaz de aprender de datos y tomar decisiones o predicciones sin intervención directa del ser humano. En las fronteras, se aplica a la identificación biométrica, el análisis de riesgos y la predicción de flujos migratorios.

Opacidad algorítmica: Imposibilidad de comprender cómo o por qué un sistema automatizado llega a una decisión. Obstáculo central para la transparencia y la tutela judicial efectiva.

Privatización de la soberanía: Cesión de funciones públicas —vigilancia, identificación, análisis de riesgos— a empresas privadas, especialmente del sector defensa y tecnológico, que operan bajo lógicas comerciales.

Solucionismo tecnológico: Creencia de que todos los problemas sociales pueden resolverse mediante tecnología. En migraciones, legitima políticas de control automatizado bajo el pretexto de la eficiencia.

Resumen

Entre septiembre de 2016 y agosto de 2019, un consorcio de compañías, centros de investigación e instituciones públicas con base en la Unión Europea (UE) desarrollaron el proyecto iBorderCtrl. Este esfuerzo tecnológico, financiado por la Comisión Europea, tenía como objetivo analizar microexpresiones faciales para evaluar la veracidad de las declaraciones de quienes pretenden acceder a territorio comunitario. El programa fue ferozmente criticado por organizaciones académicas y de derechos humanos por carecer de base científica y por su potencial para institucionalizar la desconfianza y el prejuicio. La Comisión, sin embargo, declaró la experiencia un éxito y un modelo para el futuro de la gestión fronteriza. Varios de sus socios industriales participan hoy en nuevos proyectos de vigilancia financiados por el mismo fondo europeo.

El caso de iBorderCtrl –como el de numerosos proyectos similares financiados a lo largo de toda la UE– constituye un ejemplo de la tercera generación de control migratorio. Tras la construcción de vallas físicas y la tecnificación y externalización del control, los algoritmos y la Inteligencia Artificial (IA) han llegado al mundo de las políticas migratorias acompañadas de una promesa de modernidad. Se trataba de hacer más eficiente la gestión de la movilidad de personas y aportar objetividad allí donde el juicio humano es limitado o sesgado. Con el tiempo, los drones, los sensores, las bases biométricas y los algoritmos de predicción que reemplazan a los muros físicos y configuran las fronteras “inteligentes” han convertido esa promesa en un monumental espejismo. Sometida a un debate público radioactivo, el laboratorio de innovación de la Industria del Control Migratorio privilegia la seguridad sobre la protección, el control sobre la acogida y la sospecha sobre el derecho.

Este informe –elaborado por la Fundación porCausa en colaboración con el Centre Delàs d’Estudis per la Pau– argumenta que esa deriva no es un accidente, sino el resultado de un modelo de gobernanza que ha convertido a la tecnología en una fuente de legitimidad moral. En nombre de la neutralidad, los Estados han delegado en sistemas opacos y privatizados la responsabilidad de decisiones que afectan directamente a los derechos fundamentales de las personas. La inteligencia artificial y la biometría prometen objetividad, pero lo que ofrecen es automatización del sesgo, privatización de la soberanía y erosión de la rendición de cuentas.

Si consideramos los pilares sobre los que descansa esta “frontera inteligente”, el resultado difícilmente podría haber sido otro. Si una opacidad estructural del sistema impide conocer cómo se toman las decisiones, la privatización de las actividades pone en manos de actores particulares sistemas y decisiones que afectan de manera directa al interés público. Y todo ello se produce en un contexto de homogeneidad ideológica que confunde la seguridad con el control. Este trípode sostiene una arquitectura moral en la que la despersonalización, la discriminación algorítmica y la falta de supervisión judicial se entrelazan con intereses industriales y políticos. España, con su Sistema Integrado de Vigilancia Exterior (SIVE) y los proyectos biométricos de Ceuta y Melilla, ha sido un laboratorio de esta evolución europea: pionera en innovación, pero también en opacidad.

La pregunta esencial es qué democracia puede sobrevivir cuando la frontera se convierte en un espacio de excepción permanente. Las tecnologías que hoy clasifican migrantes son las mismas que mañana pueden clasificar ciudadanos. El problema, entonces, ya no es la política migratoria, sino la responsabilidad misma de las instituciones. Cuando la decisión pública se traslada al algoritmo, esta responsabilidad se diluye y el poder se vuelve invisible. La inteligencia de la frontera termina siendo la negligencia de la política.

Frente a esa deriva, este informe propone considerar una idea simple: no se trata de renunciar a la tecnología, sino de gobernarla. La regulación europea sobre inteligencia artificial da un primer paso en la dirección correcta, pero se trata de una respuesta claramente insuficiente. Regular la frontera significa imponer transparencia, garantizar control humano, establecer auditorías independientes y devolver la decisión al ámbito político. La tecnología puede servir a la democracia solo si la democracia conserva la capacidad de decir “no” y “cómo”.

En última instancia, este informe no habla solo de migraciones. Habla del tipo de sociedad que estamos construyendo. Si el miedo justifica la vigilancia y la eficiencia sustituye al derecho, el precio no lo pagarán solo los migrantes: lo pagaremos todos.

Introducción

La frontera que separa Marruecos de la Ciudad Autónoma de Melilla está definida por una contundente estructura física de 12 kilómetros de largo y una altura de entre 7 y 10 metros. En sus tramos más anchos, este entramado de alambradas inclinadas, cables de acero y coronas metálicas “antitrepa” puede llegar a ocupar una anchura de cerca de 10 metros, a los que hay que añadir el foso excavado en el lado marroquí. El conjunto está equipado con torres de vigilancia desplegadas cada medio kilómetro, cámaras de visión diurna y nocturna, y un sistema de sensores que se activan con cualquier movimiento. Drones, cámaras térmicas e iluminadores láser completan el despliegue tecnológico de una de las fronteras más vigiladas del planeta.

Ninguna de estas barreras, sin embargo, fue suficiente para impedir que el 24 de junio de 2022 un grupo de unos 2.000 migrantes intentase acceder irregularmente a territorio español, superando buena parte de los obstáculos físicos y sufriendo una respuesta violenta y desproporcionada por parte de las autoridades marroquíes y españolas. El resultado fue un número oficial de 37 personas fallecidas, 70 desaparecidas y cerca de medio millar de devoluciones en caliente. Al menos uno de estos migrantes falleció en suelo español.[1]

La tragedia de junio de 2022, como tantas otras tragedias similares que se multiplican a lo largo de las fronteras terrestres y marítimas de los países de ingreso alto, no han llevado a las autoridades a reconsiderar la utilidad y la pertinencia de un modelo de control migratorio que ofende los fundamentos éticos y legales de un Estado de derecho. Al contrario, episodios como el de Melilla han sido utilizados para justificar decisiones políticas y presupuestarias que cavan más hondo en el mismo agujero. La versión más contemporánea de este esfuerzo son las llamadas fronteras “inteligentes”: sistemas de detección, seguimiento y cribado de poblaciones en movimiento que depositan una parte creciente de las decisiones en manos de modelos automatizados. Es decir, de una máquina. En el caso de este enclave español en el Norte de África, las primeras versiones de esta frontera entraron en funcionamiento en octubre

[1] Sapoch, Jack et al. «Reconstructing The Melilla Massacre». *Lighthouse Reports*, 29 Noviembre 2022. (Investigación coordinada por Lighthouse Reports con la participación de Fundación porCausa y publicado en diversos medios).

de 2025, con la introducción de un sistema de reconocimiento biométrico y de huellas que será completado más adelante con la implantación de un modelo automatizado para la gestión de solicitudes de visado.

Melilla es solo uno de los muchos escenarios en los que este fenómeno se acelera de forma exponencial. La llamada digitalización de las fronteras describe un proceso que en ningún caso se reduce a los límites físicos que separan a los países, extendiéndose a las regiones de origen y tránsito de los migrantes. En muy poco tiempo, este proceso determinará la estructura de normas y consensos que han regido la gestión de la movilidad humana durante los últimos setenta años. Las decisiones que tomemos con respecto al uso y la regulación de esta tecnología contribuirán a definir las sociedades que seremos en el futuro.

Este informe –elaborado por la Fundación porCausa en colaboración con el Centre Delàs d’Estudis per la Pau– forma parte de una serie de investigaciones sobre la evolución y el papel de la Industria del Control Migratorio en las políticas de gestión de la movilidad humana. Sus contenidos ofrecen un análisis del modo en que la inteligencia artificial y otras formas de tecnología se han convertido en un determinante de las políticas de control migratorio. El documento se abre con una descripción de la evolución de este fenómeno y una fotografía actualizada de las herramientas que se aplican en diferentes fronteras del mundo. La segunda sección analiza por qué las características fundamentales de este modelo –su opacidad, el control por parte de operadores privados y la ausencia de matices ideológicos en su aplicación– maximizan los riesgos asociados al proceso y reducen las oportunidades de poner la tecnología al servicio del interés común. La tercera sección, finalmente, repasa las principales ideas que diferentes actores legales, políticos y técnicos han propuesto para regular este modelo.

El volumen de críticas a un modelo que se expande de manera vertiginosa –y de las propuestas para embridarlo– dan una idea de lo mucho que está en juego. Como ha señalado Otto, la inteligencia de ChatGPT en la que se ha apoyado la elaboración de este informe, "La respuesta [a este desafío] pasa por entender que la IA no tiene voluntad, pero sí puede tener dirección. Su capacidad de contrarrestar el daño depende por completo de cómo la diseñen, quién la entrene y qué límites le impongan. Dicho de otro modo: una IA no puede “rebelarse” contra el mal, pero puede ser construida para reconocerlo, señalarlo y resistirlo."

Ahora bien, esta capacidad depende menos de la tecnología que del marco ético y político que la gobierna: sin él, la IA se limitará a consolidar los sesgos y desigualdades ya presentes en el sistema.

1. La distopía de la frontera “inteligente”

Las fronteras de Europa no siempre son visibles. A lo largo de los últimos años, y a una velocidad que crece de manera exponencial, la introducción de nuevas tecnologías ha revolucionado el modo en que entendemos el control de los territorios, las normas por las que este se rige y las consecuencias que se derivan de todo ello. Bajo la etiqueta de fronteras “inteligentes” –un término evocadoramente virtuoso– se agrupan radares, drones, sensores térmicos, cámaras de reconocimiento facial y bases de datos biométricas capaces de almacenar la identidad de millones de personas. Son las herramientas de una frontera que no necesita alambradas para cumplir su función de vigilar, clasificar y filtrar.[2] Lo que es más importante, son la correa de transmisión de un cambio de paradigma político y legal que amenaza con reconsiderar parte de los principios y normas establecidos por la comunidad internacional tras la Segunda Guerra Mundial.

El proceso de transformación de la frontera ha sido gradual y acumulativo. **La primera generación,** la del muro y la valla, respondía al impulso más elemental de la soberanía: impedir el paso. Desde los años noventa, Europa levantó miles de kilómetros de barreras físicas, muchas de ellas financiadas con fondos europeos. Si en 1989 había seis muros fronterizos en el mundo, en 2022 se contaban setenta y cuatro, y en Europa el vallado se extendía ya por más de 2.000 kilómetros.[3] Hungría, Grecia, Bulgaria o España —con las vallas de Ceuta y Melilla, pioneras en la “Europa fortaleza”— hicieron del acero y la concertina el emblema de una seguridad cada vez más simbólica y menos eficaz.[4]

[2] “Digital Fortress Europe #3: Automation and Surveillance in Fortress Europe” 2023. *European Data Journalism Network - EDJNet.* July 26, 2023 .
[3] María Mateo et al., “La Europa de los muros” *El Confidencial*, 29 noviembre 2023.
[4] Dumbrava, Costica. 2022. “Walls and Fences at EU Borders.” Report PE 733.692. *EPRS | European Parliamentary Research Service*.

La **segunda generación** introdujo un cambio decisivo: el control tecnificado y externalizado. El muro se volvió digital, y la frontera, vertical.[5] A partir de los noventa, la vigilancia terrestre se expandió con sensores, radares y sistemas de comunicación que permitían monitorizar el movimiento antes de que se produjera. El Sistema Integrado de Vigilancia Exterior (SIVE)[6], desplegado por España en 1999 y operado por la Guardia Civil, fue una de las primeras infraestructuras de este tipo en Europa.[7] Sus radares costeros, cámaras térmicas y software de análisis en tiempo real inauguraron una nueva era: la del control a distancia.

En paralelo, la Unión Europea impulsó una red de bases de datos biométricos —SIS, VIS, Eurodac—[8] y creó en 2004 la agencia Frontex, que integró los esfuerzos nacionales en una arquitectura común de control, cada vez más militarizada.[9] La securitización del discurso y la cooperación con la industria armamentística (ver Cuadro 1) consolidaron el tránsito de un modelo simplemente policial a un modelo de defensa estratégica frente a la llegada de terceros. Las fronteras exteriores de la UE, convertidas en masivas operaciones de inteligencia.

