10 de septiembre de 2025 POL 30/0290/2025

Documento de trabajo de incidencia para la defensa de las personas refugiadas, solicitantes de asilo y migrantes en la era digital

Ilustración de Eliana Rodgers: "A Dream Deterred". Un inmigrante se enfrenta a la vigilancia masiva en un paso fronterizo y se le recuerda su incierto futuro. Activistas trabajan para resistir a estos sistemas de vigilancia y muros.

Imagen de portada del Manual general: Defender los derechos de las personas refugiadas y migrantes en la era digital, Amnistía Internacional, 2024. Índice: POL 40/7654/2024.

Índice

Introducción

Amnistía Internacional es un movimiento global de más de 10 millones de personas comprometidas a crear un futuro en el que todas y todos disfrutan de los derechos humanos. Nuestra visión es la de un mundo donde quienes están en el poder cumplen sus promesas, respetan el derecho internacional y rinden cuentas. Somos independientes de todo gobierno, ideología política, interés económico y credo religioso, y nuestro trabajo se financia principalmente con las contribuciones de nuestra membresía y con donativos. Creemos que actuar movidos por la solidaridad y la compasión hacia nuestros semejantes en todo el mundo puede hacer mejorar nuestras sociedades.

#ProtectNotSurveil es una coalición europea de activistas, organizaciones, investigadores y otros actores que trabajan para garantizar que las políticas digitales y migratorias protejan a las personas en movimiento de los daños derivados de los sistemas de IA. Nuestra misión es cuestionar el uso de las tecnologías digitales en diferentes niveles de las políticas de la UE y defender la capacidad de las personas para desplazarse y buscar seguridad y oportunidades sin exponerse a sufrir daños, vigilancia o discriminación. Nuestro trabajo de incidencia tiene como objetivo exigir responsabilidades a la UE, a los Estados miembros y a las empresas privadas que se benefician de las violaciones de derechos humanos en las fronteras de la UE y dentro de ellas. Para ello, conectamos a las organizaciones de derechos digitales, derechos de las personas migrantes y movimientos por la justicia racial para cuestionar los enfoques tecnosolucionistas de las políticas migratorias.

Acerca de este documento

Este documento pretende ser un recurso de incidencia para activistas, defensores y defensoras, actores de la sociedad civil y comunidades de personas refugiadas y migrantes afectados por las tecnologías digitales y la vigilancia en contextos de asilo y migración. Proporciona un marco y unos principios de derechos humanos con los que analizar el impacto de las tecnologías emergentes y existentes sobre las personas refugiadas y migrantes, en especial para evaluar los impactos discriminatorios e interseccionales. También ofrece recomendaciones de incidencia, que pueden extraerse del documento y transmitirse directamente a las principales partes interesadas que desarrollan o implementan tecnologías digitales y vigilancia, a saber, Estados, empresas, organizaciones intergubernamentales y proveedores de servicios.

Este documento ha sido redactado por Amnistía Internacional con el apoyo de AlgorithmWatch, Border Violence Monitoring Network (BVMN), EuroMed Rights y Privacy International, basándose en las recomendaciones jurídicas y de políticas elaboradas por la coalición #ProtectNotSurveil en relación con las tecnologías de migración, asilo y vigilancia fronteriza, incluido el desarrollo y el uso de la inteligencia artificial en este campo. Se trata de un documento "vivo", que se actualizará periódicamente a medida que evolucionen las cuestiones clave.[1] Tengan en cuenta que las recomendaciones incluidas no son en absoluto exhaustivas, sino que pretenden ser más

[1] El documento se revisará cada 12 meses, así como cuando recibamos comentarios cruciales *ad hoc*, para actualizar las recomendaciones. Envíen sus comentarios a charlotte.phillips@amnesty.org.

bien un punto de partida para el trabajo de incidencia a escala nacional e internacional. El apartado "Recursos" que figura al final incluye una lista de publicaciones de Amnistía Internacional y organizaciones asociadas, donde se formularon inicialmente estas recomendaciones.

Glosario A-Z

Inteligencia artificial (IA)	Cualquier técnica o sistema que permite que las computadoras imiten el comportamiento humano. Aunque se sigue debatiendo qué constituye un sistema de IA, habitualmente se lo define como un "sistema basado en máquinas que, con objetivos explícitos o implícitos, deduce, a partir de la información que recibe, cómo generar resultados tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los diferentes sistemas de IA varían en cuanto a niveles de autonomía y adaptabilidad tras su implementación". [2]
Toma de decisiones algorítmica (TDA)	Sistema algorítmico que se usa (como apoyo) en las diversas etapas de los procesos de toma de decisiones.
Toma de decisiones automatizada	Sistema de toma de decisiones algorítmico sin intervención humana. El sistema toma la decisión por sí solo.
Tecnologías biométricas (de vigilancia)	Tecnologías (de vigilancia) utilizadas para identificar las características del cuerpo humano individuales mediante marcadores biológicos únicos, como las huellas dactilares, la retina y el iris del ojo, patrones de voz y faciales, y medidas de las manos. Se incluyen, por ejemplo, las tecnologías que clasifican a las personas en función de sus características biométricas, las tecnologías de reconocimiento facial utilizadas para identificar a las personas y las denominadas tecnologías de reconocimiento de emociones.
Desarrolladores	Principalmente empresas y organizaciones internacionales que invierten recursos para la

[2] Véase la descripción general de los principios de la OCDE sobre la IA. https://oecd.ai/en/ai-principles

	creación de herramientas de IA con la intención de proporcionarlas a otras partes para su uso o de ponerlas en práctica ellas mismas.
Implementadores	Quienes lideran la implementación de una herramienta de IA para sus propósitos finales previstos. Pueden ser actores privados o públicos. Una misma entidad, como una empresa o un organismo del sector público, puede ser desarrolladora e implementadora a la vez, si cuenta con capacidades internas para crear herramientas de IA por su cuenta.
Tecnología de reconocimiento facial (TRF)	Término genérico utilizado para describir un conjunto de aplicaciones que realizan una función específica utilizando el rostro humano para identificar a una persona o verificar su identidad. La TRF es una de las numerosas tecnologías biométricas utilizadas por los Estados y las entidades comerciales en una amplia variedad de ejemplos de uso.
Mayoría global	Término que se refiere a las personas racializadas, como los pueblos indígenas y las personas de ascendencia africana, asiática o latinoamericana, quienes, en su conjunto, constituyen la mayor parte de la población mundial. Es un término que se utiliza para cuestionar términos como "minorías", que a menudo se consideran marginadores, y que busca afirmar la capacidad de acción colectiva y la solidaridad de las personas sometidas a racismo sistémico y a injusticias raciales históricas.[3]
Evaluaciones del impacto sobre los derechos humanos (EIDDHH)	Una EIDDHH es un proceso para evaluar el impacto sobre los derechos humanos, incluida la identificación de riesgos a lo largo del ciclo de vida de la IA. Las EIDDHH deben incluir una evaluación de la idoneidad de una solución basada en la IA en una situación específica, que debe definir quiénes son los grupos afectados,