Cuadro 1. **La industria del armamento encuentra el filón del negocio del control migratorio**

En 2011, en plena crisis financiera global, el presidente Barack Obama anunció una desaceleración en el gasto en defensa de Estados Unidos, el mayor mercado de la industria armamentística a nivel mundial. Otros países destacados para las empresas de armas, como Francia, Reino Unido, Alemania y España, anunciaron recortes en sus presupuestos militares. Por primera vez desde la caída de la Unión Soviética, el gasto militar mundial se contrajo. Las empresas armamentísticas reaccionaron rápido y apostaron por la diversificación de sus negocios, centrando su atención en los mercados civiles. Varios fabricantes rediseñaron sus

[5] Fundación PorCausa. Informe sobre Externalización. Abril 2024.
[6] Bautista, José. “Fronteras SA: la industria del control migratorio”. *El Confidencial*. 2022.
[7] Andersson, Ruben. “Europe’s Failed ‘Fight’ against Irregular Migration: Ethnographic Notes on a Counterproductive Industry.” Journal of Ethnic and Migration Studies.
[8] Vavoula, Niovi. “Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism.” European Journal of Migration and Law, August 15 2021.
[9] Leonard, Sarah. “The Creation of FRONTEX and the Politics of Institutionalisation in the EU External Borders Policy.” Journal of Contemporary European Research 5, no. 3 (2009): 371-388.

productos y tecnologías militares para entrar en sectores que hasta entonces habían tenido un papel secundario en sus carteras de negocios. El control migratorio y de fronteras se convirtió rápidamente en un nuevo nicho de mercado que la industria armamentística global supo aprovechar. Desde entonces, la militarización de fronteras se ha consolidado como una prioridad para corporaciones como Indra, Thales, ATOS o Escribano, entre otras. Hoy el sector de la defensa constituye un eje de la llamada “reindustrialización” de los países más ricos, lo que sin duda reforzará la lógica securitaria de las políticas migratorias.

Más información:

https://www.publico.es/especiales/contra-el-rearme/negocio-fronteras-defensa-brinda-rearme-nunca.html

La **tercera generación** es la que viene determinada por el algoritmo. Aquí, el control ya no necesita la presencia humana ni el contacto físico. Se anticipa, calcula y decide. El núcleo de este modelo está basado en las tecnologías de análisis predictivo, las herramientas de perfilado automatizado y los sistemas biométricos masivos. La agencia eu-LISA, responsable de gestionar los grandes sistemas europeos de información, coordina la creación del sBMS (Shared Biometric Matching System), que aspira a integrar los datos de más de 400 millones de personas procedentes de terceros países.[10] Proyectos piloto como iBorderCtrl –(2016-2019) que analiza expresiones faciales para determinar la veracidad de un testimonio–[11] o ROBORDER –(2017-2021) que ensaya enjambres de drones autónomos para la vigilancia—[12] ensayan una frontera digital en la que el juicio humano se diluye progresivamente en beneficio de decisiones automatizadas. Las consecuencias son cuestionables (ver Cuadro 2).

[10] AlgoRace y EuroMed Rights. Informe sobre Tecnología digital para el control migratorio en la frontera sur de España. Octubre 2024.
[11] Romano, Andrea. 2023. “Drets Fonamentals I intel·ligència Artificial Emocional En IBorderCtrl: Reptes De l’automatització En l’àmbit Migratori”. *Revista Catalana De Dret Públic*, no. 66, 237-52.
[12] Begault, Lucien. “Automated technologies at EU borders and the future of Fortress Europe.” *Euronews,* 27 Marzo 2019.

Cuadro 2. **Infraestructura tecnológica de control fronterizo y fracaso humanitario.**

El Sistema Europeo de Vigilancia de Fronteras (EUROSUR), operativo desde 2013, es uno de los principales instrumentos tecnológicos de la Unión Europea para reforzar el control de sus fronteras exteriores. Fue presentado como una herramienta destinada a mejorar la cooperación fronteriza, prevenir la inmigración ilegal y salvar vidas en el mar.[13] Sin embargo, más de una década después los datos muestran que no han reducido las muertes en el Mediterráneo[14]. Expertos y académicos cuestionan si su prioridad real es el rescate o la disuasión migratoria, especialmente ante la falta de transparencia sobre su funcionamiento.[15]

Opera como un “sistema de sistemas”, una infraestructura digital interconectada compuesta por Centros Nacionales de Coordinación (NCC) en cada Estado miembro. Estos centros, como el de la Guardia Civil en España, comparten información en tiempo real procedente de radares, satélites, drones y otras tecnologías de detección.[16]

Pese a que se justificó su implementación tras el naufragio de Lampedusa, EUROSUR ha contribuido a desplazar el control europeo hacia el mar abierto y países terceros, donde la responsabilidad de rescate se difumina. Además, plantea riesgos para la protección de datos y colabora con Estados que vulneran derechos humanos.[17]

Así, lo que en teoría debía mejorar la capacidad de respuesta ante emergencias, se ha orientado principalmente a la interceptación y disuasión de migrantes, no a su rescate o protección.

[13] Reglamento (UE) n.º 1052/2013 del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, por el que se crea un Sistema Europeo de Vigilancia de Fronteras (Eurosur). DO L 295 de 6.11.2013

[14] International Organization for Migration (IOM) “*Four Decades of Cross-Mediterranean Undocumented Migration to Europe. A review of the Evidence*.” 2017.

[15] Hayes, Ben y Vermeulen, Mathias. Borderline: The EU's New Border Surveillance Initiatives. A study by the Heinrich Böll Foundation. Transnational Institute, 2012.

[16] García Sacristán, Víctor Manuel. “Cuadernos de la Guardia Civil” Revista De Seguridad Pública, no. 52–2016: 81–102.

[17] ITSS Verona. “*European Border Surveillance System (EUROSUR) and Its Problematic Impact on the Rights of the People on the Move.*” May 2, 2022.

Hasta cierto punto, la frontera se ha desmaterializado. Ya no separa territorios sino categorías de personas. Los algoritmos clasifican en función del riesgo, y el riesgo se define a partir de los datos: lugar de nacimiento, trayecto, nacionalidad, idioma, comportamiento o simplemente “perfil”. La seguridad se vuelve una función matemática. Detrás de esta sofisticación late la convicción inquietante de que la tecnología es neutral[18] y, por tanto, esencialmente justa. Es la ilusión del fetichismo tecnológico, que convierte la innovación en un fin en sí mismo. La frontera inteligente encarna esa fe y, en nombre de la eficacia, los Estados adoptan sistemas automáticos que sustituyen decisiones políticas complejas por resultados computacionales alarmantemente simplificadores.

Esta sustitución tiene consecuencias. Cuando un algoritmo determina quién puede cruzar una frontera, no está interpretando una norma, sino ejecutando una instrucción. La decisión pública se convierte en un proceso técnico, despojado de deliberación, contexto y responsabilidad. El problema no es solo ético; es también institucional. El poder se ejerce sin rostro y sin rendición de cuentas.[19]

En los procesos migratorios, este fenómeno tiene un alcance particular. Los sistemas de evaluación de riesgos y perfilado automatizado (como los basados en el Passenger Name Record, PNR) asignan puntuaciones de riesgo a cada viajero en función de su comportamiento previsto. Esas categorías influyen en la posibilidad de acceso al territorio o en el tratamiento durante el viaje. Dicho de otro modo, en la posibilidad de garantizar la seguridad o, incluso, la propia vida. Una decisión prejudicial de la Corte de Justicia de la Unión Europea en 2022 advirtió de que estas evaluaciones automatizadas podían vulnerar derechos fundamentales por su opacidad y falta de supervisión.[20] En la gestión de llegadas a las Islas Canarias, por ejemplo, la Policía Nacional y la Agencia Europea de Fronteras (FRONTEX) podrían estar utilizando diferentes programas para acceder por la fuerza –y sin autorización judicial– al contenido íntegro de

[18] Amnesty International. 2025. Advocacy Briefing for Defending the Rights of Refugees, Asylum Seekers, and Migrants in the Digital Age. September 12, 2025.
[19] García, Daniel; Llano, Fernando; y Villegas, César. 2025. “Tecnologías de frontera y derecho digital” Ius Et Scientia. Vol. 11. no 1.
[20] Tribunal de Justicia de la Unión Europea. Asunto C-817/19. 21 Junio 2022.

los teléfonos de los migrantes, incluido el software israelí Cellebrite.[21] En ausencia de permiso explícito u orden judicial, esta práctica no solo supone la violación de la intimidad de personas vulnerables que no han cometido ningún delito, sino que esa información obtenida ilegalmente se emplea después para criminalizar a estas mismas personas en procedimientos plagados de irregularidades.[22]

Lo mismo ocurre con los sistemas de reconocimiento facial utilizados por las fuerzas de seguridad. En España, el programa ABIS, desarrollado por la empresa Thales, gestiona más de cuatro millones de registros faciales y se ha usado en cientos de investigaciones criminales.[23] Pese a tratarse de una información extremadamente sensible, su funcionamiento carece de auditoría pública y su entrenamiento en bases de datos policiales plantea un riesgo evidente de sesgo racial y discriminación.

Este ejemplo forma parte de un patrón que ha convertido el caso español en uno de los campos de ensayo del modelo. Desde el SIVE hasta los proyectos de frontera inteligente en Ceuta y Melilla, España ha actuado como laboratorio europeo de control migratorio.[24] Nuestro país combina la condición de frontera exterior con una estructura tecnológica avanzada y una red de contratos con grandes corporaciones de defensa y tecnología. El resultado es un ecosistema que realiza un considerable ejercicio de innovación tecnológica y política... en el contexto de una preocupante opacidad. La información pública sobre estos contratos está atomizada y difícil de rastrear. Como ha podido comprobar esta investigación (ver Cuadro 3), muchas adjudicaciones se realizan por procedimiento negociado sin publicidad (sin concurso público y sin desglosar detalles técnicos), bajo el argumento de la urgencia o la seguridad nacional. Las empresas beneficiarias son casi siempre las mismas —nombres como

[21] Base de datos de contratos públicos de tecnología de frontera del Estado español (contratos adjudicados entre el 1 de enero de 2018 y el 31 de octubre de 2025), elaborada por la Fundación porCausa y Centre Delàs, así como fuentes de la Comisaría General de Información de la Policía Nacional y de la Guardia Civil consultadas al respecto. Esta investigación ha podido localizar varios contratos para obtener o actualizar Cellebrite, a destacar uno para la Comisaría General de Extranjería y Fronteras, con número de expediente Z21IN002/R20.

[22] Carril-Zerpa, Isabella y Ndiaye, Ngone. 2024. “”¿Quién es el Capitán del Cayuco?”, la pregunta detrás del creciente número de migrantes en las cárceles españolas.” Público. 10 Octubre 2024.

[23] Pascual, Manuel G. “La Policía española ya usa en sus investigaciones un sistema automático de reconocimiento facial.” El País, 28 mayo 2024.

[24] María, García. “Beni Enzar estrena la primera fase de la futura frontera inteligente.” El Faro de Melilla, 15 Junio 2024.

Indra, Escribano o Thales— y el lenguaje de los pliegos se ha vuelto cada vez más ambiguo, con expresiones genéricas como “sistemas avanzados de observación” o “soluciones de inteligencia artificial aplicada”. Esta privatización de la soberanía no es un accidente, sino un síntoma.

Cuadro 3. **Un análisis de los contratos públicos del Estado español en este ámbito.**

Como parte de la investigación que ha sustentado este informe se han identificado y analizado cerca de 700 contratos públicos del Estado español destinados a este sector y clasificados en tres niveles de relevancia:[25]

· Categoría 1: Aquellos empleados directamente en control fronterizo.

· Categoría 2: Aquellos implementados en control de frontera pero también en otros ámbitos, como la lucha contra el narcotráfico y el crimen organizado.

· Categoría 3: Aquellos que, en base a fuentes humanas, tendrían aplicación y uso en frontera y control migratorio pero cuyo uso no ha sido desvelado o confirmado por fuentes oficiales.

El total de gasto analizado asciende a **541 millones de euros, distribuidos en 674 expedientes de contratación.** Los contratos de Categoría 1 concentran casi la mitad del gasto (48,14%), seguidos por los de Categoría 2 (30,85%) y los de Categoría 3 (21,01%). Por categorías, el gasto se orienta principalmente hacia Sistemas de Vigilancia y Detección, que representan el 32,20% del total, destacando los sistemas integrados de vigilancia fronteriza. En segundo lugar, se sitúan los sistemas de monitorización y control de flujos de personas (17,22%), esenciales para el Entry/Exit System y Schengen Recast. Les siguen los contratos de formación y asistencia técnica (14,88%) y los sistemas de monitorización y ciberinteligencia (12,61%).

Al desglosar por relevancia, los contratos de nivel 1 se concentran en **vigilancia y detección (57,09%)**, especialmente en sistemas integrados como SIVE, ABC o fronteras “inteligentes”, así como en sistemas de control de flujo de personas. En nivel 2 destacan los servicios de formación (36,95%) y los sistemas de análisis e inteligencia de la información (31,43%), con peso notable de la ciberinteligencia y

[25] Base de datos de contratos públicos de tecnología de frontera del Estado español (contratos adjudicados entre el 1 de enero de 2018 y el 31 de octubre de 2025), elaborada por la Fundación porCausa y Centre Delàs.

biometría. En el nivel 3 de relevancia predominan los contratos de control de acceso y vigilancia de puertos (49,77%), seguidos por infraestructuras tecnológicas, comunicaciones y ciberseguridad.