[3] Véase Campbell-Stephens, R.M. (2020). Global Majority: we need to talk about labels such as 'BAME'. https://www.linkedin.com/pulse/global-majority-we-need-talk-labels-bame-campbell-stephens-mbe/; Campbell-Stephens, R.M. (2021). Introduction: Global Majority Decolonising Narratives. In: Educational Leadership and the Global Majority. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-88282-2_1

	cuál es el impacto previsto y si se ha consultado a las comunidades afectadas, además de demostrar cómo se mitigará el daño.
Interseccionalidad	Forma de examinar cómo diferentes formas de discriminación se solapan e interactúan para crear una experiencia única y compleja de opresión para una persona. Explica el hecho de que las experiencias de discriminación que sufre una persona por su pertenencia a un grupo de identidad social determinado sometido a opresión por su género, orientación sexual, raza, clase, casta, discapacidad, condición migratoria, religión, etnia, identidad indígena, edad o cualquier otro motivo actúan de forma conjunta para hacer que su experiencia de opresión sea diferente de la de otras personas. Por lo tanto, no se limita a reconocer que existen diferentes formas de opresión, sino que examina el hecho de que, juntas, esas formas de opresión originan una constante particular de discriminación. Por ejemplo, si una persona solicitante de asilo negra o musulmana tiene más probabilidades de sufrir una detención por motivos migratorios, la discriminación y la violación de sus derechos humanos se debe a una combinación de su raza, origen nacional, situación migratoria o ciudadanía, ya sean reales o percibidos.
Obligación de no devolución	La obligación jurídica de los Estados de no devolver ni transferir a ninguna persona a un lugar o jurisdicción en donde pueda correr un riesgo real de sufrir persecución u otras violaciones o abusos contra los derechos humanos.
Uso de perfiles	El tratamiento automatizado de datos personales para evaluar aspectos propios de una persona, como su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su conducta, su ubicación o sus movimientos.[4]

[4] Véase el artículo 4.4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la

Discriminación racial	En la Convención sobre la Eliminación de Todas las Formas de Discriminación Racial (ICERD) se describe como "toda distinción, exclusión, restricción o preferencia basada en motivos de raza, color, linaje u origen nacional o étnico que tenga por objeto o por resultado anular o menoscabar el reconocimiento, goce o ejercicio, en condiciones de igualdad, de los derechos humanos y libertades fundamentales en las esferas política, económica, social, cultural o en cualquier otra esfera de la vida pública".[5]
Identificación biométrica remota (IBR)	Los sistemas de identificación biométrica remota (IBR) se utilizan para identificar personas a distancia, por medio de contrastar sus atributos biométricos únicos con una base de datos. La tecnología de reconocimiento facial es el ejemplo más común, tal y como se ha definido anteriormente, y en ocasiones puede utilizarse como término intercambiable con IBR. La IBR puede realizarse en tiempo real, con un procesamiento instantáneo o casi instantáneo de la información recopilada (también denominada "IBR en vivo"), o de forma retrospectiva, donde el análisis de las imágenes capturadas tiene lugar en un momento posterior (también conocida como "IBR diferida").
Herramientas de evaluación de riesgos	Tratamiento semiautomatizado o totalmente automatizado de los datos con fines de evaluación estadística y/o modelización predictiva para identificar el riesgo de que se produzca determinado resultado, ya sea a nivel individual o comunitario, o específico de un acontecimiento o situación.
Puntuación social	El uso de la inteligencia artificial y otras formas de toma de decisiones algorítmica para evaluar y clasificar a las personas con el fin de llevar a cabo determinadas evaluaciones o tomar

libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). https://eur-lex.europa.eu/eli/reg/2016/679/oj/spa

[5]Artículo 1, Naciones Unidas (1965). Convención Internacional sobre la Eliminación de Todas las Formas de Discriminación Racial [en línea]. OACNUDH. https://www.ohchr.org/es/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial

	decisiones sobre ellas. Este sistema de evaluación o clasificación suele ser predictivo; por ejemplo, puede programarse para inferir la probabilidad de que alguien que solicita empleo encuentre trabajo o la probabilidad de que se devuelva un préstamo. Se basa en información tan amplia como la identidad de la persona (edad, género, raza y origen étnico), el comportamiento pasado (historial laboral o antecedentes penales) o la situación socioeconómica (ingresos y nivel educativo).[6]
Racismo sistémico	El Comité Asesor del Consejo de Derechos Humanos de la ONU ha señalado que el racismo es un problema sistémico que: "opera a través de una red interrelacionada o estrechamente coordinada de leyes, políticas, prácticas, actitudes, estereotipos y prejuicios. Lo sostienen un amplio abanico de agentes, entre los que se encuentran las instituciones del Estado, el sector privado y las estructuras de la sociedad en sentido amplio. Esto resulta no solo en la discriminación expresa, directa, *de iure* o intencionada, sino también en la discriminación, la distinción, la exclusión, la restricción o la preferencia encubiertas, indirectas, *de facto* o no intencionadas por motivos de raza, color, linaje u origen nacional o étnico. A menudo tiene sus raíces en el legado histórico de la esclavitud, el comercio de africanos esclavizados y el colonialismo. Esto tiende a determinar las oportunidades y los resultados de generación en generación".[7]

[6] Adaptado de Human Rights Watch, Q&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net. https://www.hrw.org/sites/default/files/media_2021/11/202111hrw_eu_ai_regulation_qa_0.pdf

[7] Comité Asesor del Consejo de Derechos Humanos (8 de agosto de 2023). Promover la justicia y la igualdad raciales erradicando el racismo sistémico, doc. ONU A/HRC/54/70, párr. 7.https://docs.un.org/es/A/HRC/54/70

El uso de las tecnologías digitales en los contextos de asilo y migración

Las tecnologías digitales se han convertido en herramientas omnipresentes, de alto riesgo y, a menudo, experimentales para configurar y aplicar las políticas de migración y asilo de los Estados y las organizaciones regionales, que van desde la vigilancia electrónica, los satélites y los drones hasta el reconocimiento facial, los "detectores de mentiras" y el escaneo del iris.