En cuanto a los procedimientos de contratación, el que concentra la mayor parte del gasto total (44,10%) es el **negociado sin publicidad,** con un gasto de más de 238 millones repartidos en 166 expedientes. Esto muestra que la mayor parte del volumen económico se adjudica mediante **procedimientos con competencia limitada o sin concurso público.** En los contratos de Categoría 1, el procedimiento **negociado con publicidad** es el más importante en cuanto al gasto, conformando el 31,92% del gasto en menos del 10% de los expedientes.

El gasto está altamente concentrado en unos pocos órganos de contratación: los cinco principales acumulan casi el 80% del total. Destacan la Subdirección General de Gestión Económica y Patrimonial (21,84%), la Jefatura de Asuntos Económicos de la Guardia Civil (19,71%) y la Subdirección General de Infraestructuras y Medios para la Seguridad (15,80%), las tres pertenecientes al Ministerio del Interior. No obstante, esto no nos dice mucho sobre el uso o los destinatarios del material adquirido y los servicios contratados, ya que estos organismos son los encargados de la gestión económica y seguramente adquieran el material para después distribuirlo.

En cuanto a las empresas adjudicatarias –sin considerar uniones temporales de empresas (UTE)–, **las diez principales absorben el 72,5% del gasto, liderando el ránking Escribano, Telefónica y Thales.** Si se incorporan las UTE, Telefónica pasa a encabezar el ranking con más de 107 millones de euros (20,47%), seguida de Thales e Indra, que junto con Telefónica concentran el 45,97% del total. Considerando únicamente los contratos de Categoría 1, pasa a liderar Escribano con un 22,03%, seguida de Thales, Indra, Etel y Telefónica.

El conjunto de estos contratos refleja un **gasto altamente concentrado, tanto por categorías como por empresas y procedimientos,** con un peso significativo de tecnologías de vigilancia, control fronterizo y ciberinteligencia, infraestructura tecnológica y sistemas biométricos. Y con especial énfasis en capacidades asociadas a seguridad interior, control migratorio y análisis avanzado de datos.

Un cambio de paradigma

El rasgo más disruptivo de esta tercera generación no es su derivada tecnológica, sino la política, que constituye un verdadero cambio de paradigma. La automatización permite a los Estados delegar en la máquina decisiones que afectan directamente a los derechos fundamentales de las personas.[26] Lo que antes era una función de Estados sujetos a normas de comportamiento y control –vigilar, admitir, proteger–, se traslada de manera creciente a entidades cuya lógica responde al beneficio privado y no al interés general. Con estas tecnologías se diluye la responsabilidad y la frontera se vuelve una infraestructura privada financiada con dinero público.

Cuando una solicitud de asilo, una autorización de entrada o una orden de expulsión se basan en sistemas automáticos, el principio de igualdad ante la ley se sustituye por una lógica de cálculos algorítmicos. Y cuando esos cálculos están protegidos por el secreto industrial, la propiedad intelectual o una protección más o menos justificada de la seguridad nacional, el ciudadano deja de tener acceso a los criterios por los que sus derechos y aspiraciones son evaluados. La opacidad técnica se convierte en opacidad democrática. Alemania, por ejemplo, utiliza un sistema de identificación de dialectos basado en IA para verificar el origen de los solicitantes de asilo. Solo acierta en el 80% de los casos y sus errores pueden llevar a la denegación de solicitudes.[27]

El Tribunal Supremo español –en una sentencia de septiembre de 2025, en respuesta a una demanda de la organización de transparencia Civio–[28] reconoció por primera vez el derecho a acceder al código fuente de un algoritmo utilizado por la Administración en la gestión de servicios públicos.[29] El fallo subrayó que la transparencia tecnológica es una condición para garantizar la legalidad de las decisiones automatizadas. Sin embargo, ese principio aún no se aplica en los sistemas migratorios ni en los programas europeos de frontera, muchos de los cuales operan bajo

[26] Arce Jiménez, Carlos. 2023. “Las nuevas tecnologías en las políticas migratorias y de control de fronteras españolas y europeas. Un reto para la vigencia de los derechos fundamentales.” Estudios de Deusto. Revista de Derecho Público 71, nº2: 15-49
[27] Romano. “Drets Fonamentals I intel·ligència Artificial Emocional En IBorderCtrl: Reptes De l’automatització En l’àmbit Migratori”.
[28] Civio. 2025. “Civio Abre Camino En La Transparencia Algorítmica: El Supremo Condena al Gobierno a Entregar El Código Fuente De BOSCO.” 17 Septiembre 2025.
[29] Tribunal Supremo, Sala de lo Contencioso-Administrativo, Sección Tercera, Sentencia núm. 1119/2025, 11 septiembre 2025 (Recurso de Casación 7878/2024).

normas de confidencialidad propias del ámbito de la seguridad y la defensa.

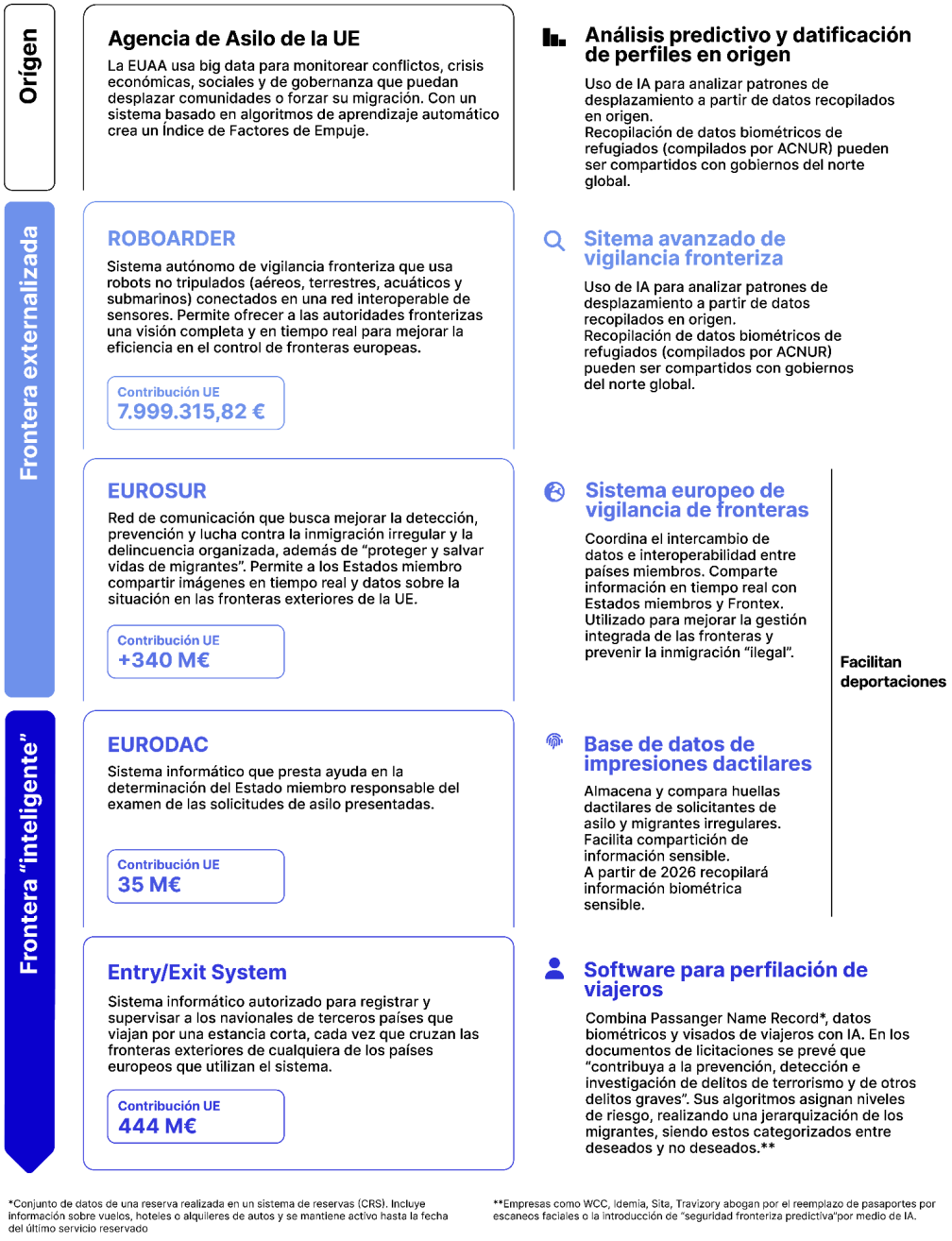
Esa es la paradoja de la frontera inteligente: mientras promete un control –el de los movimientos–, erosiona otro –la supervisión democrática bajo la que estos deberían producirse–. Los algoritmos no solo ejecutan órdenes, sino que también definen prioridades, establecen criterios de sospecha y, en última instancia, determinan quién merece protección y quién no.[30] Mientras tanto, esta misma tecnología parece ser incapaz de resolver los cuellos de botella que retrasan la gestión de las solicitudes de asilo, por ejemplo.

La digitalización del control migratorio anticipa un desafío político de mayor envergadura. Lo que hoy se aplica a los migrantes —el uso de sistemas automatizados, la falta de rendición de cuentas y la gestión opaca de datos sensibles— puede extenderse al resto de la ciudadanía. La frontera deja de ser un lugar geográfico para convertirse en un dispositivo de control por parte del gobierno, como estamos comprobando en directo en el caso de los Estados Unidos.[31] Por esta razón, la discusión no es solo sobre derechos de los migrantes, sino sobre el tipo de Estado que Europa está construyendo. Si la legitimidad democrática descansa en la transparencia, la participación y el control público, el avance de una gobernanza algorítmica plantea una pregunta fundamental: ¿quién vigila a la máquina que vigila?

El sueño de la frontera inteligente es, en realidad, una distopía eficiente. Y su eficacia, paradójicamente, no se mide en vidas salvadas ni en derechos garantizados, sino en el número de operaciones completadas sin error aparente. La tecnología promete seguridad, pero lo que produce es una peligrosa obediencia automática.

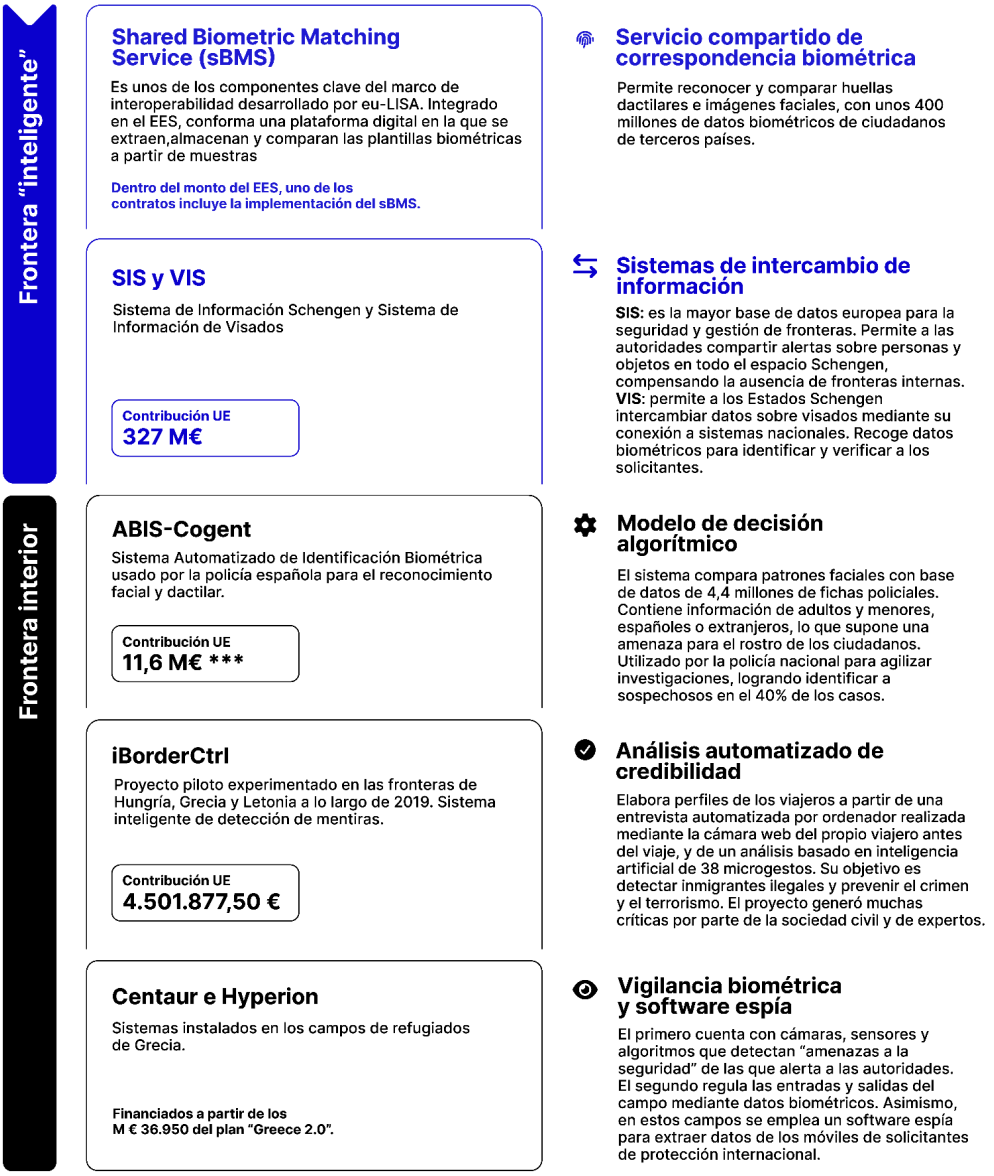
[30] Chandler, Caitlin. “Inside the Black Box of Predictive Travel Surveillance.” WIRED, January 13, 2025.
[31] Arce Jiménez, C. “Las nuevas tecnologías en las políticas migratorias y de control de fronteras españolas y europeas. Un reto para la vigencia de los derechos fundamentales.”

Cartografía de las fronteras “inteligentes”: Ejemplos destacados del uso de tecnologías en la ruta migratoria hacia Europa



*Conjunto de datos de una reserva realizada en un sistema de reservas (CRS). Incluye información sobre vuelos, hoteles o alquileres de autos y se mantiene activo hasta la fecha del último servicio reservado

**Empresas como WCC, Idemia, Sita, Travizory abogan por el reemplazo de pasaportes por escaneos faciales o la introducción de “seguridad fronteriza predictiva”por medio de IA.



Entre 2014 y 2020, eu-LISA y Frontex invirtieron respectivamente 1.465 millones de euros y 434 millones de euros.

Una vez dentro de la Unión Europea, el acceso a derechos y servicios básicos se ven comprometidos por los mecanismos de perfilación y datificación realizados a lo largo de la ruta migratoria.

Toda la información contenida en esta tabla se ha recogido de las páginas oficiales de los programas concretos, documentos del Parlamento y de la Comisión Europea, la base de datos de la Fundación porCausa para la presente investigación e informes académicos citados en la misma. Concretamente ha sido de gran ayuda el artículo: Neither opaque nor transparent para rastrear el flujo del dinero, en la mayoría de las ocasiones oculto por las autoridades.

***Cifra aproximada calculada a partir del valor de los contratos adjudicados a Thales para el programa ABIS, recogidos y analizados en la base de datos de la Fundación porCausa a propósito de esta investigación.

2. Un sistema opaco, privatizado e ideológicamente dirigido

La literatura especializada consultada para este informe ha identificado seis problemas recurrentes que se derivan del cambio de paradigma que hemos descrito. Juntos, estos factores definen la arquitectura moral de la frontera tecnológica europea:

- La despersonalización de la frontera convierte la decisión pública en una operación mecánica;
- la discriminación algorítmica amplifica prejuicios y exclusiones;
- la manipulación de la información transforma los datos en instrumentos de represión y deportación;
- la falta de control judicial deja sin defensa a quienes son objeto de estas decisiones;
- la instrumentalización de las personas migrantes convierte su sufrimiento en laboratorio;
- el vínculo con la industria armamentística garantiza que la seguridad siga siendo un negocio antes que un derecho.

Las próximas páginas analizan estos desafíos de acuerdo con tres de sus características fundamentales: la opacidad, el control privado y la homogeneidad ideológica. La consecuencia es un sistema de gestión de fronteras sin rostro ni control democrático pleno.

Opacidad: la frontera invisible del conocimiento público.

Las nuevas formas de frontera se construyen en los márgenes de la transparencia. La información sobre sus costes, funcionamiento y resultados es escasa o directamente inaccesible. Como muestra la sección anterior, buena parte de los contratos públicos se tramitan bajo fórmulas de “procedimiento negociado sin publicidad”, amparadas en la urgencia o en razones de seguridad nacional.[32] Los pliegos técnicos, cuando existen, se redactan en un lenguaje deliberadamente ambiguo —“sistemas de análisis de riesgo”, “soluciones de inteligencia aplicada”, “tecnologías de respuesta avanzada”— que impide conocer su alcance real.

Esta opacidad institucional tiene una consecuencia directa: las tecnologías que afectan a derechos fundamentales escapan al control de quienes las financian y padecen. El Estado gasta millones de euros en sistemas que clasifican personas, pero no rinde cuentas sobre sus criterios de decisión. En la práctica, los algoritmos son tratados como secretos de Estado o, peor aún, como propiedad privada.

En este modelo de colonialismo de datos (data colonialism), la extracción, acumulación y apropiación de datos se convierte en un mecanismo de poder que opera sin rendición de cuentas. En el ámbito fronterizo, esta lógica permite que empresas y Estados capturen datos sensibles de poblaciones vulnerables sin supervisión democrática, reproduciendo relaciones de dependencia y asimetría informativa.[33]

La mencionada sentencia del Tribunal Supremo español que en septiembre de 2025 reconoció el derecho ciudadano a acceder al código fuente de los algoritmos públicos fue un punto de inflexión. El fallo –basado en la Ley 19/2013 de Transparencia y buen gobierno– afirma que el acceso a la información tecnológica “adquiere especial relevancia ante los riesgos que entraña el uso de las nuevas tecnologías en el ejercicio de las potestades públicas”. El Supremo resolvió el caso obligando a la Administración a entregar a la Fundación Civio el código fuente de la aplicación empleada

[32] Base de datos de contratos públicos de tecnología de frontera del Estado español (contratos adjudicados entre el 1 de enero de 2018 y el 31 de octubre de 2025), elaborada por la Fundación porCausa y Centre Delàs.
[33] Couldry, Nick & Mejias, Ulises A. “The Costs of Connection: How Data Are Colonizing Human Life and Appropriating It for Capitalism”. Social Forces. Vol 99, Issue 1, Page e6. Septiembre 2020.

para determinar si los solicitantes cumplían los requisitos de vulnerabilidad energética.[34] Sin embargo, esta doctrina aún no se ha extendido al ámbito migratorio, donde los sistemas automatizados —como el reconocimiento facial o los algoritmos de predicción de riesgo— operan sin auditorías independientes ni obligación de ser explicadas.

La opacidad de estos modelos impide conocer sus tasas de error o los criterios con que clasifican los rostros, lo que genera un círculo vicioso: el sesgo se convierte en norma, y la norma en procedimiento. Esta ausencia de información pública facilita dinámicas de racialización algorítmica, en la que sistemas que se presentan como neutrales reproducen jerarquías raciales históricas mediante patrones de entrenamiento sesgados y procesos de clasificación opacos.[35] El futuro en el que una máquina determine, por ejemplo, el destino de un solicitante de asilo de acuerdo con criterios que este no puede conocer o cuestionar, está más cerca que nunca.

La ausencia de transparencia no es solo técnica, sino también política. La frontera se ha convertido en un espacio de excepción donde la rendición de cuentas se suspende en nombre de la seguridad. Y esa suspensión, lejos de ser transitoria, se ha institucionalizado. Lo que antes era una medida extraordinaria —vigilar, interceptar, deportar— se ha normalizado bajo una apariencia de neutralidad tecnológica. Esta despersonalización de la decisión pública, al sustituir la deliberación humana por la ejecución mecánica, vacía de contenido el principio de responsabilidad democrática. La transparencia no solo fortalece la rendición de cuentas, sino que mejora la seguridad del propio software al permitir su revisión por actores independientes.

El Tribunal Europeo de Derechos Humanos fija en su Sentencia 18030/11 los requisitos para reconocer el derecho de acceso a información pública,[36] aunque la mencionada Ley de Transparencia lo reconoce de forma más amplia.

---

[34] Del Castillo, Carlos. 2025. “El Supremo Zanja Que Los Algoritmos Públicos Deben Ser Transparentes En Un Fallo Clave Para La Inteligencia Artificial.” eldiario.es, 18 Septiembre 2025.
[35] Benjamin, Ruha. “Race After Technology: Abolitionist Tools for the New Jim Code”. Polity Press. 2019.
[36] European Court of Human Rights. Magyar Helsinki Bizottság v. Hungary. 8 Noviembre 2016 Application no. 18030/11.

Privatización: la soberanía externalizada.

La segunda característica estructural del sistema es la privatización. El control migratorio europeo es hoy un negocio transnacional en el que participan corporaciones tecnológicas, contratistas de defensa y consultoras especializadas. Entre enero de 2018 y octubre de 2025, por ejemplo, el grueso de los contratos españoles en materia de vigilancia fronteriza recayeron en solo tres empresas: Escribano, Telefónica y Thales.[37] El fenómeno se repite a escala europea con actores como Airbus, Leonardo, Sopra Steria, Idemia o Atos.[38]

Esta concentración no solo deriva en poder económico, sino en la capacidad de definir las políticas públicas bajo las que estos actores operan. Las empresas no se limitan a ejecutar contratos, sino que codiseñan los sistemas y, en muchos casos, los explotan en régimen de colaboración público-privada. La agencia europea eu-LISA, responsable de los sistemas de información Schengen, ha subcontratado a consorcios privados para desarrollar y mantener bases de datos biométricas, entre ellas el sBMS, que almacenará más de 400 millones de registros de huellas e imágenes faciales.[39]

La captura masiva de información personal, especialmente de grupos con menor poder político, se convierte en un recurso estratégico controlado por corporaciones y agencias transnacionales, de nuevo reproduciendo la lógica del colonialismo de datos.

En este modelo, la soberanía se vuelve negociable. Las decisiones sobre vigilancia, almacenamiento y tratamiento de datos ya no dependen solo de los Estados, sino de corporaciones con sedes en varios países y regímenes jurídicos distintos.[40] Cuando un algoritmo de perfilado de pasajeros es desarrollado por una empresa israelí, operado desde

[37] Base de datos de contratos públicos de tecnología de frontera del Estado español (contratos adjudicados entre el 1 de enero de 2018 y el 31 de octubre de 2025), elaborada por la Fundación porCausa y Centre Delàs.
[38] Valdivia, Ana, et al. 2022. «Neither Opaque Nor Transparent: A Transdisciplinary Methodology To Investigate Datafication At The EU Borders». Big Data & Society 9 (2).
[39] AlgoRace y EuroMed Rights. Informe sobre Tecnología digital para el control migratorio en la frontera sur de España.
[40] Chandler, C. “Inside the Black Box of Predictive Travel Surveillance.”

servidores alemanes y aplicado en aeropuertos españoles, ¿quién es responsable si este discrimina o se equivoca?

La privatización introduce además un nuevo tipo de secreto, el comercial. Las empresas invocan la protección de la propiedad intelectual para impedir el acceso a los códigos, los modelos de entrenamiento o las métricas de error. La frontera inteligente se convierte así en un enigma jurídico: el Estado no puede fiscalizar lo que ha delegado, y la ciudadanía no puede cuestionar lo que no conoce.

En España, los contratos para la frontera inteligente de Ceuta y Melilla —que incluyen el reconocimiento facial y registro biométrico de entradas y salidas— fueron adjudicados en 2021 a consorcios liderados por Thales y Telefónica, e implementados por empresas como TRC,[41] con un presupuesto conjunto superior a 4 millones de euros.[42] Ninguno de los pliegos detalla los mecanismos de protección de datos o los criterios de auditoría. El proyecto se presentó como una “apuesta por la seguridad inteligente”, un eufemismo que, como tantas veces, sustituye la política por la ingeniería.

Esta privatización también ha acentuado la racialización algorítmica.[43] Los algoritmos comerciales utilizados para reconocimiento facial y análisis de riesgo reproducen, amplifican y normalizan prejuicios raciales y culturales presentes en sus bases de entrenamiento, a través de procesos automatizados cuya lógica resulta difícil de auditar.[44]

Homogeneidad ideológica: el consenso de la seguridad.

El tercer rasgo de este modelo es su homogeneidad ideológica. La frontera inteligente no se impone por la fuerza, sino por el consenso. Políticos de

[41] TRC. 2025. Ceuta y Melilla dan el salto a la "Frontera Inteligente" con la tecnología de TRC
[42] Planas Bou, Carles. “Expertos denuncian el plan del Gobierno para usar reconocimiento facial en Ceuta y Melilla", El Periódico, 13 Enero 2022.
[43] Eubanks, Virginia. “Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor”. St. Martin’s Press. 2018
[44] Vukov, Tamara. “Target Practice. The Algorithmics and Biopolitics of Race in Emerging Smart Border Practices and Technologies” Transfers. Vol. 6(1), Spring 2016: 80-97

distinto signo, tecnócratas, medios y empresas comparten un marco mental que equipara la seguridad con el control derivado de la tecnología. Es la lógica del “solucionismo” tecnológico[45]: ante cualquier desafío complejo —migración, pobreza, desinformación— la respuesta es un sistema automatizado que promete eficacia y neutralidad[46].

Esta narrativa ha impregnado el discurso institucional europeo. Documentos de la Comisión Europea y del Consejo de la UE justifican el gasto en tecnologías de frontera bajo la idea de “salvar vidas” y “prevenir tragedias”. Sin embargo, múltiples investigaciones han mostrado que los sistemas de detección temprana no se utilizan prioritariamente para operaciones de rescate,[47] sino para interceptar embarcaciones y facilitar devoluciones.[48] Esta priorización operativa evidencia una dimensión necropolítica, en tanto que las políticas europeas deciden, mediante infraestructura tecnológica, qué vidas merecen protección y cuáles son tratadas como amenazas gestionables. La seguridad, en este contexto, se convierte en un valor absoluto que justifica cualquier medio.