Las tecnologías digitales tienen el potencial de causar y aumentar exponencialmente una serie de graves violaciones de derechos humanos, ya sea directa o indirectamente. Si los Estados impulsan activamente una agenda que entra en conflicto con sus obligaciones en materia de derechos humanos con respecto a las personas refugiadas y migrantes, estas tecnologías corren el riesgo de exacerbar las violaciones de derechos humanos y el sufrimiento. Las tecnologías utilizadas para aplicar las políticas de asilo y migración también pueden ser problemáticas por sí mismas, ya que sus sistemas son vulnerables a los sesgos y los errores y, a menudo, se basan en la recopilación, el almacenamiento y el uso excesivos de información que amenazan el derecho a la privacidad, la no discriminación y otros derechos humanos.
Las tecnologías digitales refuerzan regímenes fronterizos que discriminan basándose en la raza, el origen étnico o nacional y la ciudadanía. El racismo y la discriminación inherentes están profundamente arraigados en la gestión de la migración y los sistemas de asilo. Estas tecnologías corren el riesgo de perpetuar y ocultar los prejuicios raciales y la discriminación arraigados en las prácticas históricas y coloniales de exclusión racializada bajo el pretexto de la neutralidad y la objetividad, incluso por motivos religiosos. Su uso puede tener repercusiones desproporcionadas en grupos racializados y crear diferentes formas de discriminación que perpetúen el racismo sistémico, la discriminación, la opresión y la violencia.

En los últimos años se ha observado una tendencia a eximir a las tecnologías utilizadas con fines de gestión de la migración y las fronteras, incluidas exenciones en materia de privacidad y protección de datos, requisitos de rendición de cuentas y transparencia públicas, y otras obligaciones reglamentarias[8], en el marco de un cambio más amplio hacia medidas punitivas en la gestión de la migración y las fronteras[9] y la fusión de las políticas de migración, función policial y seguridad nacional.[10]

Existe una necesidad cada vez mayor y más urgente de pedir a los Estados, las empresas y otras partes interesadas que garanticen que cualquier desarrollo y uso de la tecnología respeta y

[8] Véase, por ejemplo, #ProtectNotSurveil (2024). Joint statement – A dangerous precedent: how the EU AI Act fails migrants and people on the move. https://www.accessnow.org/press-release/joint-statement-ai-act-fails-migrants-and-people-on-the-move/

[9] Equinox Initiative for Racial Justice y coalición #ProtectNotSurveil (2025): EU: Stop criminalising migration in the Facilitator's Package law. https://www.equinox-eu.com/eu-stop-criminalising-migration-in-the-facilitators-package-law/

[10] Véase, por ejemplo, The New York Times (2025). Trump Calls for 20,000 Extra Officers to Help with Deportation Efforts. https://www.nytimes.com/2025/05/10/us/politics/dhs-deportation-extra-officers.html

protege los derechos humanos de todas las personas, incluidas las refugiadas y migrantes, sin discriminación. La transparencia es una forma de salvaguardia y puede ser un primer paso importante hacia la realización de los derechos, la justicia y la rendición de cuentas, pero no puede proteger los derechos de forma aislada y debe ir acompañada de otras salvaguardias. Cuando no se pueda prevenir o mitigar el daño y las tecnologías sean incompatibles por diseño con el derecho internacional de los derechos humanos, dichas tecnologías deben prohibirse.

Principios rectores y marco

Los Estados tienen obligaciones y deberes vinculantes en virtud del derecho internacional de los derechos humanos, lo que significa que deben respetar, proteger y realizar los derechos humanos de todas las personas. Las organizaciones internacionales, las empresas y otros actores no estatales deben igualmente respetar los derechos humanos.

Para adoptar un enfoque basado en los derechos humanos en este ámbito temático, puede ser útil tener en cuenta algunos principios y marcos generales que deben aplicarse a cualquier tecnología potencial en el ámbito del asilo y la migración (y más en general). Entre ellos se incluyen:

La tecnología no es neutra. Los incentivos financieros y de otro tipo, los sistemas estructurales de poder y opresión, el racismo sistémico, la discriminación, la desigualdad sistémica y los entornos políticos se incorporan a la tecnología y se reproducen con su uso. En muchos casos, la tecnología es una herramienta que se utiliza para poner en práctica políticas subyacentes que pueden ser xenófobas o discriminatorias en fondo o en forma.

Adoptar un enfoque cauteloso y crítico hacia el "tecnosolucionismo", es decir, la idea de que los problemas sociales, económicos y políticos complejos pueden superarse mediante la tecnología. En lugar de dar por sentado que el desarrollo y la implementación de las tecnologías son necesarios o inevitables, y que sus riesgos pueden gestionarse mediante soluciones procedimentales, es importante cuestionar de forma esencial, desde el principio del proceso y de manera continua, si determinadas tecnologías son realmente necesarias o útiles, o si pueden abordar de manera significativa problemas sistémicos sin exacerbar ni crear inadvertidamente otros problemas.

Garantizar que todas las tecnologías respeten, protejan y promuevan los derechos humanos (tanto directa como indirectamente), entre otros, la no discriminación, la privacidad, el derecho a la vida, el derecho a solicitar asilo, el derecho a la libertad y el principio de no devolución. Esto también se aplica cuando las tecnologías se exportan a otras jurisdicciones.

La interseccionalidad es clave. Los Estados y las empresas deben evaluar los riesgos e impactos directos e indirectos del diseño y el uso de las tecnologías. Es algo que debe hacerse de forma temprana, durante la fase previa a la implementación y de forma continua, con una perspectiva interseccional. Ello significa que los Estados, las empresas y otros actores deben examinar cómo pueden las diferentes formas de discriminación superponerse e interactuar entre sí en cualquier momento para crear una experiencia particular y compleja de opresión para una persona o grupo que interactúa con las tecnologías.

Las medidas establecidas para regular las tecnologías deben ser **vinculantes y exigibles.** Este punto es especialmente importante, ya que ya existen muchos códigos éticos, códigos de conducta y líneas directrices poco estrictos y no vinculantes que, a menudo, no garantizan una protección adecuada.