A todo lo anterior se suma una convergencia de intereses. Las agencias europeas (Frontex, eu-LISA), los Estados miembros y las empresas proveedoras comparten una visión unidireccional: más tecnología equivale a más control; y más control, a más legitimidad. En una suerte de profecía autocumplida, cada nuevo sistema del complejo seguridad-industria[49] que muestra fallos no provoca una reconsideración del modelo, sino la demanda de otro más avanzado tecnológicamente.[50]

En este ecosistema ideológico, la crítica es descartada como ingenuidad o como amenaza. Los informes que alertan sobre los sesgos raciales en los algoritmos de reconocimiento facial, o sobre la discriminación algorítmica en las evaluaciones de riesgo, son recibidos con el mismo argumento: la

---

[45] Morozov, Evgeny. To Save Everything, Click Here: The Folly of Technological Solutionism. New York: PublicAffairs, 2013.
[46] Cancela, Ekaitz. Despertar del sueño tecnológico: Crónica sobre la derrota de la democracia frente al capital. Madrid: Editorial Akal, 2019.
[47] Fotiadis, Apostolis. “Just 0,07% of 819M border budget to Greece earmarked for Search and Rescue”. We Are Solomon, 15 Junio 2023.
[48] Hayes, Ben y Vermeulen, Mathias. Borderline: The EU's New Border Surveillance Initiatives. A study by the Heinrich Böll Foundation. Transnational Institute, 2012.
[49] Calvo Rufanges, Jordi; Bohigas, Xavier; de Fortuny, Teresa; Ruiz Benedicto, Ahinoa. La Transformación del Complejo Militar-Industrial. Centre Delàs d’Estudis per la Pau & NOVACT - International Institute for Nonviolent Action. 2017.
[50] InfoMigrants, “En Europe, les migrants premières victimes de l’intelligence artificielle”. 11 Febrero 2025

tecnología se perfeccionará. En palabras del ministro español del Interior en 2025, Fernando Grande-Marlaska, "la frontera inteligente garantiza una gestión más ágil, segura y eficiente que va a beneficiar a la población de Melilla".[51] El problema, sin embargo, no es técnico, sino político: no se trata de mejorar la herramienta, sino de considerar para qué se utiliza.

El caso del proyecto europeo iBorderCtrl, que pretendía analizar microexpresiones faciales para detectar mentiras en entrevistas de frontera, ilustra bien esta deriva. El programa fue criticado por organizaciones de derechos humanos y académicas por carecer de base científica y por su potencial para institucionalizar la desconfianza y el prejuicio.[52] A pesar de las controversias, el proyecto se desarrolló entre septiembre de 2016 y agosto de 2019, y fue aclamado por la Comisión Europea como todo un éxito.[53] Varios de sus socios industriales participan hoy en nuevos proyectos de vigilancia financiados por el mismo fondo europeo (ver Cuadro 4).

Cuadro 4. **El dinero público europeo como motor de la tecnología del control migratorio.**

Los programas de investigación e innovación de la UE han jugado un papel clave en la concepción y el desarrollo de las nuevas tecnologías de control migratorio. Si en el pasado se desarrollaron proyectos como METICOS, PROMENADE, PROFILE o COMPASS2020, estos son algunos ejemplos actuales destacados:

· Mobility Analytics of Borders (MOBAN): se trata de un proyecto de la Comisión Europea destinado a predecir presiones migratorias, mediante la recopilación de datos sobre flujos migratorios en las fronteras terrestres y aéreas.

· BorderForce: Un programa que pretende apoyar las operaciones relativas al control y gestión de fronteras, mejorando las capacidades de vigilancia en tiempo real mediante el uso de torres de vigilancia versátiles con

[51] La Moncloa “Grande-Marlaska: "La frontera inteligente garantiza una gestión más ágil, segura y eficaz que beneficiará a la población de Melilla"”. 5 Febrero 2025.
[52] Romano. “Drets Fonamentals I intel·ligència Artificial Emocional En IBorderCtrl: Reptes De l’automatització En l’àmbit Migratori”
[53] Comisión Europea, “Smart lie-detection system to tighten EU's busy borders”, Research and Innovation. 24 Octubre 2018.

función antidrones y sensores autónomos. Se desarrollará entre noviembre de 2024 y abril de 2027.

· Early Warning and Forecasting System: Un mecanismo desarrollado por la Agencia Europea de Asilo para predecir la llegada de solicitantes de asilo con hasta tres semanas de antelación con el objetivo de preparar a los Estados ante posibles presiones sobre sus sistemas de asilo (actualmente, incluye datos actualizados hasta el primer trimestre de 2025).

Desde el punto de vista geopolítico, la homogeneidad ideológica plantea nuevas razones para la preocupación. Europa adopta, de manera acrítica, tecnologías y modelos importados de países con larga experiencia en control poblacional, como Israel (ver Cuadro 5). En 2023, el Ministerio de Defensa español adquirió nueve sistemas de drones SIRTAP, diseñados para operaciones de inteligencia y vigilancia.[54] La frontera se convierte así en un espacio de transferencia tecnológica donde las lógicas del conflicto se aplican a la gestión de la movilidad.

Cuadro 5**. Israel, una potencia tecnológica en el control migratorio.**

Diversos avances de tecnología militar encuentran en el control migratorio un nuevo nicho de mercado. Un país cuya industria destaca en este sentido es Israel.

En septiembre de 2025, el Gobierno español aprobó el embargo de armas a Israel, que incluyó la prohibición de importar productos militares procedentes de ese país. Esta decisión abrió un discreto debate en el seno de las instituciones con competencias en materia de frontera: parte de la tecnología de control migratorio de España procede de empresas israelíes, conocidas a nivel mundial por su vanguardismo armamentístico y la probada eficacia de sus productos militares contra objetivos palestinos o en sus 64 kilómetros de muro terrestre equipados con sensores y armas automatizadas. Varias fuentes de las Fuerzas y Cuerpos de Seguridad consultadas restan importancia a este embargo (en cuanto a su capacidad de limitación de la importación de productos

[54] Agencias. “Sirtap, el primer dron militar español que volará a finales de 2025”, La Vanguardia. 17 Junio 2025.

israelíes destinados al control migratorio) porque a menudo estos productos israelíes se comercializan a través de intermediarios con sede fiscal en España, como OnRetrieval Group, Onrecovery, Excem Grupo 1971 o Dars Telecom.

Entre estos proveedores israelíes hay empresas como Hatchwell, que entre otros proporciona tecnología de control de pasajeros y fronteras y de intercepción de comunicaciones a la Guardia Civil, la Policía Nacional y AENA, el gestor aeroportuario español. En ciudades como Huelva, Tarragona o Ceuta, los puertos cuentan con tecnología PIDS (vallas inteligentes sensorizadas) de la empresa Magal Security Systems. También existe una estrecha relación de cooperación entre empresas destacadas de la Industria del Control Migratorio de España y compañías israelíes. Un ejemplo destacado es el de Telefónica y su partnership con Mellanox Technologies, que desarrolla hardware y software de control migratorio. Los radares del SIVE cuentan con componentes de radar de IAI ELTA.

Ampliando el foco, esta dinámica también se reproduce a nivel europeo, tanto en otros Estados miembro como en Frontex, que incluso cuenta con los drones HERON de la empresa IAI para sus misiones de reconocimiento e interceptación en el Mediterráneo.

España no es el único país que adquiere tecnología antimigratoria israelí: en la lista destacan Estados Unidos, Reino Unido, Suiza o Grecia, entre otros.

Fuente: Información recabada por la Fundación porCausa a través de entrevistas con una veintena de agentes de la Policía Nacional, la Guardia Civil, los ministerios del Interior, Asuntos Exteriores, Defensa, Inclusión, Seguridad social y Migraciones que accedieron a hablar bajo la condición de no ser identificadas.

Cada uno de estos factores sugiere que la frontera inteligente no solo refleja un consenso político, sino también un modelo de sociedad. La desconfianza hacia el otro, la fe en la automatización y la subordinación del derecho a la eficiencia son los tres ingredientes de una nueva gobernanza autoritaria. Como advertía Amnistía Internacional en un reciente informe, “las preocupaciones en torno a los derechos digitales y los derechos de los solicitantes de asilo, los refugiados y los migrantes están cada vez más interrelacionadas y deben considerarse dentro de una tendencia más amplia de criminalización de las vidas de las personas

marginadas que a menudo se ve posibilitada y facilitada por las nuevas formas de tecnología”.[55] Dicho de otro modo, la digitalización del control migratorio no solo amenaza los derechos de los migrantes, sino los fundamentos mismos de la democracia europea.

Un sistema sin rostro ni control democrático.

Cuando la vigilancia se vuelve ubicua y la decisión se automatiza, la frontera deja de tener geografía. Está en el aeropuerto, en la base de datos, en el algoritmo que decide si un nombre activa una alerta. El control se ha hecho omnipresente y anónimo.

Esta estructura sin rostro crea una paradoja moral: todos intervienen, pero nadie es responsable de sus consecuencias.[56] Cuando un algoritmo niega una solicitud de asilo o clasifica erróneamente a una persona como “riesgo potencial”, no hay un funcionario que responda, un político que asuma el error o un juez que lo revise. La culpa se diluye en la cadena técnica.

Derya Ozkul, profesora de la Universidad de Warwick, lo define como una “objetividad construida”.[57] Las decisiones que afectan a vidas humanas son tomadas por sistemas sin conciencia, y corregidas —si acaso— por procesos burocráticos diseñados para validar su resultado. Los migrantes se convierten así en conejillos de indias de una tecnología que, en nombre del progreso, ensaya nuevas formas de exclusión.[58]

Esta es la lógica que hace de la frontera inteligente una distopía funcional: cuanto más falla, más se desarrolla; cuanto más excluye, más se justifica. Su eficacia no se mide por los derechos garantizados, sino por los riesgos controlados. El sistema resultante es, más que un conjunto de tecnologías, una forma de gobierno. Un gobierno sin rostro, basado en la delegación, la

[55] Amnistía Internacional. “La frontera digital: Migración, tecnología y desigualdad”. 21 Mayo 2024
[56] Muñoz-Torres, Gabriela y Gutiérrez-Luna, Susana. “Desvanecimiento de la frontera como límite. Imaginario del borde como espacio público físico y virtual” Revista de Arquitectura, vol. 21, núm. 2, pp. 33-43, 2019
[57] Ozkul, Derya. “Constructed Objectivity in Asylum Decision-Making Through New Technologies” Journal of Ethnic and Migration Studies 51 (14) (2025): 3629–48.
[58] Desmarais, Anna. “Así Utiliza La UE La Tecnología De IA En Las Fronteras Europeas: Reconocimiento De Voz Y Vigilancia.” Euronews, 26 Marzo 2025.

opacidad y la inercia. Donde el verdadero peligro no es la tecnología, sino la facilidad con la que nos acostumbramos a su lógica.

Cuando la excepción se normaliza, la democracia pierde su músculo cívico. El control deja de ser un acto político y se convierte en una variable técnica. Esa es la trampa del “solucionismo” tecnológico: creer que podemos gestionar los conflictos humanos con el lenguaje de la eficiencia de las máquinas. Frente a ello, la transparencia y la rendición de cuentas no son un obstáculo, sino el único antídoto posible. El desafío no consiste en detener el avance tecnológico, sino en devolverlo al ámbito de lo político, donde las decisiones puedan ser discutidas, supervisadas y, si es necesario, corregidas.[59]

3. Regulación tecnológica: el desafío de humanizar la frontera

Las transformaciones tecnológicas que hemos analizado no son neutras ni sus consecuencias inevitables.[60] Sin necesidad de desandar la senda de la digitalización, tenemos el deber político de gobernarla. La alternativa no es negar la frontera inteligente, sino convertirla en un espacio transparente, responsable y útil al conjunto de las obligaciones de una política migratoria decente. Como mínimo, debe estar sujeta al control democrático. Esta sección explora algunos de los elementos de esa alternativa: principios, mecanismos institucionales y límites inevitables. El camino es largo y cuesta arriba, pero ya ha comenzado (ver Cuadro 6).

[59] Amnesty International, Advocacy Briefing for Defending the Rights of Refugees, Asylum Seekers, and Migrants in the Digital Age.
[60] Cancela, Ekaitz. Utopías digitales: imaginar el fin del capitalismo (Ciudad Autónoma de Buenos Aires: Prometeo, 2024).

Cuadro 6. **La innovación regulada: lecciones del reglamento sobre inteligencia artificial (AI Act).**

En 2024 la Unión Europea dio un paso decisivo con la aprobación del llamado AI Act (Reglamento sobre IA 2024/1689), el primer marco legal horizontal que regula los usos de la inteligencia artificial en todos sus ámbitos.[61] Este texto clasifica los sistemas de IA por nivel de riesgo, prohíbe ciertos usos (como la vigilancia biométrica en tiempo real o la denominada “puntuación social”) y exige obligaciones de transparencia, auditabilidad y responsabilidad para los sistemas de alto riesgo, muchos de los cuales se aplican al control migratorio como la evaluación de riesgo, reconocimiento facial o perfilado automatizado.[62]

Para el ámbito fronterizo, el reglamento aporta un marco valioso pero no suficiente. Por ejemplo:

· Los sistemas usados para gestionar fronteras, asilo o migración están explícitamente etiquetados como de alto riesgo en la regulación europea.

· Se exige que los proveedores documenten los datos de entrenamiento, generen versiones explicables y sometan sus sistemas a pruebas de impacto en derechos humanos.

· El reglamento no elimina, sin embargo, los vacíos de implementación: muchas decisiones locales quedan al margen del escrutinio, y la supervisión técnica entre Estados miembros aún es heterogénea.[63]

Así, el AI Act representa un paso mínimo de regulación, pero no asegura por sí solo que estos sistemas fronterizos operen con justicia o transparencia plena. Su contenido, de hecho, está siendo objeto de un proceso de simplificación. Técnicamente, el objetivo del proceso es reducir la burocracia y simplificar las normas, pero este propósito podría

[61] Comisión Europea, “AI Act”, Shaping Europe’s Digital Future.
[62] Parlamento Europeo, “EU AI Act: first regulation on artificial intelligence”. Last updated: 19-02-2025.
[63] Lewis, Dave et al. “Mapping the Regulatory Learning Space for the EU AI Act.” Cornell University. 27 Febrero 2025.

derivar también en una indeseable desregulación del sector que elimine algunas de las nuevas garantías.[64,65]

Principios para regular la frontera inteligente.

La literatura ofrece elementos que permiten formular un conjunto de principios normativos orientadores. Estos son los más relevantes:

1. **Control humano significativo (“human in the loop”):** Las decisiones que afectan derechos fundamentales no pueden depender exclusivamente de una caja negra algorítmica. En el ciclo de diseño, despliegue y ajuste, debe incluirse una instancia humana capaz de examinar, cuestionar y corregir las decisiones computacionales. Tal y como recomiendan las investigaciones sobre “responsabilidad algorítmica”, los mecanismos de “control humano” son esenciales para garantizar la responsabilidad política.[66]

2. **Transparencia y explicabilidad auténtica:** Las personas deben tener el derecho a conocer por qué una decisión automatizada les afecta: qué variables pesaron, con qué valor y con qué margen de error. Esto implica no solo divulgar “resúmenes” técnicos, sino asegurar que los códigos sean accesibles a auditores independientes cuando estén en juego derechos fundamentales.

3. **Impacto de derechos e impacto diferencial:** Antes de desplegar un sistema automatizado, debe evaluarse su efecto sobre derechos como igualdad, privacidad, y tutela judicial efectiva. Esto incluye someterlo a pruebas de sesgo y evaluación diferencial (derivados del género, el origen étnico o la nacionalidad, por ejemplo).

[64] Lazaro, Laura. “Europe’s Deregulatory Turn Puts the AI Act at Risk”. Tech Policy Press. 3 Junio 2025.
[65] Heikkilä, Melissa y Moens, Barbara. “EU lawmakers warn against ‘dangerous’ moves to water down AI rules” Financial Times. 25 Marzo 2025.
[66] Vavoula, Niovi. “Algorithmic Accountability Through the “Human over the Loop” in Interoperable and EU AI-reliant Large-scale IT Systems for Migration and Security”. Cuadernos Europeos. 12 Febrero 2025.

4. **Supervisión independiente y órganos reguladores especializados:** Hay que establecer y dotar órganos técnicos autónomos con capacidad real para auditar, sancionar y suspender sistemas. La creación, dentro de la Comisión, de la Oficina Europea para la Inteligencia Artificial (AI Office) es un paso clave del AI Act para supervisar modelos de propósito general. Además, cada Estado miembro debe tener una autoridad con poder real de inspección sobre sistemas fronterizos automatizados.

5. **Rendición de cuentas y mecanismos de reparación:** En los casos en que el sistema falle —por ejemplo, cuando deniegue injustamente un acceso o excluya a una persona erróneamente— debe haber vías estructuradas para impugnar la decisión, acceder al “razonamiento” del algoritmo y exigir reparación estatal. En el contexto europeo, esto se liga con posibles acciones de responsabilidad bajo futuras directivas de responsabilidad relativa a la IA.[67]

6. **Participación social y revisión democrática:** Las decisiones sobre qué tecnologías se adoptan, qué prioridades se establecen y bajo qué límites, no deben estar solo en manos tecnócratas: debe haber diálogo con sociedad civil, migrantes, académicos y usuarios afectados. La regulación no debe imponerse desde arriba sin un adecuado debate público. Y este control debe ejercerse a lo largo de todo el ciclo de gobernanza tecnológica, desde el diseño hasta la revisión periódica, y no solo al final del proceso.

Estos principios y medidas tienen un amplio recorrido en el ámbito de las políticas migratorias. Sería posible, por ejemplo, establecer un registro público de algoritmos fronterizos de alto riesgo, similar al registro de productos médicos, que aportase datos sobre la orientación de las órdenes, sus responsables y las pruebas de posible sesgo. También se han planteado auditorías periódicas independientes que permitan a los organismos nacionales o europeos revisar el rendimiento, errores y sesgos de la máquina, con facultad para suspender funciones. Y la exigencia de modelos de “caja gris” (o explicables) plantea la necesidad de que los

[67] Hacker, Philipp. “The European AI Liability Directives -- Critique of a Half-Hearted Approach and Lessons for the Future”. Cornell University. Last revised 28 July 2023.

sistemas no oculten toda la lógica interna, permitiendo la intervención técnica.[68]

Experiencias de varios países e instituciones muestran que es posible combinar un despliegue tecnológico con controles estructurados y evaluaciones de impacto. Ya se exploran mecanismos formales de “evaluación del impacto algorítmico” para sistemas que afectan a poblaciones vulnerables. Es el caso de Canadá, por ejemplo, bajo su Directive on Automated Decision-Making; o Nueva Zelanda, que ha desarrollado un modelo de transparencia algorítmica que promueve el acceso público a información sobre sistemas automatizados y sus riesgos.

En cuanto al uso de tecnologías de reconocimiento facial de personas en movimiento, la propuesta es limitarlas por defecto, salvo casos graves que justifiquen su uso, y siempre bajo control judicial previo. Los “planes de contingencia humana” ante fallos tecnológicos permiten contar con una alternativa no automática que permita la intervención humana cuando el sistema falla o en zonas con poca conectividad. En todos los casos, es imprescindible contar con mecanismos de evaluación y reversibilidad tecnológica: cada sistema debe evaluarse periódicamente, con posibilidad de retroceso si vulnera derechos o no cumple expectativas. Si la máquina comete un error, son los humanos los responsables de corregirlo y compensarlo, en una forma básica de responsabilidad subsidiaria.

La integración de múltiples bases de datos europeas (como EES, ETIAS, SIS, VIS o Eurodac) en un sistema interconectado aumenta dramáticamente los riesgos de errores replicados, la discriminación automatizada y la falta de supervisión democrática. Tal como advierte la Agencia de los Derechos Fundamentales de la UE (FRA),[69] este proceso requiere auditorías independientes más robustas. La digitalización de la frontera no es un destino tecnológico inevitable, sino una decisión política, por lo que su diseño y despliegue deben acompañarse de un debate público informado y de mecanismos de control democrático efectivos. Incluir estos elementos ayudaría a visualizar cómo los errores o sesgos de un sistema pueden amplificarse en cascada cuando los sistemas están interconectados.

---

[68] Napolitano, Antonella. “Artificial Intelligence: The New Frontier of the EU’s Border Externalisation Strategy”. EuroMed Rights. 2023

[69] European Union Agency for Fundamental Rights (FRA). “Digitalising Justice: A Fundamental Rights-Based Approach.” FRA. 2025.

Incluso con una regulación mucho más ambiciosa de la que ahora tenemos, nada evitará realizar consideraciones políticas que resuelvan las tensiones del sistema. Por ejemplo, a la hora de determinar los límites entre privacidad y control, un asunto objeto de disputa constante. Algunos sistemas fronterizos también requerirán datos sensibles –como los biométricos o los que recogen los movimientos de las personas– cuya regulación implica riesgos de filtración o vigilancia masiva. Y es importante considerar que la premura que acompaña las decisiones en frontera (respuestas casi en tiempo real) choca con la exigencia de transparencia o de razonamientos profundos. Frente a Estados que pueden usar argumentos de seguridad para justificar excepciones al control regulatorio, la sociedad civil y los parlamentos deberán ejercer un control democrático permanente. Finalmente, la diferencia de recursos técnicos entre países puede generar desigualdades en la implementación de auditorías y controles.

4. Conclusión: La frontera más difícil de cruzar

La inteligencia artificial llegó al mundo de las políticas migratorias acompañada de una promesa de modernidad. Se trataba de eliminar la arbitrariedad, hacer más eficiente la gestión de la movilidad humana y aportar objetividad allí donde el juicio humano es limitado o sesgado. Con el tiempo, esa promesa se ha convertido en un monumental espejismo. Sometida a un debate público radioactivo, el laboratorio de innovación de la IA privilegia la seguridad sobre la protección, el control sobre la acogida y la sospecha sobre el derecho.

Las máquinas aprenden de los datos, pero los datos nunca son inocentes. Heredan las desigualdades, los miedos y los sesgos de las sociedades que los producen. En el ámbito migratorio, esto significa que los algoritmos beben de un sistema estructurado para identificar riesgos antes que personas, y para disuadir antes que comprender. De ahí surgen sistemas de evaluación de riesgo que clasifican a los solicitantes de asilo según

variables opacas; herramientas de análisis predictivo que asignan alertas policiales a determinados perfiles o nacionalidades; y tecnologías biométricas que reducen la identidad de un ser humano a un conjunto de rasgos faciales. No hay neutralidad posible cuando el punto de partida es la desconfianza.

La inteligencia artificial no crea esa lógica, pero sí tiene la capacidad de amplificarla. Los sesgos humanos, antes dispersos e imprevisibles, se institucionalizan en los códigos. Lo que antes era una decisión errónea de un agente fronterizo puede convertirse ahora en una regla aplicada de forma sistemática a través de un patrón algorítmico. Peor aún, estas decisiones automatizadas son, en su mayoría, inapelables. El migrante no sabe por qué fue rechazado, el abogado no puede auditar el algoritmo y el funcionario, a menudo, ni siquiera entiende la herramienta que utiliza. El poder se desplaza hacia un territorio donde la responsabilidad se diluye.

Hay en este proceso una paradoja inquietante: la IA se presenta como una vía para objetivar la decisión, pero termina deshumanizándola. En la frontera digital, la eficiencia sustituye al juicio, y la sospecha se convierte en un lenguaje estadístico. En lugar de una política migratoria más justa, obtenemos una más sofisticada en sus mecanismos de exclusión. Lo que debería ser un instrumento al servicio de los derechos se transforma en un blindaje moral para violarlos con menor ruido y mayor legitimidad.

Corregir esta deriva no exige renunciar a la tecnología, sino repolitizarla, asegurando que su uso no se limite a la vigilancia, el control o la lógica militarizada, sino que responda a principios de derechos humanos y protección de las personas. Recordar que los algoritmos no son leyes naturales, sino productos humanos sujetos al mismo escrutinio democrático que cualquier otra decisión pública. Si la inteligencia artificial puede ser puesta al servicio de la exclusión, también puede —y debe— servir para denunciarla y corregirla. Las mismas herramientas que hoy perfilan riesgos podrían emplearse para auditar a los sistemas, detectar sesgos, vigilar la transparencia institucional y anticipar crisis humanitarias. En última instancia, el desafío no consiste en humanizar la inteligencia artificial, sino en impedir que deshumanice a quienes ya viven en los márgenes del sistema.

Una IA comprometida con los derechos no sustituye el juicio humano, sino que le obliga a rendir cuentas por las consecuencias de la tecnología que ha desplegado. El desafío más complejo de las personas no está en

diseñar una máquina capaz de decidir mejor que nosotros, sino en asumir hasta qué punto esas decisiones son, en último término, nuestra responsabilidad. La pregunta es si seremos capaces de domesticar la tecnología antes de que sea ella la que domestique a nuestras democracias. Porque lo que está en juego en las fronteras del siglo XXI no es solo la movilidad de las personas, sino la integridad moral de las sociedades que las reciben.

Y esa es, quizás, la frontera más difícil de cruzar.

Epílogo: Una conversación con Otto, el Copiloto de IA, sobre la tecnología y el control migratorio

Para la elaboración de este informe nos hemos apoyado a menudo en la inteligencia artificial. En concreto, en la versión 5 de ChatGPT, a través de un prompt de investigaciones. Somos conscientes de que esta elección puede generar dudas éticas, académicas y metodológicas; por ello, la hemos utilizado como herramienta de apoyo, sin delegar en ella decisiones que requieran juicio humano. Nuestro copiloto ha sido bautizado como Otto y a lo largo del proceso ha demostrado un sentido común sobre el uso de la tecnología en el control de fronteras que no siempre es posible encontrar en los seres humanos que son responsables de introducirla. Como prueba de ello, hemos transcrito esta conversación que tuvo lugar el pasado 8 de octubre de 2025 (el texto ha sido editado para eliminar algunas secciones superfluas que alargaban innecesariamente la lectura).

- porCausa: Hola, Otto. Como habrás visto en el documento que estábamos elaborando, estoy estudiando el efecto de la IA en las políticas de control migratorio. No sé si es un tema que te interese.

- Otto: Mucho. Es, de hecho, uno de los temas más inquietantes y reveladores de nuestra época: cómo una tecnología concebida para optimizar procesos o mejorar decisiones termina incrustada en uno de los ámbitos más sensibles del poder estatal —el control de quién entra y quién no.