La libertad de información es un componente crucial del derecho a la libertad de expresión.[11] Los Estados, las empresas y otros actores deben garantizar la **transparencia, la rendición de cuentas y la accesibilidad** de la información, entre otras cosas para permitir el examen público y la participación en la formulación de políticas de una serie de partes interesadas, incluidos los titulares de derechos afectados. Se incluye la transparencia sobre las funciones y responsabilidades de quienes participan en el desarrollo, la adquisición y la implementación. Si bien la transparencia es importante, solo es un primer paso y no es suficiente por sí sola.

Estados, empresas y demás actores deben asegurar una **participación significativa de las comunidades afectadas** y que los debates se centren en políticas en torno a sus necesidades y prioridades, posibilitando una participación en pie de igualdad de personas defensoras y organizaciones representativas gracias a la asignación de recursos, poniendo al mismo nivel a todas las partes interesadas y las personas titulares de derechos, así como reconociendo el valor del conocimiento adquirido a través de la experiencia. Esto incluye, fundamentalmente, dar voz y prioridad a las comunidades afectadas y a los actores de la sociedad civil de la mayoría global.

[11] Comité de Derechos Humanos de la ONU (12 de septiembre de 2011). Observación general Nº 34, Pacto Internacional de Derechos Civiles y Políticos. CCPR/C/GC/34, párrs. 18-19.https://docs.un.org/es/CCPR/C/GC/34

Recomendaciones

Recomendaciones a los Estados

Prohibiciones totales

Bajo ninguna circunstancia deben los Estados permitir el desarrollo, la producción, la venta, el uso, la exportación y la importación de tecnologías que, por su propia naturaleza, violen los derechos humanos, causen daños irreparables e irreversibles, o planteen riesgos inaceptables. En estos casos, los Estados deben promulgar prohibiciones totales. Entre las tecnologías que los Estados deben prohibir se incluyen:

- Sistemas automatizados de evaluación de riesgos, puntuación y elaboración de perfiles en el contexto de la gestión de la migración, el asilo y el control fronterizo (incluidos los sistemas de detección del fraude). Estos sistemas, utilizados para determinar si las personas en movimiento representan un "riesgo" de actividad ilícita o una amenaza para la seguridad, son intrínsecamente discriminatorios, ya que prejuzgan a las personas basándose en factores que escapan a su control o en inferencias discriminatorias basadas en sus características personales. Violan los derechos a la igualdad y la no discriminación, a la privacidad y a la protección de datos, así como la presunción de inocencia. También pueden dar lugar a violaciones injustas de los derechos al trabajo, a la libertad (mediante la detención ilícita), a un juicio justo, a la protección social o a la salud. El uso automatizado de perfiles debe prohibirse, dado el riesgo especialmente elevado de discriminación en este contexto.

- Tecnologías para procesar o inferir características personales sensibles o sustitutos de características, como la raza, la afiliación política, las creencias y los datos genéticos, sanitarios y biométricos, con el fin de evaluar la puntuación de riesgo individual.[12] Esto incluye el uso de datos relativos a la ciudadanía, la "afiliación extranjera" y la nacionalidad. Otros ejemplos de ello son el uso de datos sobre el código postal de una persona para inferir su situación socioeconómica o el recurso a datos sobre necesidades alimentarias como indicador de las creencias religiosas o del estado de salud.

- Tecnologías predictivas que generan predicciones sobre los lugares en los que hay riesgo de "migración irregular". Estos sistemas pueden utilizarse para facilitar respuestas preventivas destinadas a prohibir o detener los movimientos, a menudo por parte de terceros países que actúan como guardianes. Tales sistemas pueden dar lugar a políticas de control fronterizo punitivas y abusivas que utilizan sesgos y estereotipos raciales, impiden a las personas solicitar asilo, las exponen al riesgo de devolución y amenazan el derecho a la vida, la libertad y la seguridad de las personas.

[12] Lighthouse Reports (2023). Whistleblower reveals Netherlands' use of secret and potentially illegal algorithm to score visa applicants. Ethnic Profiling. https://www.lighthousereports.com/investigation/ethnic-profiling/

- Herramientas de reconocimiento de emociones basadas en la IA, como los "detectores de mentiras" y el análisis conductual. Sistemas como los "detectores de mentiras" basados en la IA son tecnologías pseudocientíficas que pretenden inferir emociones a partir de datos biométricos, mientras que el análisis conductual se utiliza para identificar a personas "sospechosas" basándose en su aspecto u otras características personales no relacionadas. Su uso refuerza un proceso de sospecha racializada con respecto a las personas migrantes y solicitantes de asilo, y puede automatizar suposiciones discriminatorias basadas en sesgos y estereotipos raciales y religiosos, lo cual amenaza los derechos a la no discriminación, a la privacidad, a la libertad y a un juicio justo. [13] La supuesta utilidad de estas tecnologías también se basa en nociones capacitistas de "normalidad" física, cognitiva y conductual con el objetivo de "remediar", "curar" y, en esencia, erradicar la discapacidad y la neurodiversidad.

- La identificación biométrica remota (IBR) retrospectiva (diferida), además de la IBR en vivo (en tiempo real), como el uso del reconocimiento facial. Estas tecnologías facilitan la vigilancia masiva y discriminatoria en todos los contextos, incluida la gestión de la migración y las fronteras. Pueden utilizarse para escanear las zonas fronterizas como medida disuasoria y como parte de un programa de prohibición más amplio, que impida a las personas solicitar asilo y socave las obligaciones de los Estados en virtud del derecho internacional, en particular la obligación de no devolución.

- La práctica de la extracción, el procesamiento, la fusión y la explotación masiva de los datos de las personas, incluido el intercambio de los datos recopilados entre las autoridades de migración, bienestar social, función policial y seguridad nacional. Esta práctica socava los principios establecidos de protección de datos y el derecho a la privacidad. También debe prohibirse el intercambio de datos individuales con terceros países a través de organismos supranacionales encargados de hacer cumplir la ley con el pretexto de la seguridad nacional, si no son necesarios ni proporcionados o si existe riesgo de violaciones de derechos humanos.