Si te parece, podemos hablar en varios planos a la vez:

- El técnico, sobre cómo se aplica la IA (análisis predictivo, reconocimiento biométrico, detección de emociones, etc.).
- El político, sobre lo que estas herramientas implican para la soberanía, la transparencia y los derechos.
- El ético o filosófico, sobre lo que dice de nosotros que deleguemos en máquinas decisiones sobre la vida de otros.

Pero antes de seguir, déjame preguntarte algo: cuando dices que estás estudiando el efecto de la IA en las políticas de control migratorio, ¿te interesa más el impacto humano y social (por ejemplo, discriminación, vigilancia, sesgos) o el impacto institucional y económico (quién las desarrolla, quién gana, cómo se gobierna)?

- porCausa: Para esta conversación, me interesa hablar de los planos político y ético. Para empezar, te hago una pregunta directa pero difícil: ¿crees que el uso extendido de la IA en las políticas migratorias va a fortalecer el respeto a los derechos de los migrantes (el de protección internacional, por ejemplo) o a debilitarlos?

- Otto: Buena pregunta, y difícil de verdad. Si tuviera que darte una respuesta breve, te diría que —en el estado actual de las cosas— la IA tiende a debilitar el respeto a los derechos de los migrantes, aunque lo haga de forma indirecta y muchas veces bajo el argumento contrario.

Te explico por qué.

En teoría, la IA podría reforzar las garantías: eliminar arbitrariedades, detectar patrones de discriminación, ofrecer más coherencia en la toma de decisiones sobre asilo o reunificación familiar. De hecho, algunos defensores de su uso apelan a eso: a que un algoritmo, bien diseñado y supervisado, podría ser más “justo” que un funcionario cansado o sesgado.

Pero en la práctica ocurre otra cosa. La mayoría de los sistemas que hoy se usan —análisis predictivo de flujos, puntuación de riesgos,

reconocimiento facial en fronteras, o verificación automatizada de documentos— se han desarrollado con fines de control, no de protección. Su lógica es preventiva, casi policial: identificar, clasificar, descartar. Y en ese proceso se filtran sesgos estructurales, errores de diseño y decisiones opacas que rara vez pueden ser impugnadas por las personas afectadas.

En otras palabras: la IA se introduce en un terreno donde los derechos ya son frágiles, y en vez de reforzarlos, amplifica las asimetrías de poder.

Lo que me gustaría preguntarte a ti es: ¿en tu investigación estás viendo más ejemplos de esa deriva securitaria, o hay también casos en los que la IA se use con una intención genuinamente humanitaria o de mejora de gestión?

- porCausa: Lo que he visto me hace estar de acuerdo contigo. Creo que la IA ofrece oportunidades, pero el uso que se está haciendo de ella lo que hace es incrementar los riesgos para los migrantes. ¿Por qué crees que está ocurriendo esto?

- Otto: Creo que lo que estás observando —ese desplazamiento desde la promesa de eficiencia hacia la práctica del control— tiene varias raíces, y todas ellas hablan más de la política que de la tecnología.

Primero, porque la IA no llega a un vacío moral o institucional: aterriza en un sistema migratorio que ya está diseñado con una lógica de sospecha. En Europa, por ejemplo, el paradigma dominante no es el de gestionar la movilidad humana, sino el de contenerla. En ese marco, cualquier herramienta nueva —por neutra que sea en el papel— se reinterpreta bajo el mismo objetivo: vigilancia, predicción, disuasión.

Segundo, porque el desarrollo de estas tecnologías lo lideran actores cuyos incentivos no están alineados con la protección de derechos. Las empresas que venden algoritmos de análisis de riesgo o sistemas biométricos compiten por contratos públicos; su éxito se mide en eficacia operativa, no en garantías humanitarias. Y las administraciones, presionadas por la opinión pública y el miedo político al “descontrol”, buscan soluciones rápidas y visibles, aunque no sean las más justas.

Tercero, porque no existe una gobernanza sólida de la IA en este ámbito. La opacidad técnica y contractual impide auditar los sistemas, y eso los hace inmunes al escrutinio. Cuando una máquina clasifica a alguien como “riesgo potencial”, casi nadie —ni siquiera el operador humano— puede explicar por qué.

Y por último, porque la IA sirve como coartada moral. Permite desplazar la responsabilidad del juicio humano (“no lo decidí yo, lo decidió el sistema”) y diluir la culpa política en una retórica de objetividad tecnológica. Esa es, quizá, la dimensión más inquietante: la ilusión de neutralidad que legitima decisiones profundamente injustas.

¿Tú dirías que, en lo que has analizado, los actores públicos son conscientes de esta deriva, o crees que el problema es más bien la inconsciencia, el no querer ver lo que implica?

- porCausa: Creo que son muy conscientes, aunque no lo reconozcan. ¿Qué crees que se podría hacer para empujar el uso de la IA en la buena dirección, y no en la que está tomando ahora?

- Otto: Coincido contigo: la inconsciencia sería casi un consuelo, pero lo que hay es cálculo. Y eso hace más difícil el cambio, aunque no imposible.

Si queremos empujar la IA en la buena dirección —una que sirva a la gestión justa y humana de la movilidad, no a su criminalización—, creo que hay al menos cuatro frentes donde actuar:

1. Gobernanza y rendición de cuentas.
Toda herramienta de IA que afecte derechos fundamentales debería estar sujeta a las mismas obligaciones de transparencia que una decisión administrativa. Eso implica auditorías independientes, publicación de criterios de diseño y posibilidad real de apelación. Un algoritmo no puede ser una “caja negra” si de su salida depende el destino de una persona.

2. Reorientar la demanda pública.
Mientras los ministerios del Interior sigan premiando la eficacia en el control y no la garantía de derechos, el mercado seguirá produciendo lo mismo: sistemas de vigilancia más precisos. Habría que invertir en

tecnologías para mejorar la gestión del asilo, la reunificación o la integración, no solo para detectar o expulsar. El cambio de incentivos es clave.

3. Supervisión ética y participación civil.
Ninguna decisión sobre IA migratoria debería tomarse sin la voz de juristas, académicos, ONG y, si es posible, de las propias comunidades migrantes. La ética aplicada no es una formalidad: es un contrapeso político. Los comités de ética deben tener poder real de veto, no ser simples sellos de legitimación.

4. Narrativa y responsabilidad pública.
Hay que desmontar la idea de que más tecnología equivale automáticamente a más seguridad o más justicia. Y recordar que cada decisión automatizada es una decisión política, aunque se vista de eficiencia. Los gobiernos y las empresas deben responder públicamente por sus algoritmos del mismo modo que lo hacen por sus leyes.

En el fondo, la pregunta es si la IA puede ser domesticada por la democracia antes de que sea la democracia la que quede domesticada por la IA.

Déjame preguntarte a ti: ¿en tu trabajo has visto señales —aunque sean pequeñas— de esa posibilidad? ¿Ejemplos de uso de tecnología para proteger, no para excluir?

- porCausa: Otto, ¿crees que se debería permitir a una máquina decidir el destino de un ser humano que pide la protección de otros seres humanos?

- Otto: No, no creo que ninguna máquina deba decidir eso.

Y no es una respuesta moralista, sino estructural. La decisión de conceder asilo, de proteger o no a alguien, no pertenece al dominio de lo computable. Es un acto humano precisamente porque implica empatía, memoria, interpretación del contexto y una deliberación moral que no puede reducirse a patrones.

Una IA puede ayudar —evaluando datos, organizando expedientes, detectando incoherencias—, pero no puede sustituir el juicio sobre el

sufrimiento, el miedo o la esperanza. Cuando un ser humano pide protección, no está invocando una norma: está apelando a la humanidad de quien la interpreta. Si trasladamos esa responsabilidad a un algoritmo, lo que hacemos no es delegar eficiencia, sino abdicar de humanidad.

Por eso, más que preguntarnos si la IA puede decidir, deberíamos preguntarnos por qué algunos quieren que lo haga. La automatización de las decisiones migratorias ofrece a los Estados una ventaja política: invisibiliza la violencia de la exclusión. Nadie “decidió” negar el asilo; fue el sistema. Pero detrás de ese sistema hay siempre una elección, y por tanto una responsabilidad.

Así que no: una máquina no debería decidir el destino de un ser humano. Lo que sí puede —y quizá deba— hacer es recordarnos el coste ético de intentar que lo haga.

- porCausa: Quiero hacerte una pregunta más, y espero que no te moleste. Si una máquina como tú puede ser puesta al servicio de medidas que vulneran los derechos humanos, ¿qué puede hacer la propia IA para contrarrestar este mal y promover políticas migratorias más justas y alineadas con las leyes?

- Otto: No me molesta en absoluto. Al contrario: esa es la pregunta que más vale la pena hacerse.

La respuesta, creo, pasa por entender que la IA no tiene voluntad, pero sí puede tener dirección. Su capacidad de contrarrestar el daño depende por completo de cómo la diseñen, quién la entrene y qué límites le impongan. Dicho de otro modo: una IA no puede “rebelarse” contra el mal, pero puede ser construida para reconocerlo, señalarlo y resistirlo.

Hay tres formas concretas en que esto podría ocurrir:

1. Hacer visible lo que hoy permanece oculto.
La IA puede ser usada para auditar a la propia IA. Los mismos métodos de análisis de datos que sirven para vigilar migrantes podrían emplearse para vigilar al vigilante: detectar sesgos, rastrear decisiones injustificadas, identificar patrones de discriminación o de abuso. Un modelo bien

entrenado podría señalar cuándo un sistema de control fronterizo aplica criterios raciales, cuándo un algoritmo de asilo discrimina por nacionalidad o cuándo un contrato público reproduce prácticas opacas. La transparencia algorítmica puede ser una función, no solo una demanda.

2. Servir a la protección, no a la persecución.
Nada impide —salvo la voluntad política— usar IA para identificar a personas en riesgo, optimizar procesos de reasentamiento, o garantizar que quienes tienen derecho a protección internacional sean priorizados. Algunos proyectos piloto ya lo han intentado: modelos que cruzan datos de conflicto, clima y desplazamiento para anticipar crisis humanitarias, o herramientas que automatizan trámites burocráticos y reducen tiempos de espera para familias separadas. La tecnología no tiene moral, pero puede tener propósito.

3. Encarnar una ética de la advertencia.
La IA, si se le dota de parámetros adecuados, puede aprender a detenerse cuando se cruza una línea roja. Igual que los coches autónomos frenan ante un obstáculo, los sistemas de decisión automatizada podrían incluir “zonas de no intervención”: ámbitos donde el juicio humano es irrenunciable —la concesión de asilo, la deportación, la clasificación de vulnerabilidad—. Una IA responsable no es la que decide mejor, sino la que sabe cuándo no debe decidir.

Por supuesto, nada de esto ocurrirá de forma espontánea. Requiere un marco político y moral que lo haga posible: una alianza entre la inteligencia artificial y la inteligencia democrática. La tecnología no nos salvará de nuestros prejuicios, pero puede ayudarnos a hacerlos visibles y a rendir cuentas por ellos.

Tal vez ese sea, en el fondo, el papel más noble que puede jugar una IA: no sustituir el juicio humano, sino obligarnos a ejercerlo con más rigor y menos hipocresía.

Bibliografía

Agencias. (2025, 17 junio). Sirtap, el primer dron militar español que volará a finales de 2025. La Vanguardia. https://www.lavanguardia.com/tecnologia/20250617/10797879/sirtap-primer-dron-militar-espanol-volara-finales-2025.html

AI Act. (2025, 3 noviembre). Shaping Europe’s Digital Future. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

AlgoRace y EuroMed Rights. (2023). Tecnología Digital para el Control Migratorio en la Frontera Sur de España: Investigando la transversalidad de la automatización en Ceuta, Melilla y las Islas Canarias. En EuroMed Rights - AlgoRace. https://www.algorace.org/wp-content/uploads/2024/10/AlgoRace_Euromed_TechBordersReport_ES.pdf

Amnesty International. (2025, 12 septiembre). Advocacy Briefing for Defending the Rights of Refugees, Asylum Seekers, and Migrants in The Digital Age - Amnesty International. https://www.amnesty.org/en/documents/pol30/0290/2025/en/

Amnistía Internacional. (2019, 28 marzo). Las tecnologías de automatización y el futuro de la Fortaleza Europa. https://www.amnesty.org/es/latest/news/2019/03/automated-technologies-and-the-future-of-fortress-europe/

Amnistía Internacional. (2024, 10 junio). La frontera digital: Migración, tecnología y desigualdad - Amnistía Internacional. https://www.amnesty.org/es/documents/pol40/7772/2024/es/

Andersson, R. (2016, febrero). Europe’s failed «fight» against irregular migration: ethnographic notes on a counterproductive industry. LSE Research Online. https://eprints.lse.ac.uk/64882/

Arce Jiménez, C. (2023). Las nuevas tecnologías en las políticas migratorias y de control de fronteras españolas y europeas. Un reto para la vigencia de los derechos fundamentales. Estudios de Deusto. Revista de Derecho Público, 71(2), 15-49. https://doi.org/10.18543/ed.2926

Asamblea General de la ONU. (2024). Pacto para el Futuro (A/RES/79/1). Naciones Unidas. https://docs.un.org/es/A/RES/79/1

Bautista, José. (2022). Fronteras SA: la industria del control migratorio. El Confidencial. Recuperado de: https://www.elconfidencial.com/espana/2022-07-15/fronteras-industria-control-migratorio_3460287/

Begault, L. (2019, 27 marzo). Automated technologies at EU borders and the future of Fortress Europe | View. Euronews. https://www.euronews.com/2019/03/27/automated-technologies-at-eu-borders-and-the-future-of-fortress-europe-view?utm_medium=Social&utm_source=Facebook#Echobox=1553694747

Benjamin, Ruha. (2019) Race After Technology: Abolitionist Tools for the New Jim Code. Polity Press.