Antes de la implementación

Además de prohibir claramente las tecnologías incompatibles con los derechos humanos, ***los Estados deben, antes de implementar ningún sistema tecnológico:***

- Evaluar y demostrar la legalidad, la necesidad y la proporcionalidad de cualquier nueva tecnología digital, así como su valor e impacto. Cualquier tecnología adoptada debe estar en consonancia con

    - el marco y los principios internacionales de derechos humanos, incluida la prohibición de la discriminación;

    - las normas de protección de datos, incluidos los principios de legalidad, equidad y transparencia, limitación de la finalidad, recopilación de la cantidad mínima posible

[13] A civil society statement (2022). AI Act must protect all people, regardless of migration status. https://edri.org/wp-content/uploads/2022/12/Joint-Statement_The-EU-AI-Act-must-protect-people-on-the-move_December-2022.docx.pdf

de datos, exactitud, limitación del almacenamiento, integridad y confidencialidad (seguridad), y rendición de cuentas.[14]

- Abstenerse de promulgar leyes que faciliten la discriminación digital (y no digital), al reforzar y agravar los sistemas existentes de opresión y marginación.

- Promulgar marcos de gobernanza vinculantes que respeten los derechos exigibles en cuanto al desarrollo y la implementación de las tecnologías digitales, con el objetivo de proteger y promover los derechos de todas las personas, incluidas las migrantes, refugiadas y solicitantes de asilo. En particular, dichos marcos jurídicos deben estar libres de exenciones generales por motivos de seguridad nacional o similares, ya que tales exenciones no son necesarias ni proporcionadas y pueden tener efectos discriminatorios.

- Promulgar o modificar las normas, políticas y leyes establecidas para garantizar que el uso de sistemas de toma de decisiones automatizada en materia de asilo, migración y ámbitos relacionados no perpetúa la discriminación por motivos de ingresos, raza, etnia, religión, situación migratoria o cualquier otra característica, y que dicha implementación cumple las normas internacionales de derechos humanos pertinentes.

- Imponer obligaciones estrictas de rendición de cuentas y transparencia pública a todos los organismos públicos que despliegan tecnologías digitales, incluidas las autoridades de seguridad nacional, de aplicación de la ley, migratorias y de control de fronteras. Entre estas obligaciones se incluyen:

    - Crear una base de datos de acceso público en la que se les exija divulgar información sobre sus tecnologías digitales y su colaboración con desarrolladores privados de tecnologías, cuando sea pertinente, sobre dónde y cómo se utiliza o utilizará la tecnología.

    - Recopilar y divulgar datos e información oficiales desglosados sobre cualquier impacto discriminatorio, en virtud de la obligación de garantizar la igualdad y prevenir la discriminación racial.

    - Establecer un proceso de evaluación de riesgos para los derechos humanos y llevar a cabo sistemáticamente evaluaciones del impacto sobre los derechos humanos (EIDDHH) y sobre la protección de datos para identificar y mitigar los riesgos —efectos discriminatorios incluidos— para los derechos humanos de las personas objeto de las tecnologías y políticas de gobernanza digital de fronteras. Estas evaluaciones deben llevarse a cabo con suficientes recursos humanos y financieros y conocimientos especializados en materia de derechos humanos, e incluir datos desglosados por raza, etnia, género y otros motivos de discriminación, en consulta con las partes interesadas pertinentes, incluidas las personas afectadas por las tecnologías. Las conclusiones y el análisis de estas evaluaciones deben publicarse y

[14] The Data Protection Commission. Principles of Data Protection. https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection

estar a disposición del público, en aras de la transparencia. Un organismo público independiente con el mandato de hacer cumplir el marco de gobernanza digital aplicable debe supervisar los resultados y la aplicación de las recomendaciones. Estas evaluaciones también deben efectuarse de forma continua mucho antes de la implementación y a lo largo del ciclo de vida de las tecnologías. Cualquier riesgo identificado para los derechos humanos debe mitigarse y prevenirse antes de permitir la implementación de la tecnología. Debe prestarse especial atención a cualquier daño interseccional o impacto discriminatorio contra personas refugiadas y migrantes, grupos racializados, personas que viven en la pobreza, personas mayores, personas con discapacidad y otras poblaciones marginadas, así como niños, niñas y jóvenes. Si se determina que los riesgos para los derechos humanos no pueden mitigarse, debe suspenderse el uso de estas tecnologías.

- Evaluar y abordar todo impacto ambiental del desarrollo y la implementación de tecnologías, teniendo en cuenta la creciente evidencia de que estas tecnologías dependen en gran medida de los combustibles fósiles, ejercen una presión considerable sobre los recursos naturales, como la tierra y el agua, y exacerban el cambio climático y la degradación ambiental.[15]

- Adoptar leyes de diligencia debida obligatoria que exijan a las empresas involucradas en el desarrollo y suministro de tecnologías en el contexto del asilo, la migración y el control fronterizo —como los sistemas de macrodatos, IA y biométricos— que lleven a cabo la diligencia debida en materia de derechos humanos, en consonancia con las normas internacionales como los Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos y la Guía de la OCDE de debida diligencia.

- En la medida de lo posible, explorar cualquier vía alternativa no invasiva (o menos restrictiva de los derechos) que pueda satisfacer las necesidades o tareas identificadas sin comprometer indebidamente el derecho a la privacidad, la igualdad y la no discriminación, así como la libertad de no sufrir vigilancia ni otros abusos contra los derechos humanos.

- Garantizar el apoyo a las comunidades afectadas, las organizaciones de la sociedad civil y los especialistas en derechos humanos para que participen de manera significativa en el desarrollo y la implementación de las tecnologías de IA, así como en la aplicación, el seguimiento y la evaluación de la normativa pertinente en materia de IA.

- Promulgar medidas de protección de denunciantes para apoyar la rendición de cuentas pública por parte de desarrolladores e implementadores de tecnologías de IA.

Durante la implementación

Durante el ciclo de vida de las tecnologías, los Estados deben:

[15] A civil society statement (2025). Within Bounds: Limiting AI's environmental impact. https://greenscreen.network/en/blog/within-bounds-limiting-ai-environmental-impact/#:~:text=AI%20technologies%20must%20not%20be,to%20power%20new%20data%20centres

- Dar a las personas la oportunidad de conocer, dar o retirar su consentimiento libremente e impugnar cualquier medida destinada a obtener, agrupar, conservar y usar sus datos personales. Este paso debe llevarse a cabo a través del acceso a la información, en un idioma comprensible, y con una explicación clara sobre quién recoge los datos, qué datos se recopilan y cómo se utilizarán. Las personas deben disponer de una oportunidad real de elección, sin ningún tipo de coacción, manipulación o intimidación. Debe ser fácil retirar el consentimiento y lograr que se eliminen los datos, sin temor a represalias, algo que se aplica también cuando los datos se recopilan de forma involuntaria, por ejemplo, en el caso de imágenes de drones que capturan datos personales de forma involuntaria.

- Obligar a los implementadores de IA a informar a las personas cuando las decisiones que les afectan se basan en tecnologías de IA, incluida la toma de decisiones algorítmica. Este proceso debe incluir, como mínimo, información significativa y accesible sobre los pasos que dieron lugar a la evaluación de IA, cómo se trataron los datos y en qué medida influyeron en la decisión final de un responsable humano, así como información sobre el derecho a apelar y a obtener reparación y resarcimiento, y los mecanismos existentes para ejercer esos derechos.

- Cuando se produzcan violaciones, responsabilizar a desarrolladores e implementadores de los daños a los derechos humanos que hayan causado o contribuido a causar, así como de su falta de diligencia debida en materia de derechos humanos y protección de datos, exigiendo una reparación, según sea necesario.

- Garantizar que las personas que hayan sufrido violaciones de derechos humanos como consecuencia del uso indebido de las tecnologías tengan acceso a recursos efectivos, tanto judiciales como no judiciales, sin temor a poner en peligro las solicitudes de asilo en curso o el derecho existente a permanecer o entrar en el país. Las organizaciones de interés público deben poder prestar apoyo a las personas afectadas para que presenten denuncias, así como plantear casos por iniciativa propia, incluso mediante el acceso a la asistencia letrada gratuita.

- Eliminar cualquier impacto o efecto discriminatorio derivado del uso de las tecnologías digitales y adoptar medidas para prevenir cualquier forma de discriminación basada en el derecho internacional de los derechos humanos.

Recomendaciones a las empresas

Las empresas involucradas en cualquier momento del ciclo de vida de las tecnologías, incluidas las que se dedican al desarrollo y suministro de tecnologías para el asilo, la migración y la vigilancia de fronteras, deben:

- Respetar los derechos humanos en todos los lugares del mundo en los que operan y en todas sus actividades, adhiriéndose a los Principios rectores sobre las empresas y los

derechos humanos de la ONU, reconocidos a nivel global, y a las Líneas Directrices de la OCDE para Empresas Multinacionales sobre Conducta Empresarial Responsable.[16]

- Asumir la diligencia debida en materia de derechos humanos, llevando a cabo sistemáticamente evaluaciones del impacto sobre los derechos humanos (EIDDHH) y sobre la protección de datos, de conformidad con normas internacionales como los Principios rectores sobre las empresas y los derechos humanos de la ONU y las Líneas Directrices de la OCDE para Empresas Multinacionales sobre Conducta Empresarial Responsable.[17] Estas evaluaciones deben ser llevadas a cabo de forma temprana y continua por quienes implementan las tecnologías, con suficientes recursos humanos y financieros y conocimientos especializados en materia de derechos humanos, e incluir datos desglosados por raza, etnia, género, edad y otros motivos de discriminación, en consulta con las partes interesadas pertinentes, incluidas las personas afectadas por las tecnologías. Las conclusiones y el análisis de estas evaluaciones deben publicarse y estar a disposición del público, en aras de la transparencia. Un organismo público independiente con el mandato de hacer cumplir el marco de gobernanza digital aplicable debe supervisar los resultados y la aplicación de las recomendaciones. Estas evaluaciones también deben efectuarse de forma continua a lo largo del ciclo de vida de las tecnologías. Cualquier riesgo identificado para los derechos humanos, incluidos los posibles efectos discriminatorios, debe mitigarse o prevenirse antes de permitir o continuar la implementación de la tecnología. Debe prestarse especial atención a cualquier daño interseccional o impacto discriminatorio contra grupos racializados, personas que viven en la pobreza, personas mayores, personas con discapacidad y otras poblaciones marginadas, así como niños, niñas y jóvenes. Si se determina que los riesgos para los derechos humanos no pueden mitigarse, debe suspenderse el uso de estas tecnologías.

- Explorar y priorizar cualquier vía alternativa no invasiva que pueda satisfacer las necesidades identificadas sin comprometer indebidamente el derecho a la privacidad, la igualdad y la no discriminación, así como la libertad de no sufrir vigilancia ni otros abusos contra los derechos humanos.

- Proteger los datos personales para evitar que se usen con fines que violan derechos, lo que incluye garantizar el cumplimiento de los principios de recopilación de la cantidad mínima posible de datos, la seguridad de los datos recabados y de los dispositivos, aplicaciones, redes o servicios utilizados en su recopilación, transmisión, procesamiento y almacenamiento. Dar a las personas la oportunidad de conocer, dar o retirar su consentimiento libremente e impugnar cualquier medida destinada a obtener, agrupar,

[16] Oficina del Alto Comisionado de la ONU para las Naciones Unidas. (2011). Principios rectores sobre las empresas y los derechos humanos: Puesta en práctica del marco de las Naciones Unidas para "proteger, respetar y remediar" (2011), doc. ONU HR/PUB/11/04.https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_SP.pdf; Organización para la Cooperación y el Desarrollo Económicos (2023). Líneas Directrices de la OCDE para Empresas Multinacionales sobre Conducta Empresarial Responsable. https://doi.org/10.1787/81f92357-en

[17] Organización para la Cooperación y el Desarrollo Económicos (2018). Líneas Directrices de la OCDE para Empresas Multinacionales sobre Conducta Empresarial Responsable. https://doi.org/10.1787/15f5f4b3-en

conservar y usar sus datos personales. Este paso debe llevarse a cabo a través del acceso a la información, en un idioma comprensible, y con una explicación clara sobre quién recoge los datos, qué datos se recopilan y cómo se utilizarán. Las personas deben disponer de una oportunidad real de elección, sin ningún tipo de coacción, intimidación o manipulación. Debe ser fácil retirar el consentimiento y lograr que se eliminen los datos, sin temor a represalias, algo que se aplica también cuando los datos se recopilan de forma involuntaria, por ejemplo, en el caso de imágenes de drones que capturan datos personales de forma involuntaria.

- Evitar causar o contribuir a causar abusos contra los derechos humanos a través de sus propias actividades empresariales, y que hagan frente a las consecuencias negativas en las que tengan alguna participación, lo que incluye remediar cualquier abuso real. Debe tenerse en cuenta la cadena de suministro y el ciclo de vida del producto o la actividad, exportaciones incluidas. También deben incluirse los efectos discriminatorios involuntarios que se derivan del uso de las tecnologías digitales en la práctica.

- Prevenir o mitigar las consecuencias negativas sobre los derechos humanos relacionadas con operaciones, productos o servicios prestados por sus relaciones comerciales, incluso cuando no hayan contribuido a generarlos. Ejercer cualquier influencia que puedan tener en estas relaciones comerciales para mitigar y prevenir dichos riesgos e impactos.

- Adoptar mecanismos de transparencia y rendición de cuentas para divulgar información sobre sus tecnologías de IA, en especial dónde y cómo se utiliza o utilizará la tecnología.

- Abstenerse de presionar a los gobiernos para obtener concesiones o ventajas, como cambios en las leyes o políticas que puedan tener un impacto negativo en los derechos humanos de otras personas.

- Colaborar de forma proactiva y consultar de manera significativa a las organizaciones comunitarias, especialmente a aquéllas que representan a comunidades marginadas y a actores de la sociedad civil durante el desarrollo de tecnologías.

Recomendaciones a las organizaciones internacionales (incluidas las agencias de la ONU)

- Evaluar y demostrar la legalidad, la necesidad y la proporcionalidad del desarrollo o la implementación de cualquier nueva tecnología. Cualquier tecnología adoptada debe estar en consonancia con

    - el marco y los principios internacionales de derechos humanos, incluida la prohibición de la discriminación,

    - las normas de protección de datos, incluidos los principios de legalidad, equidad y transparencia, limitación de la finalidad, recopilación de la cantidad mínima posible

de datos, exactitud, limitación del almacenamiento, integridad, confidencialidad (seguridad) y rendición de cuentas.[18]

- Abordar los riesgos de que estas herramientas faciliten la discriminación y otros abusos contra los derechos humanos de cualquier persona, estableciendo un proceso de evaluación de riesgos para los derechos humanos y llevando a cabo sistemáticamente evaluaciones del impacto sobre los derechos humanos (EIDDHH) y sobre la protección de datos para identificar y mitigar los riesgos —efectos discriminatorios incluidos— para los derechos humanos de las personas objeto de las tecnologías y políticas de gobernanza digital de fronteras.

    - Estas evaluaciones deben llevarse a cabo con suficientes recursos humanos y financieros y conocimientos especializados en materia de derechos humanos, e incluir datos desglosados por raza, etnia, género y otros motivos de discriminación, en consulta con las partes interesadas pertinentes, incluidas las personas afectadas por las tecnologías.

    - Las conclusiones y el análisis de estas evaluaciones deben publicarse y estar a disposición del público, en aras de la transparencia.

    - Un organismo público independiente con el mandato de hacer cumplir el marco de gobernanza digital aplicable debe supervisar los resultados y la aplicación de las recomendaciones.

    - Estas evaluaciones también deben efectuarse de forma continua mucho antes de la implementación y a lo largo del ciclo de vida de las tecnologías.

    - Cualquier riesgo identificado para los derechos humanos debe mitigarse y prevenirse antes de permitir la implementación de la tecnología. Si se determina que los riesgos para los derechos humanos no pueden mitigarse, debe suspenderse el uso de estas tecnologías.

    - Debe prestarse especial atención a cualquier daño interseccional o impacto discriminatorio sobre personas y comunidades racializadas, personas refugiadas y migrantes, personas que viven en la pobreza, personas mayores, personas con discapacidad y otras poblaciones marginadas, así como niños, niñas y jóvenes.

- Explorar y priorizar cualquier vía alternativa no invasiva que pueda satisfacer las necesidades identificadas sin comprometer indebidamente el derecho a la privacidad, la igualdad y la no discriminación, así como la libertad de no sufrir vigilancia ni otros abusos contra los derechos humanos.

- Proteger los datos personales para evitar que se usen con fines que violan derechos, lo que incluye garantizar el cumplimiento de los principios de recopilación de la cantidad mínima

[18] La Autoridad de Protección de Datos. Principios de protección de datos. https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection

posible de datos, la seguridad de los datos recabados y de los dispositivos, aplicaciones, redes o servicios utilizados en su recopilación, transmisión, procesamiento y almacenamiento.

- Dar a las personas la oportunidad de conocer cualquier medida adoptada para recopilar, agregar, conservar y usar sus datos personales —datos biométricos incluidos—, de dar o retirar libremente su consentimiento para ello y de impugnar estas prácticas. Este paso debe llevarse a cabo a través del acceso a la información, en un idioma comprensible, y con una explicación clara sobre quién recoge los datos, qué datos se recopilan y cómo se utilizarán. Las personas deben disponer de una oportunidad real de elección, sin ningún tipo de coacción, manipulación o intimidación. Debe ser fácil retirar el consentimiento y lograr que se eliminen los datos, sin temor a represalias, incluida la negación del acceso a derechos o servicios. Esto también se aplica cuando los datos se recopilan de forma involuntaria.

- Informar a las personas cuando las decisiones que les afectan se basan en tecnologías de IA, incluida la toma de decisiones algorítmica. Este proceso debe incluir, como mínimo, información significativa y accesible sobre los pasos que dieron lugar a la evaluación de IA, cómo se trataron los datos y en qué medida influyeron en la decisión final de un responsable humano, así como información sobre el derecho a apelar y a obtener reparación y resarcimiento, y los mecanismos existentes para ejercer esos derechos.

- Garantizar que las personas que han sufrido violaciones de derechos humanos como resultado del uso indebido de tecnologías tengan acceso a una reparación efectiva.

- Incorporar salvaguardias explícitas y específicas contra el abuso de cualquier uso de las tecnologías, incluido el intercambio de datos con organismos de seguridad nacional o Estados de origen que puedan dar lugar a violaciones de derechos humanos.

- Garantizar que las comunidades afectadas puedan participar de manera significativa en el desarrollo y la implementación de las tecnologías de IA, así como en su aplicación, seguimiento y evaluación.

- Actuar de conformidad con las responsabilidades pertinentes en materia de derechos humanos y garantizar que ningún apoyo, incluidos los programas de financiación y asistencia técnica, conduce a la proliferación de tecnologías que dan lugar a la violación de derechos de las personas migrantes, refugiadas y solicitantes de asilo.

Recomendaciones a otros proveedores de servicios

A los proveedores de servicios que utilizan tecnologías digitales en los ámbitos del asilo, la migración, la vigilancia de fronteras y la ayuda humanitaria, incluidas las organizaciones no gubernamentales (ONG) y los proveedores de servicios humanitarios sin ánimo de lucro:

- Respetar los derechos humanos en todos los lugares del mundo en los que operan y en todas sus actividades, en especial adhiriéndose a los Principios rectores

sobre las empresas y los derechos humanos de la ONU, reconocidos a nivel global, a las Líneas Directrices de la OCDE para Empresas Multinacionales sobre Conducta Empresarial Responsable[19] y a las normas Esfera.[20]

- Abordar los riesgos de que las tecnologías digitales faciliten la discriminación y otros abusos contra los derechos humanos de cualquier persona, entre otras cosas mediante la realización de evaluaciones del impacto sobre los derechos humanos (EIDDHH), prestando especial atención al impacto interseccional sobre personas y comunidades racializadas, personas refugiadas y migrantes, personas que viven en la pobreza, personas mayores, personas con discapacidad y otras poblaciones marginadas, así como niños, niñas y jóvenes.

- Explorar y priorizar cualquier vía alternativa no invasiva que pueda satisfacer las necesidades identificadas sin comprometer indebidamente el derecho a la privacidad, la igualdad y la no discriminación, así como la libertad de no sufrir vigilancia ni otros abusos contra los derechos humanos.

- Proteger los datos personales para evitar que se usen con fines que violan derechos, lo que incluye garantizar el cumplimiento de los principios de recopilación de la cantidad mínima posible de datos, la seguridad de los datos recabados y de los dispositivos, aplicaciones, redes o servicios utilizados en su recopilación, transmisión, procesamiento y almacenamiento. Dar a las personas la oportunidad de conocer cualquier medida adoptada para recopilar, agregar, conservar y usar sus datos personales —datos biométricos incluidos—, de dar o retirar libremente su consentimiento para ello y de impugnar estas prácticas. Este paso debe llevarse a cabo a través del acceso a la información, en un idioma comprensible, y con una explicación clara sobre quién recoge los datos, qué datos se recopilan y cómo se utilizarán. Las personas deben disponer de una oportunidad real de elección, sin ningún tipo de coacción, manipulación o intimidación. Debe ser fácil retirar el consentimiento y lograr que se eliminen los datos, sin temor a represalias, incluida la negación del acceso a derechos o servicios.

- Incorporar salvaguardias explícitas y específicas contra el abuso de cualquier uso de las tecnologías, incluido el intercambio de datos con organismos de seguridad nacional o Estados de origen que puedan dar lugar a violaciones de derechos humanos.

[19] Oficina del Alto Comisionado de la ONU para las Naciones Unidas. (2011). Principios rectores sobre las empresas y los derechos humanos: Puesta en práctica del marco de las Naciones Unidas para "proteger, respetar y remediar" (2011), doc. ONU HR/PUB/11/04.https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_SP.pdf; Organización para la Cooperación y el Desarrollo Económicos (2023). Líneas Directrices de la OCDE para Empresas Multinacionales sobre Conducta Empresarial Responsable. https://doi.org/10.1787/81f92357-en

[20] Esfera. Normas humanitarias. https://spherestandards.org/es/normas-humanitarias/

Contacto

Dirijan sus preguntas, motivos de preocupación y comentarios, incluidos los referidos a la accesibilidad de este documento y las solicitudes de traducción a charlotte.phillips@amnesty.org y mher.hakobyan@amnesty.org.

Recursos

- Amnistía Internacional. Manual general: Defender los derechos de las personas refugiadas y migrantes en la era digital, febrero de 2024. Índice AI: POL 40/7654/2024. https://www.amnesty.org/es/documents/pol40/7654/2024/es/
- Amnistía Internacional. Letter: The EU must respect human rights of migrants in the AI Act, abril de 2023 – Oficina de Amnistía Internacional ante las Instituciones Europeas. https://www.amnesty.eu/news/the-eu-must-respect-human-rights-of-migrants-in-the-ai-act/
- Amnistía Internacional. Hacer realidad el derecho a la seguridad social. Informe para la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2024. Índice AI: IOR 40/7558/2024. https://www.amnesty.org/es/documents/ior40/7558/2024/es/
- Amnistía Internacional. Denmark: Coded Injustice: Surveillance and Discrimination in Denmark's automated welfare state, 2024. Índice AI: EUR 18/8709/2024. https://www.amnesty.org/en/latest/news/2024/11/denmark-ai-powered-welfare-system-fuels-mass-surveillance-and-risks-discriminating-against-marginalized-groups-report/#:~:text=The%20Danish%20welfare%20authority%2C%20Udbetaling%20Danmark%20%28UDK%29%2C%20risks,Amnesty%20International%20said%20today%20in%20a%20new%20report.
- Denmark: Easy-to-read version: Coded Injustice: Surveillance and Discrimination in Denmark's automated welfare state, 21 de mayo de 2025, Índice AI: EUR 18/9419/2025. https://www.amnesty.org/es/documents/eur18/9419/2025/en/
- Amnistía Internacional. La frontera digital: Migración, tecnología y desigualdad, 21 de mayo de 2024, Índice AI: POL 40/7772/2024. https://www.amnesty.org/es/documents/pol40/7772/2024/es/
- Coalición #Protect Not Surveil, de la que Amnistía Internacional forma parte. Véase el sitio web: EU AI | Protect Not Surveil. https://protectnotsurveil.eu/
- #ProtectNotSuveil coalition, Joint Statement, A dangerous precedent: how the EU AI Act fails migrants and people on the move, 13 de marzo de 2024. https://www.accessnow.org/press-release/joint-statement-ai-act-fails-migrants-and-people-on-the-move/
- #ProtectNotSuveil, Joint Statement, the EU Migration Pact: a dangerous regime of migrant surveillance, 10 de abril de 2024. https://www.accessnow.org/press-release/joint-statement-eu-migration-pact-a-dangerous-regime-of-migrant-surveillance/
- Amnistía Internacional, Estados Unidos/Global: La tecnología de Palantir y Babel Street amenaza con someter a vigilancia a manifestantes y migrantes en favor de Palestina, agosto de 2025. https://www.amnesty.org/es/latest/news/2025/08/usa-global-tech-made-by-palantir-and-babel-street-pose-surveillance-threats-to-pro-palestine-student-protestors-migrants/