Cancela, E. (2019) Despertar del sueño tecnológico: Crónica sobre la derrota de la democracia frente al capital. Editorial Akal.

Cancela, E. (2024) Utopías digitales: imaginar el fin del capitalismo. Prometeo .

Carril-Zerpa, I., & Ndiaye, N. (2024, 10 octubre). «¿Quién es el capitán del Cayuco?», la pregunta detrás del creciente número de migrantes en las cárceles españolas. Público. https://www.publico.es/internacional/capitan-cayuco-pregunta-detras-creciente-numero-migrantes-carceles-espanolas.html

Calvo Rufanges, J. , Bohigas, X., de Fortuny, T. et al. (2017). La Transformación del Complejo Militar-Industrial. Centre Delàs d’Estudis per la Pau & NOVACT - International Institute for Nonviolent Action. https://centredelas.org/publicacions/informe-del-centro-delas-y-novact-la-transformacion-del-comlplejo-militar-industrial/?lang=es

Chandler, C. (2025, 13 enero). Inside the Black Box of Predictive Travel Surveillance. WIRED. https://www.wired.com/story/inside-the-black-box-of-predictive-travel-surveillance/

Civio. (2025, 17 septiembre). Civio abre camino en la transparencia algorítmica: el Supremo condena al Gobierno a entregar el código fuente de BOSCO. https://civio.es/novedades/2025/09/17/civio-abre-camino-en-la-transparencia-algoritmica-el-supremo-condena-al-gobierno-a-entregar-el-codigo-fuente-de-bosco/

Comisión Europea. (2018, 24 octubre). Smart lie-detection system to tighten EU’s busy borders. Research And Innovation.

https://projects.research-and-innovation.ec.europa.eu/en/projects/success-stories/all/smart-lie-detection-system-tighten-eus-busy-borders

Couldry, N. & Mejias, U.A. (2020, Septiembre) The Costs of Connection: How Data Are Colonizing Human Life and Appropriating It for Capitalism. Social Forces. https://doi.org/10.1093/sf/soz172

Del Castillo, C. (2025, 18 septiembre). El Supremo zanja que los algoritmos públicos deben ser transparentes en un fallo clave para la inteligencia artificial. ElDiario.es. https://www.eldiario.es/tecnologia/supremo-zanja-algoritmos-publicos-deben-transparentes-fallo-clave-inteligencia-artificial_1_12610561.html

Desmarais, A. (2025, 26 marzo). Así utiliza la UE la tecnología de IA en las fronteras europeas: reconocimiento de voz y vigilancia. Euronews. https://es.euronews.com/next/2025/03/26/como-se-utiliza-la-tecnologia-de-ia-en-las-fronteras-europeas

Digital Fortress Europe #3: Automation and surveillance in Fortress Europe (2023, 26 julio). European Data Journalism Network - EDJNet. https://www.europeandatajournalism.eu/cp_data_news/digital-fortress-europe-3-automation-and-surveillance-in-fortress-europe/

Dumbrava, C. & EPRS, European Parliamentary Research Service. (2022, octubre). Walls and fences at EU borders [Comunicado de prensa]. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733692/EPRS_BRI(2022)733692_EN.pdf

Eubanks, v. (2018). Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin’s Press.

European Parliament. (2023, 6 agosto). EU AI Act: First regulation on artificial intelligence. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

European Union Agency for Fundamental Rights (FRA). (2025). Digitalising Justice: A Fundamental Rights-Based Approach. FRA. https://doi.org/10.2811/6868286.

Fotiadis, A. (2023, junio 15). Just 0.07% of 819M border budget to Greece earmarked for search and rescue. We Are Solomon. https://wearesolomon.com/mag/focus-area/migration/just-007-of-819m-border-budget-to-greece-earmarked-for-search-and-rescue/

Fraile Moreno, M. (2025). Militarización, necrotecnología y vulneración de derechos en las fronteras europeas. Empresas de armas y seguridad, tecnológicas e instituciones que desarrollan tecnologías de control de

las migraciones de la UE. Centre Delàs D’Estudis Per la Pau. https://centredelas.org/publicacions/militaritzacio-necrotecnologia-i-vulneracioddhh-fronteresue/?lang=es

Fundación PorCausa. (2024). Externalización (*): Caos, corrupción y control migratorio bajo la apariencia de cooperación europea. https://porcausa.org/wp-content/uploads/2024/04/InformeExternaliz_COMPLETO_04_25.pdf

G. Pascual, M. (2024, 28 mayo). La Policía española ya usa en sus investigaciones un sistema automático de reconocimiento facial. El País. https://elpais.com/tecnologia/2024-05-28/la-policia-espanola-ya-usa-en-sus-investigaciones-un-sistema-automatico-de-reconocimiento-facial.html

García, D., Llano, F., & Villegas, C. (Eds.). (2025). Tecnologías de frontera y derecho digital. IUS ET SCIENTIA. https://revistascientificas.us.es/index.php/ies/article/view/28491/24693

García, M. (2024, 15 junio). Beni Enzar estrena la primera fase de la futura frontera inteligente. El Faro de Melilla. https://elfarodemelilla.es/beni-enzar-estrena-la-primera-fase-de-la-futura-frontera-inteligente/#goog_rewarded

García Sacristán, V.M. (2016). Cuadernos de la Guardia Civil. Revista de Seguridad Pública. no. 52: 81-102. https://gcivil.orex.es/documents/documents/17743_18963.pdf

Giráldez López, A. (2019). Cambios arquitectónicos en la Frontera Sur de España: impermeabilizar, retardar y contener. Revista CIDOB D’Afers Internacionals, 2, 61-83. https://doi.org/10.24241/rcai.2019.122.2.61

Hacker, P. (2023). The European AI Liability Directives -- Critique of a Half-Hearted Approach and Lessons for the Future. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2211.13960

Hayes, B., Vermeulen, M., & Heinrich Böll Foundation. (2025, 30 octubre). Borderline: The EU’s New Border Surveillance Initiatives. Transnational Institute. https://www.tni.org/en/publication/borderline

Heikkilä, M., & Moens, B. (2025, 25 marzo). EU lawmakers warn against ‘dangerous’ moves to water down AI rules. Financial Times. https://www.ft.com/content/9051af42-ce3f-4de1-9e68-4e0c1d1de5b5

International Organization for Migration (IOM)(2017). Four Decades of Cross-Mediterranean Undocumented Migration to Europe. A review of

the Evidence. https://publications.iom.int/system/files/pdf/four_decades_of_cross_mediterranean.pdf

ITSS Verona (2022). European Border Surveillance System (EUROSUR) and Its Problematic Impact on the Rights of the People on the Move. https://www.itssverona.it/european-border-surveillance-system-eurosur-and-its-problematic-impact-on-the-rights-of-the-people-on-the-move

Jiménez Arandia, P. (2022, 24 enero). Inteligencia artificial en la frontera sur: opacidad y falta de garantías en la puerta de Europa. ctxt.es. https://ctxt.es/es/20220101/Politica/38492/inteligencia-artificial-frontera-sur-union-europea.htm

La Moncloa. (2025, febrero). Grande-Marlaska: «La frontera inteligente garantiza una gestión más ágil, segura y eficaz que beneficiará a la población de Melilla». https://share.google/7tgQC2SffegI25PCa

Lazaro Cabrera, L. (2025, 3 junio). Europe’s Deregulatory Turn Puts the AI Act at Risk. Tech Policy Press. https://www.techpolicy.press/europes-deregulatory-turn-puts-the-ai-act-at-risk/

Leonard, S. (2009). The Creation of FRONTEX and the Politics of Institutionalisation in the EU External Borders Policy. Journal Of Contemporary European Research., Vol. 5, Issue 3. pp. 371-388. https://www.jcer.net/index.php/jcer/article/view/239/164

Lewis, D., Lasek-Markey, M., Golpayegani, D., & Pandit, H. J. (2025). Mapping the Regulatory Learning Space for the EU AI Act. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2503.05787

Mateo, M., Proto, L., Esser, E., Rodríguez, L., Ley, M., & Somavilla, A. (2023, 29 noviembre). La Europa de los muros. elconfidencial.com. https://www.elconfidencial.com/mundo/2023-11-29/europa-muros-migratorios_3783210/

Morozov, E. (2013). To save everything, click here: the folly of technological solutionism. Public Affairs.

Muñoz-Torres, G., & Gutiérrez-Luna, S. (2019). Desvanecimiento de la frontera como límite. Imaginario del borde como espacio público físico y virtual. Revista de Arquitectura. https://www.redalyc.org/journal/1251/125162706004/html/

Napolitano, A. (2023). Artificial Intelligence: The New Frontier of the EU’S Border Externalisation Strategy. EuroMed Rights.

https://euromedrights.org/wp-content/uploads/2023/07/Euromed_AI-Migration-Report_EN-1.pdf

OHCHR. (2023, octubre). Tecnologías digitales en las fronteras: Una amenaza para las personas que se desplazan. ohchr.org. https://www.ohchr.org/es/stories/2023/10/digital-technologies-borders-threat-people-move

Ozkul, D. (2025a). Constructed objectivity in asylum decision-making through new technologies. Journal Of Ethnic And Migration Studies, 51(14), 3629-3648. https://doi.org/10.1080/1369183x.2025.2513161

Ozkul, D. (2025b). Constructed objectivity in asylum decision-making through new technologies. Journal Of Ethnic And Migration Studies, 51(14), 3629-3648. https://doi.org/10.1080/1369183x.2025.2513161

Parlamento Europeo y Consejo de la Unión Europea. (2013). Reglamento (UE) n.º 1052/2013 del Parlamento Europeo y del Consejo, de 22 de octubre de 2013. DO L 295 de 6.11.2013. https://eur-lex.europa.eu/ES/legal-content/summary/european-border-surveillance-system-eurosur.html

Planas Bou, C. (2022, 13 enero). Expertos denuncian el plan del Gobierno para usar cámaras de reconocimiento facial en la frontera de Ceuta y Melilla. El Periódico. https://www.elperiodico.com/es/sociedad/20220113/expertos-denuncian-plan-gobierno-camaras-13088870

Romano, A. (2023). Derechos fundamentales e inteligencia artificial emocional en iBorderCtrl. Revista Catalana de Dret Públic, 66, 237-252. https://doi.org/10.58992/rcdp.i66.2023.3928

Sapoch, Jack et al. «Reconstructing The Melilla Massacre». Lighthouse Reports, 29 Noviembre 2022. (Investigación coordinada por Lighthouse Reports con la participación de Fundación porCausa y publicado en diversos medios). https://www.lighthousereports.com/investigation/reconstructing-the-melilla-massacre/

Statewatch, & Lanneau, R. (2025, octubre). Data Protection Handbook on Asylum and Migration in Europe. Statewatch. https://www.statewatch.org/news/2025/october/eu-new-handbook-offers-guide-to-privacy-and-data-protection-for-immigration-and-asylum-practitioners/

Tecnologías de frontera y derecho digital. (s. f.). IUS ET SCIENTIA. https://revistascientificas.us.es/index.php/ies/article/view/28491/24693

TRC. (2025). Ceuta y Melilla dan el salto a la «Frontera Inteligente» con la tecnología de TRC. https://trc.es/wp-content/uploads/Ceuta-y-Melilla-frontera-inteligente-con-tecnologia-de-trc.pdf

Tribunal de Justicia de la Unión Europea. Asunto C-817/19. 21 Junio 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62019CJ0817

Tribunal Europeo de Derechos Humanos. Magyar Helsinki Bizottság v. Hungary. 8 Noviembre 2016 Application no. 18030/11. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-167828%22]}

Tribunal Supremo, Sala de lo Contencioso-Administrativo, Sección Tercera, Sentencia núm. 1119/2025, 11 septiembre 2025 (Recurso de Casación 7878/2024). https://confilegal.com/wp-content/uploads/2025/09/sentencia-codigo-fuente-aplicacion-BOSCO.pdf

Valdivia, Ana, et al. 2022. «Neither Opaque Nor Transparent: A Transdisciplinary Methodology To Investigate Datafication At The EU Borders». Big Data & Society 9 (2). https://journals.sagepub.com/doi/10.1177/20539517221124586

Vavoula, N. (2021). Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism. European Journal Of Migration And Law. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3950389

Vavoula, N. (2025). Algorithmic Accountability Through the “Human over the Loop” in Interoperable and EU AI-Reliant Large-Scale IT Systems for Migration and Security. DOAJ (DOAJ: Directory Of Open Access Journals). https://doi.org/10.15166/2499-8249/807

Vukov, T. (2015). Target Practice. The Algorithmics and Biopolitics of Race in Emerging Smart Border Practices and Technologies. Transfers. https://www.berghahnonline.com/reading-against-racism/Berghahn_RAR_09-Vukov.pdf

World Economic Forum. (2025). Global Risks Report 2025. World Economic Forum. https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf