



Asamblea General

Distr. general
17 de diciembre de 2021
Español
Original: inglés

Consejo de Derechos Humanos

48º período de sesiones

13 de septiembre a 1 de octubre de 2021

Tema 9 de la agenda

**Racismo, discriminación racial, xenofobia y formas
conexas de intolerancia: seguimiento y aplicación
de la Declaración y el Programa de Acción de Durban**

Discriminación racial y xenofobia y uso de tecnologías digitales en el control de fronteras e inmigración

Informe de la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia, E. Tendayi Achiume*

Resumen

El presente informe complementa el informe de la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia, E. Tendayi Achiume, presentado al Consejo de Derechos Humanos en su 44º período de sesiones, titulado “La discriminación racial y las tecnologías digitales emergentes: un análisis de los derechos humanos”. En el presente informe, la Relatora Especial pone de relieve cómo se están utilizando las tecnologías digitales para el trato xenófobo y racialmente discriminatorio y la exclusión de las personas migrantes, refugiadas y apátridas. En algunos casos, la discriminación y la exclusión se producen en ausencia de una animadversión explícita, pero como resultado de la búsqueda de la eficiencia burocrática y humanitaria sin las necesarias salvaguardias de los derechos humanos. Además, la Relatora Especial subraya que los enormes beneficios económicos asociados al blindaje y la digitalización de las fronteras son una parte importante del problema.

* Este informe se presentó con retraso para incluir en él la información más reciente.



Índice

	<i>Página</i>
I. Introducción	3
II. El auge de las fronteras digitales	5
III. Cartografía de la discriminación racial y xenófoba en el control digital de las fronteras y de la inmigración	9
A. Discriminación directa e indirecta	9
B. Estructuras discriminatorias	13
IV. Recomendaciones	22

I. Introducción

1. En el presente informe, la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia, E. Tendayi Achiume, desarrolla el análisis que inició en el informe que presentó al Consejo de Derechos Humanos en su 44º período de sesiones, titulado “La discriminación racial y las tecnologías digitales emergentes: un análisis de los derechos humanos”¹. En ese informe, la Relatora Especial adoptó un enfoque basado en la igualdad para la gobernanza de los derechos humanos en el ámbito de las tecnologías digitales emergentes, centrándose en la intersección de esas tecnologías con los principios de igualdad racial y no discriminación en virtud del derecho internacional de los derechos humanos. Instó a los actores estatales y no estatales a ir más allá de las estrategias de “daltonismo racial” o “neutralidad racial”, que pasan por alto los efectos raciales y étnicos de las tecnologías digitales emergentes, y a enfrentarse directamente a las formas interseccionales de discriminación que se derivan de la adopción generalizada de esas tecnologías y que resultan agravadas por ellas. Ese enfoque implica, asimismo, no limitarse a las tendencias de los marcos reguladores y de derechos humanos de centrarse en exclusiva en los prejuicios explícitos en la labor por prohibir la discriminación racial. En su informe anterior, la Relatora Especial examinó la discriminación por motivos de raza, etnia y condición de indígena, y llamó la atención sobre los efectos del género, la religión y la condición de discapacidad. En el presente informe, aporta un matiz adicional al centrarse en las repercusiones xenófobas y racialmente discriminatorias de las tecnologías digitales emergentes para las personas migrantes, apátridas, refugiadas y no ciudadanas, así como para los pueblos nómadas y otros con tradiciones migratorias. En este análisis, el término “refugiados” incluye a las personas solicitantes de asilo que se ajustan a la definición de refugiado pero cuya condición de refugiadas no ha sido reconocida formalmente por ningún Estado. Además, la Relatora Especial examina de qué manera el despliegue de las tecnologías digitales emergentes para contener la pandemia de enfermedad por coronavirus (COVID-19) ha acelerado esas tendencias discriminatorias.

2. Las tecnologías digitales desempeñan actualmente un papel central en la mediación del disfrute de los derechos fundamentales, dado que los Estados y las empresas privadas dependen de esas tecnologías para suministrar bienes y servicios esenciales². Los expertos han acuñado la expresión “fronteras digitales”³ para hablar de las fronteras cuya infraestructura se basa cada vez más en el aprendizaje automático, los macrodatos, los sistemas algorítmicos automatizados de toma de decisiones, el análisis predictivo y las tecnologías digitales conexas. Esas tecnologías forman parte de los documentos y sistemas de identificación, los sistemas de reconocimiento facial, los sensores terrestres, los drones de videovigilancia aérea, las bases de datos biométricos e incluso los procesos de toma de decisiones en materia de concesión de visados y asilo. En los últimos tiempos, el control de las fronteras y de la inmigración ha experimentado una digitalización acelerada en respuesta a la pandemia de COVID-19.

3. Aunque las tecnologías digitales emergentes están ahora presentes en la gobernanza de todos los aspectos de la sociedad, existen preocupaciones singulares en el contexto de las fronteras y la inmigración por al menos dos razones. En la mayoría de los marcos nacionales de gobernanza, si no en todos:

a) Las personas no ciudadanas y apátridas y los grupos afines tienen menos derechos y protecciones jurídicas frente al abuso de poder del Estado, y pueden ser objeto de formas únicas de violencia privada xenófoba;

b) El poder ejecutivo y otros poderes del Estado conservan amplias facultades discrecionales y no revisables en el ámbito del control de las fronteras y de la inmigración, que no están sujetas a las limitaciones sustantivas y de procedimiento que suelen garantizarse a los ciudadanos.

¹ [A/HRC/44/57](#).

² Véanse, por ejemplo, [A/74/493](#), [A/73/348](#) y [A/HRC/44/57](#).

³ Véase, por ejemplo, Dennis Broeders, “The new digital borders of Europe: EU databases and the surveillance of irregular migrants”, *International Sociology*, vol. 22, núm. 1 (2007), págs. 71 a 92.

4. Las personas refugiadas, migrantes y apátridas son objeto de las vulneraciones enumeradas en el presente informe debido a su origen nacional, su raza, su etnia, su religión y otros motivos inadmisibles. Esas vulneraciones no pueden descartarse como formas admisibles de distinguir entre ciudadanos y no ciudadanos. A ese respecto, la Relatora Especial llama la atención sobre su informe relativo a la discriminación racial en el contexto de las leyes, las políticas y las prácticas relativas a la ciudadanía, la nacionalidad y la situación migratoria⁴.

5. Las fronteras digitales aumentan el alcance y la precisión del funcionamiento racialmente discriminatorio de las fronteras. Los Gobiernos y los actores no estatales están desarrollando y desplegando tecnologías digitales emergentes de forma singularmente experimental y peligrosa en el contexto del control de las fronteras y de la inmigración. Mediante esa labor, están sometiendo a las personas refugiadas, migrantes, apátridas y a otras personas a violaciones de los derechos humanos, y extrayendo grandes cantidades de datos de esos grupos en condiciones de explotación que los despojan de la potestad y la dignidad humanas fundamentales. Aunque la Relatora Especial se centra en el presente informe en las últimas innovaciones tecnológicas, muchas de esas tecnologías tienen antecedentes históricos en las tecnologías coloniales de la gobernanza racializada.

6. El análisis que figura en el anterior informe de la Relatora Especial sobre la discriminación racial y las tecnologías digitales emergentes proporciona información de fondo esencial. Ese informe es especialmente útil para explicar los mecanismos que hacen posible que las tecnologías digitales emergentes den lugar a la discriminación racial y para poner de relieve los factores económicos, políticos y sociales que impulsan la expansión del uso discriminatorio de esas tecnologías. En el presente informe, la Relatora Especial reitera que —a pesar de la sensación generalizada de que las tecnologías digitales emergentes son neutrales y objetivas en su funcionamiento—, la raza, el origen étnico, el origen nacional y la situación en materia de ciudadanía determinan el acceso a los derechos humanos y su disfrute en todos los campos en los que estas tecnologías están actualmente generalizadas. Los Estados tienen la obligación de prevenir, combatir esa discriminación racial y corregir esa situación, y los agentes privados, como las empresas, tienen la responsabilidad conexas de hacer otro tanto. En el contexto del control de las fronteras y de la inmigración, la prevención de las violaciones de los derechos humanos puede exigir la prohibición total o la supresión de las tecnologías debido a la incapacidad de controlar o mitigar sus efectos.

7. La tecnología no solo no es neutral, sino que su diseño y uso suelen reforzar las tendencias sociales, políticas y económicas dominantes. Como se ha destacado en informes anteriores, el resurgimiento del populismo etnonacionalista a nivel mundial ha tenido graves consecuencias xenófobas y de discriminación racial para las personas refugiadas, migrantes y apátridas⁵. En el presente informe, la Relatora Especial pone de relieve cómo se están desplegando las tecnologías digitales para promover las ideologías xenófobas y racialmente discriminatorias que han proliferado en parte debido a la percepción generalizada de las personas refugiadas y migrantes como amenazas *per se* para la seguridad nacional. En otros casos, la discriminación y la exclusión no se producen debido a una animadversión explícita, sino como resultado de la búsqueda de la eficiencia burocrática y humanitaria sin las necesarias salvaguardias de los derechos humanos. El blindaje actual de las fronteras y los cuantiosos beneficios económicos conexos son una parte importante del problema.

8. El presente informe se ha beneficiado de las valiosas contribuciones de los expertos que participaron en las reuniones organizadas por el Promise Institute for Human Rights de la Facultad de Derecho de la Universidad de California en Los Ángeles (UCLA), el Center for Critical Internet Inquiry de esa misma universidad, el Institute on Statelessness and Inclusion y el colectivo Migration and Technology Monitor; de las entrevistas con investigadores, incluidas personas apátridas, migrantes y refugiadas; y de las comunicaciones recibidas de una serie de interesados en respuesta a una convocatoria pública de presentación de comunicaciones. Las comunicaciones no confidenciales se pueden consultar en línea⁶.

⁴ A/HRC/38/52.

⁵ Véase, por ejemplo, A/73/312.

⁶ Véase <https://www.ohchr.org/EN/Issues/Racism/SRRacism/Pages/CallRaceBordersDigitalTechnologies.aspx>.

II. El auge de las fronteras digitales

9. La tecnología siempre ha formado parte del control de las fronteras y de la inmigración, y los instrumentos que abarcan desde los pasaportes hasta los muros físicos de las fronteras se conciben correctamente como ejemplos de esa tecnología. En el presente informe, la Relatora Especial se centra específicamente en la creciente preeminencia de las tecnologías digitales en el control de las fronteras y de la inmigración. La pandemia de COVID-19 ha acelerado esa tendencia al fomentar la dependencia de las soluciones tecnológicas para los retos migratorios. La “industria fronteriza” ha comenzado a abogar por la tecnología “biométrica sin contacto” para combatir la propagación del virus⁷, y las preocupaciones por la salud pública y la seguridad nacional se utilizan para justificar el aumento del seguimiento y la recopilación de datos sobre los migrantes⁸.

10. En general, las tecnologías digitales en las fronteras están reforzando los regímenes fronterizos paralelos que segregan la movilidad y la migración de diferentes grupos en función del origen nacional y la clase social, entre otros motivos. Los controles fronterizos automatizados son un ejemplo de regímenes fronterizos paralelos en acción. En los puntos de entrada a Irlanda, como el aeropuerto de Dublín, los titulares de pasaportes electrónicos de la Unión Europea, el Espacio Económico Europeo y Suiza pueden cruzar las puertas electrónicas de autoservicio para pasar el control de inmigración⁹. Solo las personas de determinadas nacionalidades —es decir, los nacionales de países predominantemente blancos y acomodados (y del Japón)— pueden utilizar la opción de autoservicio; las demás personas que viajen a Irlanda por vía aérea o marítima deberán presentarse ante un funcionario de inmigración a su llegada.

11. En las fronteras digitales se utiliza ampliamente la biometría, que se define como el reconocimiento automatizado de las personas a partir de sus características biológicas y de comportamiento¹⁰. La biometría puede recurrir a las huellas dactilares, los escaneos de retina y el reconocimiento facial, así como al reconocimiento de los patrones de las venas y los vasos sanguíneos de una persona, la forma de las orejas y el modo de andar. La biometría se utiliza para establecer, inscribir y verificar la identidad de las personas migrantes y refugiadas. Por ejemplo, las Naciones Unidas han recogido los datos biométricos de más de ocho millones de personas, la mayoría de las cuales huyen de conflictos o necesitan asistencia humanitaria¹¹. Los investigadores han documentado los orígenes racializados de las tecnologías biométricas¹², así como su uso contemporáneo, que es discriminatorio por motivos de raza, etnia y género¹³. En un informe sobre la tecnología de reconocimiento facial desplegada en contextos de cruce de fronteras, como los aeropuertos, se ha observado que, aunque los mejores algoritmos reconocen erróneamente a las mujeres negras 20 veces más que a los hombres blancos, la utilización de estas tecnologías está aumentando en todo el mundo¹⁴. En consecuencia, cuando se aplica el reconocimiento facial como tecnología de control de acceso, se excluye a los viajeros de los mecanismos de control fronterizo en función de la raza, el sexo y otras características demográficas (por ejemplo, el país de origen)¹⁵. Este trato diferencial suele perpetuar los estereotipos negativos y puede incluso entrañar una discriminación prohibida que podría dar lugar a la devolución.

12. La recopilación gubernamental y humanitaria de datos biométricos de refugiados y migrantes se ha relacionado con graves violaciones de los derechos humanos de esos grupos,

⁷ Véase <https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf>.

⁸ Véase <https://www.opendemocracy.net/en/pandemic-border/covid-19-can-technology-become-tool-oppression-and-surveillance/>.

⁹ Comunicación del Consejo de Inmigración de Irlanda.

¹⁰ Véase <https://www.biometricsinstitute.org/what-is-biometrics/>.

¹¹ Es bien sabido que estos vastos conjuntos de datos son difíciles de rastrear y también pueden incluir la reconversión de datos antiguos a partir de datos recién recogidos. Véase, por ejemplo, [youtube.com/watch?v=7qt4U7elpiA](https://www.youtube.com/watch?v=7qt4U7elpiA) y [youtube.com/watch?v=DgYs1scVHYM](https://www.youtube.com/watch?v=DgYs1scVHYM).

¹² Véase, por ejemplo, Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Duke University Press, 2015).

¹³ [A/HRC/44/57](https://www.a/hrc/44/57).

¹⁴ Tamir Israel, *Facial Recognition at a Crossroads: Transformation at our Borders and Beyond* (2020).

¹⁵ *Ibid*, pág. 158.

a pesar de las justificaciones burocráticas y humanitarias que se esconden tras la recopilación de dichos datos. Además, no está claro qué sucede con los datos, ni si los grupos afectados tienen acceso a sus propios datos. El Programa Mundial de Alimentos (PMA), por ejemplo, ha sido criticado por celebrar un contrato de 45 millones de dólares de los Estados Unidos con la empresa de minería de datos Palantir Technologies y por compartir datos sobre 92 millones de receptores de ayuda¹⁶. Empresas privadas como Palantir han demostrado ser esenciales en el suministro de la tecnología en que se sustentan los programas de detención y deportación gestionados por el Servicio de Inmigración y Control de Aduanas del Departamento de Seguridad Nacional de los Estados Unidos¹⁷, lo que suscita una preocupación fundada por la complicidad de las empresas en las violaciones de derechos humanos asociadas a esos programas. Todavía no está claro qué mecanismo de rendición de cuentas sobre el intercambio de datos se establecerá para la alianza entre el PMA y Palantir, ni si los interesados podrán renunciar a participar¹⁸. La recopilación de datos no es un ejercicio apolítico, especialmente cuando entidades poderosas del Norte Global recogen información sobre grupos de población vulnerables sin estar sujetas a métodos regulados de supervisión y rendición de cuentas¹⁹. La cada vez más acérrima recopilación de datos sobre los grupos de población migrantes ha sido criticada por su capacidad potencial para provocar importantes violaciones de la privacidad y problemas de derechos humanos²⁰.

13. La historia brinda numerosos ejemplos de los resultados discriminatorios e incluso mortales de la labor de recopilación de datos sobre grupos marginados. La Alemania nazi recopiló estratégicamente grandes cantidades de datos sobre las comunidades judías para facilitar el Holocausto, en gran parte en colaboración con una empresa privada: IBM²¹. Otros genocidios también se han basado en el seguimiento sistemático de grupos: el genocidio ruandés, por ejemplo, se vio facilitado por los registros de tarjetas de identidad que identificaban a los tutsis por su etnia²². Desde el 11 de septiembre de 2001, los Estados Unidos de América han probado diversos modos de recopilación de datos sobre grupos de población marginados, incluidas fotografías, información biométrica e incluso entrevistas en primera persona respecto a más de 84.000 personas señaladas que en su mayoría procedían de Estados árabes²³. En todos esos casos, diferentes actores, incluidos los Gobiernos, han explotado las ideas sobre la neutralidad o la necesidad no prejuiciosa de la recopilación de datos para dirigirse a distintos grupos marginados de forma discriminatoria.

14. Las tecnologías autónomas también se utilizan cada vez más en la vigilancia y la seguridad de los espacios fronterizos. Por ejemplo, la Agencia Europea de la Guardia de Fronteras y Costas (Frontex) ha estado probando en el Mediterráneo y el Egeo drones de uso militar para vigilar e interceptar embarcaciones con migrantes y refugiados que esperan llegar a las costas europeas²⁴. En octubre de 2020, una investigación aportó pruebas creíbles de que Frontex había sido cómplice de “devoluciones en caliente”²⁵ (es decir, la devolución forzosa de refugiados y migrantes a través de una frontera sin tener en cuenta las circunstancias de las personas y sin permitirles solicitar asilo o presentar un recurso). Es probable que las devoluciones en caliente vulneren las obligaciones de no devolución de los Estados en virtud del derecho internacional; aun así, se llevan a cabo con la ayuda de tecnologías de vigilancia.

¹⁶ Véase <https://www.thenewhumanitarian.org/news/2019/02/05/un-palantir-deal-data-mining-protection-concerns-wfp>.

¹⁷ Véase <https://www.technologyreview.com/2018/10/22/139639/amazon-is-the-invisible-backbone-behind-ices-immigration-crackdown/>.

¹⁸ Véase <https://www.devex.com/news/opinion-the-wfp-and-palantir-controversy-should-be-a-wake-up-call-for-humanitarian-community-94307>.

¹⁹ Véase <https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees/>.

²⁰ Véase <https://www.chathamhouse.org/2018/03/beware-notion-better-data-lead-better-outcomes-refugees-and-migrants>.

²¹ Edwin Black, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*, 2ª ed. (Dialog Press, 2012).

²² Véase <https://www.theengineroom.org/dangerous-data-the-role-of-data-collection-in-genocides/>.

²³ Véase <http://www.aaiusa.org/nseers>.

²⁴ Véase <https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf>.

²⁵ Véase <https://www.bellingcat.com/news/2020/10/23/frontex-at-fault-european-border-force-complicit-in-illegal-pushbacks>; y <https://www.spiegel.de/international/europe/eu-border-agency-frontex-complicit-in-greek-refugee-pushback-campaign-a-4b6cba29-35a3-4d8c-a49f-a12daad450d7>.

Las novedades legislativas en Grecia han permitido a la policía utilizar drones para vigilar la inmigración irregular en las regiones fronterizas, pero sin garantizar la necesaria protección jurídica de los derechos humanos de las personas sujetas a esa vigilancia²⁶.

15. La utilización de tecnología autónoma militar, o casi militar, refuerza el nexo entre la inmigración, la seguridad nacional, la creciente criminalización de la migración y el uso de taxonomías basadas en el riesgo para delimitar los casos e incluir una indicación al respecto²⁷. Los Estados, sobre todo los que reciben un gran número de refugiados y migrantes, han estado utilizando diversos métodos para prejuzgar y disuadir a las personas que tratan de solicitar legalmente el asilo. Este cambio normativo hacia la criminalización del asilo y la migración sirve para justificar tecnologías cada vez más duras e intrusivas, como los drones, y diversos mecanismos de control fronterizo, como los sensores remotos y las torres fijas integradas con cámaras infrarrojas (las llamadas torres de vigilancia autónomas) para mitigar el “entorno de amenaza” en la frontera²⁸. Esas tecnologías pueden tener resultados drásticos. Aunque las llamadas tecnologías de “fronteras inteligentes” han sido calificadas como una alternativa más humana a otros regímenes de control fronterizo, la utilización de esas tecnologías a lo largo de la frontera entre México y los Estados Unidos ha aumentado en realidad las muertes de migrantes y ha llevado las rutas migratorias hacia terrenos más peligrosos²⁹. De hecho, las muertes de migrantes se han duplicado con creces desde que se adoptaron estas nuevas tecnologías³⁰, al crear una “tierra de tumbas abiertas”³¹.

16. Es probable que el uso de esas tecnologías por parte de los organismos de control fronterizo solo aumente en el “régimen tecnológico militarizado”³² de los espacios fronterizos, sin que haya una consulta pública adecuada, marcos de rendición de cuentas o mecanismos de supervisión. En la zona desmilitarizada de la península de Corea, la República de Corea ha desplegado armas estacionarias semiautónomas operadas a distancia³³. El Gobierno de la República de Corea ha declarado que no tiene intención de desarrollar o adquirir sistemas de armas autónomos letales³⁴. Sin embargo, debido a la falta de transparencia, la situación del despliegue de los sistemas de armas autónomos en las fronteras es a menudo difícil de determinar. Antes de cualquier despliegue de ese tipo, es crucial que los Estados tengan en cuenta y combatan los efectos desproporcionados de origen racial, étnico y nacional que las armas totalmente autónomas tendrían sobre los grupos vulnerables, especialmente las personas refugiadas, migrantes, solicitantes de asilo y apátridas.

17. Los Estados Miembros y las entidades de las Naciones Unidas recurren cada vez más al análisis de macrodatos para fundamentar sus políticas. Por ejemplo, la Matriz de Seguimiento de los Desplazamientos de la Organización Internacional para las Migraciones (OIM)³⁵ sigue de cerca a los grupos de población en movimiento para predecir mejor las necesidades de las personas desplazadas, utilizando registros de teléfonos móviles y geoetiquetas, así como análisis de la actividad en los medios sociales. En los Estados Unidos también se están utilizando análisis de macrodatos para predecir la probabilidad de éxito de las personas refugiadas reasentadas en función de los vínculos comunitarios que existían con anterioridad³⁶. En un panorama mundial cada vez más contrario a la inmigración, se ha criticado que los datos relacionados con la migración también se hayan malinterpretado y

²⁶ Comunicación de Homo Digitalis.

²⁷ Comunicación de Dimitri Van Den Meerse.

²⁸ Raluca Csernaton, “Constructing the EU’s high-tech borders: Frontex and dual-use drones for border management”, *European Security*, vol. 27, núm. 2 (2018), págs. 175 a 200.

²⁹ Samuel Norton Chambers *et al.*, “Mortality, surveillance and the tertiary ‘funnel effect’ on the US-Mexico border: a geospatial modeling of the geography of deterrence”, *Journal of Borderland Studies*, vol. 36, núm. 3 (2019), págs. 443 a 468.

³⁰ *Ibid.*

³¹ Jason De León, *The Land of Open Graves: Living and Dying on the Migrant Trail* (University of California Press, 2015).

³² Raluca Csernaton, “Constructing the EU’s high-tech borders”.

³³ Comunicación de Campaign to Stop Killer Robots.

³⁴ *Ibid.*

³⁵ Véase <https://dtm.iom.int/about>.

³⁶ Véase <https://news.stanford.edu/2018/01/18/algorithm-improves-integration-refugees/>.

tergiversado con fines políticos, por ejemplo, para influir en la distribución de la ayuda. Los datos inexactos también pueden utilizarse para avivar el miedo y la xenofobia, como se ha visto en la caracterización del grupo de migrantes que intentan pedir asilo en la frontera entre los Estados Unidos y México³⁷ o en el impulso de los sentimientos antimigrantes en la región del Mediterráneo, incluidos los muros flotantes que se han propuesto recientemente³⁸. El miedo de la sociedad se utiliza posteriormente para justificar respuestas cada vez más duras que contravienen el derecho internacional de los derechos humanos³⁹. Como se ha señalado, en contextos políticos polarizados, contrarios a la inmigración e incluso xenófobos, los datos utilizados para moldear los algoritmos de aprendizaje automático en las fronteras o utilizados en las campañas políticas o en la legislación pueden ser erróneos, y en un entorno de sesgo estructural contra las minorías esa tergiversación de los datos puede alimentar la desinformación, el discurso del odio y la violencia⁴⁰.

18. Para evaluar el panorama de los derechos humanos en las fronteras digitales es fundamental el papel de las empresas privadas, cuyo afán de lucro ha contribuido de manera importante al impulso de la expansión de la tecnología digital en el control de las fronteras y de la inmigración, a menudo en forma de alianzas que permiten a los Gobiernos abdicar de la responsabilidad por las violaciones que puedan derivarse del empleo de esas tecnologías. El término “complejo industrial fronterizo” se ha utilizado para describir el nexo entre la vigilancia y la militarización de las fronteras y los intereses financieros⁴¹, a medida que los Gobiernos recurren cada vez más al sector privado para gestionar la migración mediante las nuevas tecnologías, predominantemente con una óptica de seguridad nacional que descuida los derechos humanos fundamentales⁴². La externalización, la militarización y la automatización de las fronteras estimulan el complejo industrial fronterizo⁴³. En los Estados Unidos, el presupuesto destinado al control de las fronteras y de la inmigración ha aumentado en más de un 6.000 % desde 1980⁴⁴. El presupuesto de la Unión Europea para la gestión de las fronteras exteriores, la migración y el asilo se multiplicará por 2,6, y ascenderá a más de 34.900 millones de euros para el período 2021-2027, en contraste con los 13.000 millones de euros del período 2014-2020⁴⁵. Varias investigaciones recientes estiman que la tasa compuesta de crecimiento anual de este mercado mundial de seguridad fronteriza será del 7,2 % al 8,6 % (entre 65 y 68 millones de dólares) en 2025⁴⁶.

19. Entre las tecnologías digitales emergentes que impulsan el complejo industrial fronterizo y la creación de “fronteras inteligentes”, los drones desempeñan un papel fundamental al vigilar las fronteras y recoger datos biométricos⁴⁷. Los grandes actores empresariales y beneficiarios del sector de servicios de vigilancia de fronteras son en su mayoría empresas militares del Norte Global, algunas de las cuales, como Lockheed Martin, se encuentran también entre los mayores vendedores de armas del mundo⁴⁸. Las empresas de tecnología de la información, como IBM, también son actores importantes, en particular en la recopilación y el tratamiento de datos⁴⁹. Muchos de estos actores empresariales influyen sobremanera en la toma de decisiones nacionales e internacionales relacionadas con la gobernanza de la industria de las fronteras digitales⁵⁰. Las empresas también están vinculadas a los Gobiernos a través de empresas conjuntas. Por ejemplo, en 2016, la empresa pública-

³⁷ Comunicación del Centro de la Facultad de Derecho de la Universidad de Nueva York sobre la Raza, la Desigualdad y el Derecho.

³⁸ Véase <https://www.dezeen.com/2020/02/10/greece-floating-sea-border-wall-news/>.

³⁹ Véase, por ejemplo, Ana Beduschi, “International migration management in the age of artificial intelligence”, *Migration Studies* (2020). Véase también la comunicación de Ana Beduschi.

⁴⁰ Comunicación de Minority Rights Group International.

⁴¹ Véase <https://www.aljazeera.com/opinions/2019/11/1/why-climate-action-needs-to-target-the-border-industrial-complex/>.

⁴² Comunicación de Dhakshayini Sooriyakumaran y Bami Jegan.

⁴³ *Ibid.*

⁴⁴ *Ibid.*

⁴⁵ *Ibid.*

⁴⁶ *Ibid.*

⁴⁷ *Ibid.*

⁴⁸ *Ibid.*

⁴⁹ *Ibid.*

⁵⁰ *Ibid.*

privada francesa Civipol creó bases de datos de huellas dactilares en Malí y el Senegal⁵¹. El proyecto, financiado con 53 millones de euros del Fondo Fiduciario de Emergencia de la Unión Europea para la estabilidad y para abordar las causas profundas de la migración irregular y del desplazamiento de personas en África, pretende identificar a las personas refugiadas que llegan a Europa procedentes de esos dos países y deportarlas⁵². Francia posee el 40 % de Civipol, mientras que los productores de armas Airbus, Safran y Thales poseen cada uno más del 10 % de sus acciones⁵³. Este hecho ilustra también la manera en que los países del Norte Global utilizan la ayuda internacional para promover sus agendas en materia de fronteras en el Sur Global.

20. Una investigadora ha destacado el auge del “tecnocolonialismo”, al subrayar que el tecnocolonialismo desplaza la atención hacia el papel constitutivo que los datos y la innovación digital desempeñan en el afianzamiento de las desigualdades entre las personas refugiadas y los organismos humanitarios y, en última instancia, de las desigualdades en el contexto mundial⁵⁴, que son estimuladas en parte por los beneficios empresariales y la abdicación de los Gobiernos de sus responsabilidades en materia de derechos humanos. Esas desigualdades se afianzan a través de formas de experimentación tecnológica, de extracción de datos y valores, y de formas directas e indirectas de discriminación (véase la sección III).

21. En resumen, muchas tecnologías digitales en las fronteras sustituyen o facilitan los procesos humanos de toma de decisiones, a veces de forma que plantean graves problemas de derechos humanos. Esas tecnologías también amplían la autoridad y el control que los Gobiernos y los actores privados pueden ejercer sobre las personas migrantes, refugiadas y apátridas y otras personas, al tiempo que protegen esa autoridad de las limitaciones legales y judiciales. En otras palabras, aumentan la posibilidad de que se produzcan graves abusos contra los derechos humanos, y lo hacen de forma que eluden las protecciones sustantivas y de procedimiento que, de otro modo, han sido esenciales en el contexto del control de las fronteras y de la inmigración. En la sección III se pone de relieve toda la gama de violaciones discriminatorias de los derechos humanos que posibilita la maquinaria y la infraestructura de índole digital en las fronteras.

III. Cartografía de la discriminación racial y xenófoba en el control digital de las fronteras y de la inmigración

A. Discriminación directa e indirecta

1. Plataformas en línea

22. Las personas migrantes, refugiadas y apátridas han denunciado que las plataformas de los medios sociales, como Facebook, Twitter y WhatsApp, se utilizan a menudo para difundir el odio racista y xenófobo, y algunas han denunciado haber sido atacadas directamente a través de mensajes personales publicados en esas plataformas. En Malasia, por ejemplo, las personas migrantes informaron de un aumento de la promoción racista y xenófoba en las plataformas de los medios sociales durante la pandemia de COVID-19. En algunos casos, los usuarios publicaron fotografías de personas migrantes y refugiadas que percibían como “ilegales”, lo que suscitó una gran preocupación por el hecho de que esto fomentara la posterior persecución de personas tanto en el mundo real como en Internet.

23. Un sitio web con listas negras gestionado de forma anónima, Canary Mission, identifica de forma prejuiciosa a estudiantes, profesores y activistas que han defendido públicamente los derechos de los palestinos, centrándose principalmente en las personas de ascendencia árabe. Se ha señalado que la información publicada en Canary Mission ha sido utilizada por los funcionarios de inmigración israelíes en el contexto de la administración y el control de las fronteras de Israel y el territorio palestino ocupado, entre otras cosas para

⁵¹ *Ibid.*

⁵² *Ibid.*

⁵³ *Ibid.*

⁵⁴ Mirca Madianou, “Technocolonialism: digital innovation and data practices in the humanitarian response to the refugee crisis”, *Social Media + Society* (2019).

denegar la entrada⁵⁵. Esas prácticas vulneran los derechos a la igualdad y a la no discriminación, así como a la libertad de expresión, y dejan a las personas cuyos derechos han sido conculcados con vías de reparación limitadas.

2. Elaboración de perfiles raciales

24. Las consultas con migrantes, refugiados y personas apátridas también pusieron de manifiesto el papel de las tecnologías digitales en la elaboración de perfiles raciales y étnicos en el control de las fronteras. En noviembre de 2020, el Comité para la Eliminación de la Discriminación Racial adoptó su recomendación general núm. 36 (2020), relativa a la prevención y la lucha contra la elaboración de perfiles raciales por los agentes del orden, en la que el Comité reconoció que las personas migrantes, refugiadas, solicitantes de asilo y afrodescendientes, los pueblos indígenas y las minorías nacionales y étnicas, incluidos los romaníes, son los grupos más vulnerables a la elaboración de perfiles raciales. En la misma recomendación general, el Comité también observó que el creciente uso de nuevas herramientas tecnológicas, incluida la inteligencia artificial, en ámbitos como la seguridad, el control de fronteras y el acceso a los servicios sociales, puede intensificar el racismo, la discriminación racial, la xenofobia y otras formas de exclusión.

25. En las consultas, los participantes plantearon su preocupación por la elaboración de perfiles étnicos de los romaníes en las fronteras de Macedonia del Norte. En 2017, se divulgó que los funcionarios almacenaban los datos biométricos de las personas a las que se les impedía cruzar esas fronteras en una “lista de exclusión”⁵⁶. Los defensores de los derechos humanos han planteado una preocupación bien fundada debido a que en ese tipo de listas aparecen de forma desproporcionada personas de etnia romaní, que son objeto de perfiles étnicos y tienen acceso a escasos medios de reparación.

3. Recogida obligatoria de datos biométricos, sistemas de identificación digital y exclusión de los servicios básicos

26. Los Estados exigen en forma creciente una amplia recopilación de datos biométricos de los no ciudadanos. La recopilación y el uso de esos datos plantean inquietud acerca de formas directas e indirectas de discriminación por motivos de raza, etnia, origen nacional, ascendencia y religión. En la mayoría de los casos, las personas refugiadas, migrantes y apátridas no tienen ningún control sobre la forma en que se comparten sus datos. La India, por ejemplo, exige que se recojan datos biométricos de los no ciudadanos; esos datos se utilizan principalmente para tomar decisiones en materia de detención y deportación, en particular de los refugiados rohinyás⁵⁷. Otro motivo de preocupación planteado en el contexto de la India es el uso de los números de identificación para excluir *de facto* a los migrantes de los servicios básicos esenciales, cuya prestación depende de sistemas automatizados⁵⁸. Dado que los refugiados sin permiso de residencia tienen prohibido poseer los documentos de identificación pertinentes, son discriminados, no pueden acceder a los servicios básicos y, por tanto, se les niega el disfrute de los derechos que garantizan un refugio digno en la India⁵⁹. Al parecer, incluso a los niños y niñas refugiados se les ha negado la educación primaria por no tener el documento correspondiente⁶⁰.

27. La expansión de los sistemas digitales de identificación está destruyendo los medios informales de supervivencia que las personas apátridas han desarrollado a falta de una documentación adecuada y del reconocimiento de los Estados donde residen. Las personas apátridas, en su mayoría miembros de minorías raciales y étnicas, son excluidas sistemáticamente de las bases de datos de identidad digital y de la obtención de documentación. Los sistemas de identificación biométrica centralizados ponen a prueba el marco internacionalmente reconocido de la nacionalidad y la ciudadanía de diferentes

⁵⁵ Comunicación de Palestine Legal.

⁵⁶ Véase http://www.errc.org/uploads/upload_en/file/5209_file1_third-party-intervention-khamdelchevo-and-others-v-north-macedonia-5-february-2020.pdf.

⁵⁷ Comunicación de Anubhav Dutt Tiwari y Jessica Field.

⁵⁸ *Ibid.*

⁵⁹ *Ibid.*

⁶⁰ *Ibid.*

maneras. Entre los principales problemas se encuentra la toma de decisiones a partir de algoritmos, lo que significa que las decisiones sobre la condición jurídica ya no son adoptadas por los funcionarios gubernamentales sino, en su lugar, por máquinas o personal que gestionan equipos de datos biométricos. Esto puede dar lugar a una desnaturalización *de facto* sin el debido proceso o sin las debidas garantías. Las consideraciones fundamentales que deben regir toda decisión de privación de la nacionalidad —incluidas la no discriminación, la evitación de la apatridia, la prohibición de la arbitrariedad, la proporcionalidad, la necesidad y la legalidad⁶¹— también deben tenerse en cuenta a la hora de instaurar sistemas centralizados de identificación biométrica. El establecimiento de estructuras digitales de gobernanza corre el riesgo de privar a las personas de una nacionalidad de manera indirecta, sin el debido proceso, ya sea intencionadamente o como resultado de sistemas de registro civil incompletos o defectuosos⁶². Las comunidades nubia y rohinyá han denunciado dificultades sistemáticas para conseguir una identificación digital, lo que a su vez ha puesto en peligro su capacidad para conseguir un empleo formal y satisfacer otras necesidades básicas. En algunos casos, los regímenes de identificación digital parecen agravar la apatridia al excluir y no reconocer a los grupos étnicos minoritarios.

4. Reconocimiento de idiomas

28. Aunque se pueden adoptar sistemas de inscripción automatizados para aumentar la eficiencia burocrática, su tecnología puede producir resultados discriminatorios. La Oficina Federal para la Migración y los Refugiados de Alemania utiliza un programa automático para transliterar los nombres árabes al alfabeto latino⁶³. Sin embargo, el sistema es más propenso a generar errores en el caso de los solicitantes cuyos nombres proceden de la región del Magreb, al transliterarlos satisfactoriamente en un 35 % de los casos, en contraste con el índice del 85 % al 90 % de transliteraciones correctas que se consigue en los nombres de solicitantes iraquíes o sirios. Los solicitantes de habla árabe también pueden ser sometidos a un análisis dialectal en el momento de la inscripción. Además, la Oficina Federal para la Migración y los Refugiados utiliza programas informáticos a fin de analizar el idioma que hablan los solicitantes y determinar la verosimilitud de su origen nacional declarado. El programa informático se basa en el dialecto árabe levantino⁶⁴, lo que hace temer que la susceptibilidad a los errores del programa informático nunca haya sido comprobada por un especialista y no pueda ser entendida por agentes externos sin recurrir a los algoritmos utilizados⁶⁵. El riesgo evidente es que los hablantes de dialectos árabes no representados por el programa informático puedan ser considerados erróneamente como no creíbles y, por tanto, excluidos de la protección jurídica y de otro tipo de forma discriminatoria.

5. Extracción de datos móviles y obtención de información de los medios sociales de las personas migrantes y refugiadas

29. Los Gobiernos se fijan cada vez más en los dispositivos electrónicos de las personas migrantes y refugiadas para verificar la información que proporcionan a las autoridades fronterizas y de inmigración. Los funcionarios pueden realizar esas verificaciones mediante herramientas que descargan los datos de los teléfonos inteligentes, incluidos los contactos, los datos de las llamadas, los mensajes de texto, los archivos almacenados y la información de localización⁶⁶. En algunos casos, los funcionarios llegan a confiscar los dispositivos personales de las personas migrantes y refugiadas. Por ejemplo, según varias informaciones, las autoridades de Croacia confiscan habitualmente las pertenencias de los migrantes interceptados, en particular sus pasaportes y otras formas de identificación, sus teléfonos móviles y baterías portátiles, y las expulsan sumariamente a Bosnia y Herzegovina⁶⁷.

30. En Alemania, Austria, Bélgica, Dinamarca, Noruega y el Reino Unido de Gran Bretaña e Irlanda del Norte, las leyes permiten confiscar los teléfonos móviles de los

⁶¹ Véase <https://files.institutesi.org/PRINCIPLES.pdf>.

⁶² *Ibid.*, principio 10.

⁶³ Comunicación de Gesellschaft für Freiheitsrechte.

⁶⁴ *Ibid.*

⁶⁵ *Ibid.*

⁶⁶ *Ibid.* Véase también la comunicación conjunta de Privacy International *et al.*

⁶⁷ Comunicación de la Border Violence Monitoring Network.

solicitantes de asilo y los inmigrantes y utilizar los datos extraídos en los procedimientos de asilo⁶⁸. Estas prácticas constituyen una injerencia grave y desproporcionada en el derecho a la privacidad de las personas migrantes y refugiadas por su situación migratoria y, de hecho, por su origen nacional. Además, la presunción de que los datos obtenidos de los dispositivos digitales dan lugar necesariamente a pruebas fiables es errónea⁶⁹. Los Gobiernos también han recurrido a las técnicas, las tecnologías y la obtención de información de los medios sociales que permiten a las empresas y a los Gobiernos vigilar los sitios web de los medios sociales⁷⁰. Algunas de esas actividades las llevan a cabo directamente los propios funcionarios públicos, pero en algunos casos los Gobiernos piden a las empresas que les proporcionen las herramientas y los conocimientos necesarios para llevar a cabo esa vigilancia⁷¹.

31. Durante la pandemia de COVID-19, la proliferación de aplicaciones de rastreo de contactos ha suscitado la preocupación de que el intercambio de información sobre zonas con altas concentraciones de infecciones podría reforzar la estigmatización social existente de los grupos y comunidades desproporcionadamente infectados, con una repercusión especialmente dispar en función de la raza, la etnia, el origen nacional y la situación en materia de ciudadanía⁷².

32. Se han planteado preocupaciones por las prácticas relativas a la incautación de datos digitales en Alemania⁷³. De acuerdo con enmienda a la Ley de Asilo, los solicitantes de asilo que no puedan presentar un pasaporte válido o un documento equivalente deben entregar todos los soportes de datos, no solo los teléfonos móviles, sino también las computadoras portátiles, las memorias USB e incluso las pulseras de actividad física, junto con los datos de acceso correspondientes, que son procesados por la Oficina Federal para la Migración y los Refugiados para confirmar la identidad o la nacionalidad⁷⁴. La Ley también faculta a la Oficina Federal a compartir los datos con otros organismos gubernamentales, como las autoridades de seguridad y los servicios de inteligencia⁷⁵. Si se considera necesario, la información se procesa antes de la audiencia de asilo, a petición de la Secretaría para la Digitalización del Procedimiento de Asilo y con el consentimiento firmado del solicitante de asilo⁷⁶, aunque se reconoce que los solicitantes están bajo una presión excepcional para seguir las peticiones gubernamentales, puesto que temen que no hacerlo tendría consecuencias negativas para su solicitud de asilo⁷⁷. Esta práctica rutinaria ha afectado a más de la mitad de todas las personas que solicitaron asilo por primera vez durante los dos últimos años⁷⁸, y a determinadas nacionalidades más que a otras, lo que suscita una grave preocupación por la discriminación *de facto* basada en el origen nacional.

33. Esta extracción invasiva de datos de los dispositivos personales no tiene precedentes, se dirige únicamente a los solicitantes de asilo y está justificada por un discurso político racista y xenófobo⁷⁹. Además, las evaluaciones de los portadores de datos han demostrado que los datos extraídos no son adecuados para verificar la identidad o el origen nacional de los solicitantes de asilo con seguridad o para prevenir el abuso de los procedimientos de asilo⁸⁰. Aproximadamente en una cuarta parte de los intentos de procesar los datos extraídos se producen fallos técnicos; incluso cuando el procesamiento es satisfactorio, la mayoría de los informes de evaluación son inutilizables porque el conjunto de datos revisado es demasiado pequeño o no es concluyente⁸¹. De los 21.505 teléfonos móviles de los que se

⁶⁸ Comunicación conjunta de Privacy International *et al.*

⁶⁹ Comunicación de Gesellschaft für Freiheitsrechte.

⁷⁰ Comunicación conjunta de Privacy International *et al.*

⁷¹ *Ibid.*

⁷² Véase <https://policyoptions.irpp.org/magazines/april-2020/five-ways-a-covid-19-contact-tracing-app-could-make-things-worse/>.

⁷³ Comunicación de Gesellschaft für Freiheitsrechte.

⁷⁴ *Ibid.*

⁷⁵ *Ibid.*

⁷⁶ *Ibid.*

⁷⁷ *Ibid.*

⁷⁸ *Ibid.*

⁷⁹ *Ibid.*

⁸⁰ *Ibid.*

⁸¹ *Ibid.*

extrajeron y se procesaron satisfactoriamente datos en 2018 y 2019, solo en unos 118, es decir, el 0,55 %, se comunicó un tema de preocupación⁸². Además, dado que ni los algoritmos utilizados ni la información con que estos se entrenan son conocidos por la población, los jueces y otros responsables de la toma de decisiones no pueden evaluar adecuadamente la fiabilidad de los datos recogidos de los teléfonos móviles⁸³.

34. Aunque normativas como el Reglamento General de Protección de Datos⁸⁴ tratan de proteger los datos y la privacidad, algunos Estados crean exenciones en el contexto del control de la inmigración, como ilustra la Ley de Protección de Datos del Reino Unido de 2018⁸⁵. En virtud de la Ley, una entidad con facultad para procesar datos, conocida como “responsable del tratamiento”, puede eludir la obligación de respetar los derechos fundamentales de una persona en materia de acceso a los datos si la defensa de esos derechos perjudica el control efectivo de la inmigración⁸⁶. Esos derechos incluyen el derecho a oponerse y restringir el tratamiento de sus datos y el derecho a que se supriman sus datos personales⁸⁷. La Ley de Policía modificada del Reino Unido faculta no solo a los agentes de policía sino también a los de inmigración a intervenir los teléfonos móviles y otros dispositivos electrónicos de los solicitantes de asilo⁸⁸. La Ley de Delitos y Tribunales del Reino Unido de 2013, que va mucho más allá de lo que se permite en Alemania, faculta a la policía y a los funcionarios de inmigración a adoptar medidas de vigilancia secreta, colocar dispositivos de escucha y piratear y registrar teléfonos móviles y computadoras⁸⁹. Es probable que las personas afectadas se vean menoscabadas de forma desproporcionada por su origen nacional, cuando el origen nacional nunca debería ser un fundamento para disminuir la privacidad y otros derechos.

B. Estructuras discriminatorias

35. La Relatora Especial ya ha señalado cómo el diseño y la utilización de las diferentes tecnologías digitales emergentes pueden producir estructuras racialmente discriminatorias que socavan el disfrute de los derechos humanos de determinados grupos, por motivos de raza, etnia u origen nacional, solos o en combinación con otros motivos. Ha pedido que las tecnologías digitales emergentes se consideren como capaces de crear y mantener la exclusión racial y étnica en términos sistémicos o estructurales⁹⁰. La Relatora Especial destaca ahora las formas en que las personas migrantes, refugiadas y apátridas y los grupos afines están siendo sometidos a intervenciones tecnológicas que los exponen a una amplia gama de vulneraciones reales y potenciales de los derechos sobre la base de la situación migratoria o el origen nacional reales o subjetivos.

1. Humanitarismo de vigilancia y asilo de vigilancia

36. Los analistas han advertido del aumento del “humanitarismo de vigilancia”⁹¹, mediante el que la creciente dependencia de las tecnologías digitales en la prestación de servicios y otros procesos burocráticos se traduce perversamente en la exclusión de las personas refugiadas y solicitantes de asilo del acceso a necesidades básicas esenciales como la alimentación⁹². Incluso un nombre mal escrito puede dar lugar a un caos burocrático y a

⁸² *Ibid.*

⁸³ *Ibid.*

⁸⁴ Reglamento (UE) 2016/79 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 libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

⁸⁵ Comunicaciones de Gesellschaft für Freiheitsrechte y la Plataforma para la Cooperación Internacional sobre Inmigrantes Indocumentados.

⁸⁶ Comunicación de la Plataforma para la Cooperación Internacional sobre Inmigrantes Indocumentados.

⁸⁷ *Ibid.*

⁸⁸ Comunicación de Gesellschaft für Freiheitsrechte.

⁸⁹ *Ibid.*

⁹⁰ A/HRC/44/57, párr. 38.

⁹¹ Véase <https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html>.

⁹² Comunicación de Ana Beduschi.

acusaciones de proporcionar información falsa, lo que ralentiza aún más el proceso de asilo⁹³. Los posibles perjuicios relacionados con la violación de la privacidad de los datos son a menudo latentes; en zonas de conflicto, pueden desembocar en violencia, dado que la filtración de datos a una de las facciones enfrentadas podría dar lugar a represalias contra quienes se percibe que están en el lado equivocado del conflicto⁹⁴.

37. En ese sentido, hay varios peligros asociados al creciente uso de las tecnologías digitales para gestionar la distribución de la ayuda⁹⁵. En los campamentos de refugiados del Afganistán, por ejemplo, los refugiados afganos que regresan tienen que registrar su iris para poder recibir asistencia, según las informaciones disponibles⁹⁶. La recogida, la digitalización y el almacenamiento de información sobre el iris de los refugiados puede ser problemática cuando los sistemas presentan deficiencias o son fuente de abusos⁹⁷. También se ha documentado que estas herramientas de vigilancia biométrica han provocado la aversión al sistema y la pérdida de acceso a bienes y servicios necesarios para la supervivencia⁹⁸. Por ejemplo, los fallos de la tecnología en los campamentos de refugiados rohinyás en Bangladesh han provocado la denegación de raciones alimentarias a las personas refugiadas⁹⁹. La Oficina del Alto Comisionado de las Naciones Unidas para los Refugiados (ACNUR), por su parte, ha informado a la Relatora Especial de que su política es que se establezcan salvaguardias para garantizar que las personas refugiadas puedan acceder a los servicios de asistencia y protección sin el uso de la tecnología biométrica, cuando sea necesario, y para hacer frente al riesgo de error o fallo en su uso.

38. La recopilación de grandes cantidades de datos sobre personas migrantes y refugiadas plantea graves problemas y posibles violaciones de los derechos humanos en relación con el intercambio de datos y el acceso a estos, sobre todo en entornos como los campamentos de refugiados, donde existen marcadas diferencias de poder entre los organismos de las Naciones Unidas, las organizaciones no gubernamentales internacionales y las comunidades afectadas. Aunque el intercambio de datos sobre crisis humanitarias o mediante la identificación biométrica se presenta a menudo como una forma de aumentar la eficacia y la cooperación interinstitucional e interestatal, no todos se benefician por igual de esa recopilación de datos. La recopilación de datos y el empleo de nuevas tecnologías, especialmente en contextos caracterizados por marcadas diferencias de poder, plantean cuestiones relativas al consentimiento informado y a la posibilidad de renunciar a participar. En varios contextos de migración forzada y asistencia humanitaria, como en Mafraq (Jordania), se están utilizando tecnologías biométricas en forma de escaneo del iris, en lugar de tarjetas de identidad, a cambio de raciones de alimentos¹⁰⁰. Sin embargo, condicionar el acceso a los alimentos a la recogida de datos elimina cualquier atisbo de posibilidad de elección o autonomía de las personas refugiadas, puesto que el consentimiento no puede darse libremente cuando la alternativa es la inanición. De hecho, una investigación en el campamento de refugiados de Azraq¹⁰¹ ha puesto de manifiesto que la mayoría de las personas refugiadas entrevistadas se sentían incómodas con estos experimentos tecnológicos, pero consideraban que no podían rechazarlos si querían comer. El objetivo o la promesa de mejorar la prestación de servicios no pueden justificar los niveles de coacción implícita en que se sustentan regímenes como este¹⁰².

⁹³ Mark Latonero *et al.*, “Digital identity in the migration and refugee context: Italy case study”, *Data and Society* (abril de 2019).

⁹⁴ Véase <https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html>.

⁹⁵ Comunicación de Amnistía Internacional.

⁹⁶ *Ibid.*

⁹⁷ *Ibid.*, en que se cita A/HRC/39/29.

⁹⁸ Comunicación de Amnistía Internacional.

⁹⁹ *Ibid.*

¹⁰⁰ Véase Fleur Johns, “Data, detection and the redistribution of the sensible in international law”, *Cambridge University Press*, vol. 111, núm. 1 (2017). Véase también <https://medium.com/unhcr-innovation-service/managing-risk-to-innovate-in-unhcr-91fe9294755b>.

¹⁰¹ Véase <http://www.irinnews.org/analysis/2016/05/18/eye-spy-biometric-aid-system-trials-jordan>.

¹⁰² Véase https://www.unhcr.org/innovation/wp-content/uploads/2020/04/Space-and-imagination-rethinking-refugees%E2%80%99-digital-access_WEB042020.pdf; <https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees>.

39. Los refugiados rohinyás en Bangladesh y la India han expresado su preocupación por el hecho de que sus datos puedan ser compartidos de forma que aumente su riesgo de devolución, por ejemplo con el Gobierno de Myanmar, lo que aumenta su vulnerabilidad a las violaciones de derechos humanos en caso de retorno forzoso y de otras formas a su país de origen. Una grave preocupación en este contexto es la “desviación de uso”, en que los datos recogidos en un contexto (por ejemplo, para vigilar el fraude de bajo nivel) se comparten y reutilizan para diferentes fines (por ejemplo, para cumplimentar registros de posibles sospechosos de terrorismo)¹⁰³, sin ninguna protección procesal o sustantiva para las personas cuyos datos se están compartiendo y reutilizando. El ACNUR afirma que no ha recogido información que pueda interpretarse como un consentimiento a la repatriación, y que ha obtenido el consentimiento de las personas refugiadas para compartir sus datos con el Gobierno de Myanmar con el fin de verificar su derecho al retorno.

40. En algunos casos, la forma en que se recogen los datos puede producir resultados profundamente discriminatorios. Un ejemplo es el de los más de 742.000 refugiados rohinyás apátridas que huyeron del genocidio en Myanmar y llegaron a Bangladesh entre agosto de 2017 y julio de 2019¹⁰⁴. El sistema de registro utilizado por el ACNUR y el Gobierno de Bangladesh no ofrecía “rohinyá” como opción de identidad étnica, sino solo “nacional de Myanmar”, término que Myanmar no reconoce y que no recoge el hecho de que las personas rohinyás son apátridas porque han sido privadas arbitrariamente de su derecho a la nacionalidad de Myanmar¹⁰⁵. La categorización de las personas mediante el uso de una expresión irreconocible en las tarjetas de identidad digitales equivale, en este caso, a una forma de aniquilación simbólica de los rohinyás que deben llevar y utilizar esas tarjetas¹⁰⁶. El ACNUR ha informado de que los refugiados rohinyás aceptaron este enfoque y fueron consultados sobre su adopción.

41. También hay personas refugiadas y solicitantes de asilo excluidas del acceso a los servicios básicos esenciales a través de sistemas tecnológicos digitales fuera de los campamentos de refugiados. Por ejemplo, en virtud de la Ley de Prestaciones para Solicitantes de Asilo de Alemania, aunque las personas indocumentadas tienen el mismo derecho a la atención de la salud que los solicitantes de asilo¹⁰⁷, la oficina de asistencia social que administra la atención de la salud para las personas indocumentadas tiene la obligación —en virtud del artículo 87 de la Ley de Residencia, que regula la transferencia por parte de todas las autoridades públicas de datos e información de las autoridades extranjeras— de comunicar los datos personales de estas personas a las autoridades de inmigración¹⁰⁸. Esto significa que el acceso legal a la atención de la salud puede dar lugar a la aplicación de disposiciones sobre inmigración que probablemente tengan un efecto disuasorio sobre el deseo de las personas migrantes y refugiadas de utilizar incluso la atención de la salud de urgencia.

2. Experimentación tecnológica

42. Se han planteado graves preocupaciones por la experimentación tecnológica generalizada que llevan a cabo actores estatales y no estatales con las personas refugiadas, migrantes y apátridas. Esa experimentación consiste en probar diversos productos tecnológicos en grupos con escasos o nulos medios para dar su consentimiento informado y sin que se conozcan de manera suficiente las consecuencias para los derechos humanos de esas pruebas y experimentos. Además, es su origen nacional y su situación en materia de ciudadanía y de inmigración lo que expone a las personas refugiadas, migrantes y apátridas a la experimentación tecnológica, cuestión que suscita una gran inquietud a raíz de las estructuras discriminatorias de vulnerabilidad.

¹⁰³ Comunicación de Mirca Madianou.

¹⁰⁴ Véase <https://www.unhcr.org/en-us/rohingya-emergency.html>.

¹⁰⁵ Mirca Madianou, “Technocolonialism”.

¹⁰⁶ Comunicación de Mirca Madianou.

¹⁰⁷ Comunicación de la Plataforma para la Cooperación Internacional sobre Inmigrantes Indocumentados.

¹⁰⁸ *Ibid.*

43. Otro ejemplo es el proyecto iBorderCtrl de la Unión Europea, un “sistema inteligente y portátil de control” que pretende posibilitar un control fronterizo más rápido y exhaustivo de los nacionales de terceros países que cruzan las fronteras terrestres de los Estados miembros de la Unión Europea¹⁰⁹. iBorderCtrl utiliza tecnologías de *hardware* y *software* con las que se pretende automatizar la vigilancia de las fronteras¹¹⁰, entre otras cosas mediante la detección automática de engaños¹¹¹. La Unión Europea ha probado este detector de mentiras en los aeropuertos de Grecia, Hungría y Letonia¹¹². Según las informaciones disponibles, en 2019 iBorderCtrl se probó en la frontera entre Serbia y Hungría y el resultado no fue satisfactorio¹¹³. iBorderCtrl es un ejemplo de la tendencia a realizar experimentos con tecnologías de vigilancia y de otro tipo con los solicitantes de asilo de acuerdo con argumentos científicamente dudosos¹¹⁴. Basándose en la controvertida disciplina de la “ciencia del reconocimiento de los afectos”, iBorderCtrl sustituye a los guardafronteras humanos por un sistema de reconocimiento facial que busca anomalías en el rostro mientras los viajeros responden a una serie de preguntas¹¹⁵. También Nueva Zelanda está realizando experimentos con la tecnología de reconocimiento facial automatizado para identificar a futuras “personas incómodas”, lo que ha llevado a las organizaciones de la sociedad civil a presentar recursos legales por motivos de discriminación y por la elaboración de perfiles raciales¹¹⁶. El Canadá y Rumania también han realizado experimentos con proyectos similares de “reconocimiento de emociones” para el control de fronteras¹¹⁷.

44. Los Estados están experimentando actualmente con la automatización de diversas facetas de la toma de decisiones en materia de inmigración y asilo. Por ejemplo, desde al menos 2014, el Canadá ha utilizado alguna forma de toma de decisiones automatizada en su sistema de inmigración y refugiados¹¹⁸. En 2018, se constató que esos procesos crean un laboratorio de experimentos de alto riesgo dentro de un sistema ya muy discrecional¹¹⁹. Las ramificaciones del uso de la toma de decisiones automatizada en el contexto de la inmigración y los refugiados son de gran alcance. Aunque el Gobierno del Canadá ha confirmado que este tipo de tecnología se limita a aumentar la toma de decisiones humanas y se reserva únicamente para determinadas solicitudes de inmigración, no existe ningún mecanismo legal que proteja los derechos procesales de los no ciudadanos y evite que se produzcan abusos contra los derechos humanos. En el Reino Unido se utilizan actualmente algoritmos similares para la concesión de visados, que han sido denunciados ante los tribunales por su potencial discriminatorio¹²⁰. El Canadá, el Reino Unido y Suiza también utilizan la toma de decisiones automatizada o algorítmica para seleccionar y reubicar a los refugiados¹²¹. La adopción de las nuevas tecnologías influye tanto en los procesos como en los resultados asociados a las decisiones que, de otro modo, tomarían los tribunales administrativos, los funcionarios de inmigración, los agentes fronterizos, los analistas jurídicos y otros funcionarios responsables de los sistemas de administración de la inmigración y los refugiados, del control de las fronteras y de la gestión de la respuesta a los refugiados. No está claro cómo interpretarán los tribunales los principios del derecho administrativo como la justicia natural, la equidad

¹⁰⁹ Comunicación conjunta de Privacy International *et al.* Véase también <https://www.iborderctrl.eu/The-project>.

¹¹⁰ Véase <https://www.iborderctrl.eu/The-project>.

¹¹¹ *Ibid.* Véase también la comunicación conjunta de Privacy International *et al.*

¹¹² Comunicación de Maat for Peace, Development and Human Rights Association. Véase también Petra Molnar, “Technology on the margins: AI and global migration management from a human rights perspective”, *Cambridge International Law Journal*, vol. 8, núm. 2 (2019); y la comunicación de Minority Rights Group International.

¹¹³ Comunicación conjunta de Privacy International *et al.*

¹¹⁴ *Ibid.*

¹¹⁵ Comunicación de Minority Rights Group International.

¹¹⁶ Véase https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12026585.

¹¹⁷ Véase <https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf>.

¹¹⁸ Petra Molnar y Lex Gill, *Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System* (2018).

¹¹⁹ *Ibid.*

¹²⁰ *Joint Council for the Welfare of Immigrants v. Secretary of State for the Home Department* CO/2057/2020.

¹²¹ Comunicación de Maat for Peace, Development and Human Rights Association y Ana Beduschi (en que se cita Petra Molnar y Lex Gill, *Bots at the Gate*).

procesal y el criterio de examen respecto a los sistemas automatizados de toma de decisiones o cuando las tecnologías se utilizan de forma opaca.

45. Una parte de la experimentación tecnológica está relacionada con la recogida de datos genéticos, que se justifica por motivos poco convincentes. Por ejemplo, en los Estados Unidos existe el Sistema de Índices Combinados de ADN (CODIS), una base de datos forense de ADN que utilizan los estados y el Gobierno federal para recoger, almacenar y compartir información genética¹²². Desde enero de 2020, el Gobierno de los Estados Unidos recoge el ADN de todas las personas recluidas por motivos de inmigración¹²³. Esto significa que, por primera vez, el CODIS almacenará los datos genéticos de personas que no han sido acusadas de ningún delito, con fines de detección de delitos, poniendo fin a la antigua práctica de recoger el ADN únicamente de personas que presuntamente han participado en una conducta delictiva¹²⁴. En general, los no ciudadanos recluidos por motivos de inmigración no son delincuentes¹²⁵. De hecho, la gran mayoría de las infracciones de inmigración por las que se recluye a los inmigrantes son de carácter civil¹²⁶. En el caso de los solicitantes de asilo, que constituyen una proporción cada vez mayor de la población no ciudadana recluida, tanto las leyes internacionales como las nacionales les permiten expresamente entrar en los Estados Unidos para reclamar el derecho de refugio¹²⁷. La nueva política de inmigración corre el riesgo de convertir el CODIS en un “panóptico genético” que incluirá a cualquier persona que se encuentre dentro de las fronteras de los Estados Unidos, incluidos los ciudadanos de a pie que no hayan sido condenados ni sean siquiera sospechosos de conducta delictiva, lo que supone una amenaza para la democracia y los derechos humanos¹²⁸.

46. Como la COVID-19 ha incentivado y legitimado aún más la vigilancia y otras tecnologías dirigidas a las personas refugiadas y migrantes, estos grupos han sido objeto de más experimentos¹²⁹. Un ejemplo es el despliegue experimental de un pasaporte de inmunidad llamado “COVI-Pass” en África Occidental¹³⁰. Fruto de la colaboración entre Mastercard y la Alianza Gavi, esta iniciativa digital combina la biometría, el rastreo de contactos, los pagos sin efectivo, la identificación nacional y el cumplimiento de la ley¹³¹. Estas tecnologías no solo funcionan al margen de las evaluaciones del impacto en los derechos humanos y de la normativa, sino que también corren el riesgo de amenazar los derechos humanos, como el derecho a la libertad de circulación, el derecho a la privacidad, el derecho a la autonomía corporal y el derecho a la igualdad y a la no discriminación, especialmente para las personas refugiadas y migrantes¹³².

47. En el Reino Unido ha surgido la preocupación de que las aplicaciones de rastreo de contactos y otras tecnologías de recopilación de datos empleadas para luchar contra la pandemia de COVID-19 podrían llegar a utilizarse para el control de la inmigración, lo que socavaría la confianza en las tecnologías de rastreo de contactos entre las comunidades de inmigrantes y desembocaría en su exclusión de las políticas de salud eficaces¹³³. La Oficina de Aduanas y Protección Fronteriza de Estados Unidos ha lanzado recientemente la aplicación CBP One, que utiliza tecnologías de reconocimiento facial y GPS, así como almacenamiento en la nube, para recopilar datos sobre los solicitantes de asilo antes de que

¹²² Comunicación conjunta de Daniel I. Morales, Natalie Ram y Jessica L. Roberts.

¹²³ *Ibid.*

¹²⁴ *Ibid.*

¹²⁵ *Ibid.*

¹²⁶ *Ibid.*

¹²⁷ *Ibid.*

¹²⁸ *Ibid.*

¹²⁹ Comunicación de Amnistía Internacional.

¹³⁰ *Ibid.*

¹³¹ *Ibid.*

¹³² *Ibid.*

¹³³ Véase <https://www.openrightsgroup.org/blog/contact-tracing-apps-vulnerable-migrants-key-concerns/>.

entren en los Estados Unidos¹³⁴. Esta aplicación plantea graves problemas de privacidad y no discriminación¹³⁵.

48. Los Estados y las organizaciones internacionales han promovido la creación de pasaportes de “inmunidad” o “sanitarios” que condicionan los viajes y la movilidad internacional al estado de vacunación de los portadores¹³⁶. Sin embargo, debido a la desigual distribución del acceso a las vacunas, estos requisitos agravarán aún más la desigualdad en las oportunidades de inmigración y movilidad. A medida que las vacunas están disponibles, los Estados y las organizaciones internacionales recurren a las nuevas tecnologías para facilitar la movilidad de los vacunados¹³⁷. Organizaciones como la Organización Mundial de la Salud, la Asociación de Transporte Aéreo Internacional, el Foro Económico Mundial y la Alianza Gavi están desarrollando de forma activa sistemas digitales que pueden rastrear los datos de vacunación y facilitar los viajes. Las empresas tecnológicas privadas también están trabajando para ofrecer un acceso digital sin fisuras a los registros de vacunación¹³⁸. La OIM y el Migration Policy Institute han pedido que esos esfuerzos sean especialmente sensibles a las desigualdades preexistentes, que se ven agravadas por la digitalización, incluidas las repercusiones en los que se encuentran en situaciones vulnerables o no pueden acceder a la tecnología pertinente¹³⁹.

3. Externalización de las fronteras

49. La externalización de fronteras —la extraterritorialización de las fronteras nacionales y regionales a otras regiones geográficas con el fin de impedir la llegada de personas migrantes y refugiadas— se ha convertido en una herramienta común de control fronterizo para muchos países y regiones. Las violaciones de los derechos humanos asociadas a la externalización de fronteras están ampliamente documentadas¹⁴⁰. La externalización de fronteras no afecta a todas las nacionalidades o grupos de origen nacional por igual. Repercute desproporcionadamente en las personas de África, América Central y del Sur y Asia Meridional, y en muchas regiones se ve estimulada por políticas racistas, xenófobas y etnonacionalistas que pretenden excluir a determinados grupos nacionales y étnicos de las regiones sobre bases discriminatorias. Los Estados y los bloques regionales recurren cada vez más a las tecnologías digitales para lograr esa externalización de las fronteras, consolidando y ampliando así los regímenes discriminatorios y excluyentes.

50. El Sistema Europeo de Vigilancia de Fronteras, por ejemplo, utiliza tecnologías basadas en macrodatos para predecir, controlar y vigilar el tráfico a través de las fronteras de la Unión Europea¹⁴¹. Despliega drones de vigilancia en el mar Mediterráneo a fin de avisar a los guardacostas libios para que intercepten las embarcaciones de personas refugiadas y migrantes y devuelvan a las personas migrantes a Libia¹⁴². Aunque la Comisión Europea insiste en que los drones tienen una mera función de vigilancia civil¹⁴³, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos se ha pronunciado en contra de las devoluciones en caliente coordinadas y los fallos en la asistencia a las personas

¹³⁴ Véase <https://www.latimes.com/politics/story/2021-06-04/asylum-bidens-got-an-app-for-that-with-privacy-risks-and-surveillance-beyond-border>.

¹³⁵ Véase <https://www.americanimmigrationcouncil.org/FOIA/investigating-cbp%E2%80%99s-use-mobile-application-cbp-one>.

¹³⁶ Organización Internacional para las Migraciones y Migration Policy Institute, *COVID-19 and the State of Global Mobility in 2020* (2021), pág. 51.

¹³⁷ *Ibid.*, págs. 51 y 52.

¹³⁸ *Ibid.*

¹³⁹ *Ibid.*, pág. 52.

¹⁴⁰ Véanse, por ejemplo, A/HRC/23/46, A/HRC/29/36 y A/72/335.

¹⁴¹ Comunicación de Maat for Peace, Development and Human Rights Association, en que se cita Btihaj Ajana, “Augmented borders: Big Data and the ethics of immigration control”, *Journal of Information, Communication and Ethics in Society*, vol. 13, núm. 1 (2015).

¹⁴² Franciscans International, comunicación en que se cita <https://www.middleeastmonitor.com/20190819-eu-using-israel-drones-to-track-migrant-boats-in-the-med/>.

¹⁴³ Franciscans International, comunicación en que se cita https://www.europarl.europa.eu/doceo/document/E-9-2019-003257-ASW_EN.pdf.

migrantes y refugiadas en el mar Mediterráneo, una de las rutas migratorias más mortíferas del mundo¹⁴⁴.

51. Otro ejemplo es la participación de 13 Estados europeos en el proyecto ROBORDER, un sistema autónomo de vigilancia de fronteras totalmente funcional, compuesto por robots móviles no pilotados capaces de funcionar de forma autónoma o en enjambre, en diversos entornos: en el aire, en el agua, debajo del agua y en tierra¹⁴⁵. Esta propuesta de aumentar el uso de drones para vigilar las fronteras de Europa agrava la descentralización de la zona fronteriza en varias capas verticales y horizontales de vigilancia, al convertir a las personas en objetos de seguridad y puntos de datos que deben ser analizados, almacenados, recogidos y convertidos en inteligibles¹⁴⁶. La utilización de tecnología autónoma militar, o casi militar, refuerza el nexo entre la inmigración, la seguridad nacional, la creciente criminalización de la migración y el uso de taxonomías basadas en el riesgo para incluir una indicación sobre los casos¹⁴⁷. En todo el mundo, los Estados han estado utilizando diversos métodos para adelantarse y disuadir a quienes intentan solicitar legalmente el asilo. Este tipo de política de disuasión es muy evidente en Grecia, Italia y España¹⁴⁸, países que se encuentran en las fronteras geográficas de Europa y que se apoyan cada vez más en políticas de disuasión violenta y de devoluciones en caliente.

52. Según la Border Violence Monitoring Network, Croacia utiliza tecnologías financiadas por la Unión Europea para detectar, detener y devolver a las personas refugiadas y migrantes que viajan por la ruta de los Balcanes, desde Bosnia y Herzegovina y Serbia, a través de Croacia, hasta la frontera Schengen¹⁴⁹. La organización alega que en los últimos tres años se han cometido cientos de abusos contra los derechos humanos, incluidas las devoluciones en caliente ilegales que reflejan “divisiones” inherentemente racistas¹⁵⁰. Las tecnologías de vigilancia, como los drones y los helicópteros con proyectores, se han convertido en armas y se utilizan contra las personas en movimiento, lo que facilita su detección y agrava su vulnerabilidad y los peligros a los que se enfrentan¹⁵¹.

53. La externalización discriminatoria de las fronteras también se consigue mediante programas transnacionales de intercambio de datos biométricos. Al parecer, uno de esos programas ha posibilitado que los Gobiernos de México y los Estados Unidos compartan datos biométricos¹⁵². En agosto de 2018, México había desplegado el programa financiado por los Estados Unidos en las 52 estaciones migratorias¹⁵³. El programa utiliza datos biométricos para examinar a los migrantes detenidos en México por ser sospechosos de haber intentado cruzar la frontera con los Estados Unidos o de pertenecer a bandas criminales¹⁵⁴. Sin embargo, el Instituto Nacional de Migración de México ha negado, en respuestas a solicitudes de acceso a la información, el tratamiento de datos biométricos¹⁵⁵.

4. Vigilancia de la inmigración¹⁵⁶

54. En la frontera entre los Estados Unidos y México se está construyendo una red de 55 torres equipadas con cámaras, sensores térmicos, sensores de movimiento, sistemas de

¹⁴⁴ Véase <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25875&LangID=E>.

¹⁴⁵ Comunicación de Homo Digitalis. Véase también <https://roborder.eu/>.

¹⁴⁶ Raluca Csernaton, “Constructing the EU’s high-tech borders”.

¹⁴⁷ Comunicación de Dimitri Van Den Meerssche.

¹⁴⁸ Véase <https://www.statewatch.org/news/2017/november/eu-spain-new-report-provides-an-x-ray-of-the-public-funding-and-private-companies-in-spain-s-migration-control-industry/>; <https://www.efadrones.org/countries/italy/>.

¹⁴⁹ Comunicación de la Border Violence Monitoring Network.

¹⁵⁰ *Ibid.*

¹⁵¹ *Ibid.*

¹⁵² Comunicación conjunta de Privacy International *et al.*

¹⁵³ *Ibid.*

¹⁵⁴ *Ibid.*

¹⁵⁵ *Ibid.*

¹⁵⁶ En Anil Kalhan, “Immigration surveillance”, *Maryland Law Review*, vol. 74, núm. 1 (2014), se señala que la vigilancia de la inmigración se define como el producto de una ampliación espectacular de las capacidades de identificación, el seguimiento y el control de la movilidad y el intercambio de

radar y un sistema GPS¹⁵⁷. Este sistema de control fronterizo, que también vigila la reserva de la nación Tohono O'odham, situada en Arizona a aproximadamente un kilómetro y medio de la frontera¹⁵⁸, ha modificado las rutas utilizadas por los migrantes, aumentando así su vulnerabilidad a las lesiones, el aislamiento, la deshidratación, la hipertermia y el agotamiento y la muerte¹⁵⁹. Distintos investigadores y organizaciones de la sociedad civil se han opuesto a estas tecnologías en las fronteras porque agravarían la desigualdad racial y étnica en la vigilancia policial y el control de la inmigración, además de frenar la libertad de expresión y el derecho a la privacidad¹⁶⁰. En otros casos se ha destacado el uso de otra infraestructura de inteligencia artificial de vigilancia autónoma en la frontera entre los Estados Unidos y México, incluidos los drones diseñados para detectar a los seres humanos y alertar a los agentes fronterizos¹⁶¹. Como se ha indicado anteriormente, según los indicios actuales, las denominadas tecnologías “inteligentes” en las fronteras obligan a los migrantes a emprender viajes cada vez más precarios y tienen un impacto desproporcionado en las personas de ciertos grupos de origen nacional, étnico y racial¹⁶².

55. En los Estados Unidos se vigilan las comunicaciones de los inmigrantes detenidos y de sus familiares y amigos¹⁶³. Las empresas proveedoras de las tecnologías utilizadas para estas comunicaciones afirman que proporcionan a los inmigrantes detenidos y a sus familias comodidad en forma de llamadas, videochats, mensajes de voz, fotografías y mensajes de texto, mientras que los verdaderos clientes de la empresa —los funcionarios de inmigración— obtienen datos sobre los usuarios¹⁶⁴. El *software* de vigilancia en la web ofrece a los funcionarios públicos análisis de patrones de llamadas, análisis de relaciones y herramientas para la visualización de datos de forma gratuita¹⁶⁵.

56. Otra faceta de la vigilancia de la inmigración es el control de los medios sociales. Desde abril de 2019, el Departamento de Estado de los Estados Unidos exige a los solicitantes de visado que divulguen la información sobre las cuentas de los medios sociales que hayan tenido en los cinco años anteriores al momento de la solicitud¹⁶⁶. Este enfoque expansivo del control de los medios sociales es especialmente preocupante debido al historial constatado en materia de control de inmigración de los Estados Unidos de utilizar la información de los medios sociales de una manera que perjudica desproporcionadamente a los miembros de grupos raciales, étnicos y religiosos minoritarios¹⁶⁷. El Departamento de Seguridad Nacional ya ha acusado falsamente a jóvenes negros y latinos de ser miembros de bandas aprovechando sus conexiones en los medios sociales, lo que ha dado lugar a su detención, deportación o denegación de beneficios en materia de inmigración¹⁶⁸. El Servicio de Inmigración y Control de Aduanas, organismo dependiente del Departamento de Seguridad Nacional, peina con frecuencia los medios sociales para sustentar las acusaciones de pertenencia a bandas¹⁶⁹. En un caso, el Departamento de Seguridad Nacional respaldó su acusación con una fotografía en Facebook de un joven inmigrante con una gorra de los Chicago Bulls. El tribunal de inmigración le denegó la fianza y rechazó sus dos solicitudes de asilo y residencia permanente

información de las personas, así como del debilitamiento de las protecciones jurídicas tradicionales, tanto sustantivas como procesales, en las que se ha basado la protección de los no ciudadanos frente a una serie de abusos contra los derechos humanos.

¹⁵⁷ Comunicación de la coalición Stop Killer Robots.

¹⁵⁸ *Ibid.*

¹⁵⁹ Samuel Norton Chambers *et al.*, “Mortality, surveillance and the tertiary ‘funnel effect’ on the US-Mexico border”.

¹⁶⁰ Comunicación de Minority Rights Group International.

¹⁶¹ Comunicaciones de Mijente e Iván Chaar-López.

¹⁶² Comunicación de Franciscans International.

¹⁶³ Comunicación de Mijente, en que se cita <https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html>.

¹⁶⁴ *Ibid.*

¹⁶⁵ *Ibid.*

¹⁶⁶ Comunicación del Programa de Asistencia a Inmigrantes y Refugiados de Harvard.

¹⁶⁷ *Ibid.*

¹⁶⁸ *Ibid.*, citando https://www.ilrc.org/sites/default/files/resources/deport_by_any_means_nec-20180521.pdf.

¹⁶⁹ Comunicación del Programa de Asistencia a Inmigrantes y Refugiados de Harvard.

y lo deportó a un país en el que temía por su vida¹⁷⁰, en contravención de las obligaciones de no devolución con arreglo al derecho internacional.

57. Además, el cribado en los medios sociales ha agravado el riesgo desproporcionado de las personas que pertenecen o se supone que son de fe musulmana o de ascendencia árabe, al crear una infraestructura en la que abundan las inferencias erróneas y la culpabilidad por asociación¹⁷¹. Por ejemplo, la Oficina de Aduanas y Protección Fronteriza, otro organismo del Departamento de Seguridad Nacional, denegó la entrada a los Estados Unidos a un estudiante universitario palestino sobre la base de las publicaciones de sus amigos en Facebook que expresaban opiniones políticas contra los Estados Unidos, aunque él mismo no había publicado tales opiniones¹⁷². Además de la carga directa que suponen para los no ciudadanos, la obligación ampliada de proporcionar información sobre los medios sociales impuestos por el Gobierno de los Estados Unidos afecta previsiblemente a los derechos de libertad de expresión y de asociación.

58. El Departamento de Investigación de Seguridad Nacional, el principal órgano de investigación del Servicio de Inmigración y Control de Aduanas, ya estaba probando la elaboración de perfiles automatizados en los medios sociales en 2016¹⁷³, a fin de reforzar sus capacidades de aprovechamiento de los medios sociales de código abierto con el fin de escudriñar a los solicitantes y titulares de visados antes y después de su llegada a los Estados Unidos¹⁷⁴. También se ha planteado la preocupación por el uso por parte del Gobierno de los Estados Unidos de tecnologías con el objetivo de tomar determinaciones mediante la automatización, es decir, su uso de tecnologías para decidir si una persona que solicita o tiene un visado de los Estados Unidos es probable que se convierta en un miembro que contribuya positivamente a la sociedad o en alguien que tiene la intención de cometer atentados criminales o terroristas¹⁷⁵. Especialmente preocupante ha sido el uso en los Estados Unidos de herramientas de evaluación del riesgo en las decisiones de detención de inmigrantes, en particular una herramienta que recurre a un algoritmo establecido para recomendar siempre la detención de inmigrantes independientemente de los antecedentes penales de una persona¹⁷⁶.

59. Todo ello apunta a una tendencia en la vigilancia de la inmigración en que los modelos predictivos utilizan la inteligencia artificial para pronosticar si personas sin antecedentes penales cometerán sin embargo delitos en el futuro. Esos modelos de predicción son propensos a crear y reproducir bucles de retroalimentación racialmente discriminatorios¹⁷⁷. Además, el sesgo racial ya está presente en los conjuntos de datos en los que se basan estos modelos¹⁷⁸. Cuando los conjuntos de datos discriminatorios se tratan como entrada de información neutral, dan lugar a modelos inexactos de criminalidad que luego perpetúan la desigualdad racial y son un factor responsable de la focalización y el exceso de vigilancia policial en los no ciudadanos¹⁷⁹.

60. La respuesta a la pandemia de COVID-19 ha provocado el rápido aumento de la “biovigilancia”, es decir, el seguimiento de la salud y el comportamiento de toda una población a una escala sin precedentes, facilitado por las nuevas tecnologías digitales¹⁸⁰. A medida que los Estados avanzan hacia un sistema de biovigilancia para combatir la pandemia, se ha incrementado el uso del rastreo digital, los drones automatizados y otras tecnologías que pretenden servir de ayuda para gestionar la migración y detener la propagación del

¹⁷⁰ *Ibid.*

¹⁷¹ *Ibid.*

¹⁷² *Ibid.*

¹⁷³ Comunicación de Mijente, en que se cita Sarah Lamdan, “When Westlaw fuels ICE surveillance: legal ethics in the era of big data policing”, *New York University Review of Law and Social Change*, vol. 43, núm. 2 (2019).

¹⁷⁴ Comunicación de Mijente, en que se cita <https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html>.

¹⁷⁵ *Ibid.*

¹⁷⁶ Comunicación de Minority Rights Group International.

¹⁷⁷ Comunicación de Mijente.

¹⁷⁸ *Ibid.*

¹⁷⁹ *Ibid.*

¹⁸⁰ Véase <https://www.newstatesman.com/science-tech/2020/03/rise-bio-surveillance-state>.

virus¹⁸¹. Existe un riesgo enorme de que estas tecnologías permitan una mayor discriminación por motivos de raza, etnia y situación en materia de ciudadanía¹⁸².

IV. Recomendaciones

61. La Relatora Especial alude a su anterior informe al Consejo de Derechos Humanos y recuerda a los Estados sus obligaciones internacionales en materia de derechos humanos aplicables, en particular:

- a) La prohibición de la discriminación racial en el diseño y uso de las tecnologías digitales emergentes;
- b) Las obligaciones de prevenir y combatir la discriminación racial en el diseño y uso de las tecnologías digitales emergentes;
- c) Las obligaciones de proporcionar vías de recurso eficaces en los casos de discriminación racial en el diseño y uso de las tecnologías digitales emergentes.

62. La Relatora Especial reitera el análisis y las recomendaciones contenidas en su informe anterior sobre las obligaciones de los Estados y de los actores no estatales e insta a los Estados a que las tengan en cuenta junto con las recomendaciones incluidas en el presente informe. En el contexto específico del control de las fronteras y la inmigración, recomienda a los Estados Miembros:

a) Hacer frente a las ideologías y estructuras racistas y xenófobas que han dado forma al control y la administración de las fronteras y de la inmigración. Los efectos de la tecnología son en gran parte producto de las fuerzas sociales, políticas y económicas subyacentes que impulsan el diseño y el uso de la tecnología. Si no se produce un cambio fundamental de los enfoques políticos racistas, xenófobos, contra los migrantes, contra las personas sin estado y contra los refugiados de la gobernanza de las fronteras, no se podrán corregir los efectos discriminatorios de las fronteras digitales que se ponen de manifiesto en el presente informe. Los Estados deben cumplir con la obligación internacional de derechos humanos de prevenir la discriminación racial en el control de las fronteras y de la inmigración y aplicar las recomendaciones contenidas en el informe anterior de la Relatora Especial. Los Estados también deben seguir la orientación proporcionada por los Principios sobre la Privación de la Nacionalidad como Medida de Seguridad Nacional¹⁸³ y los Principios de Protección para las Personas Migrantes, Refugiadas y Desplazadas durante la COVID-19¹⁸⁴, que articulan las obligaciones existentes de los Estados, entre otras cosas con respecto a la igualdad y la no discriminación, para garantizar el respeto de los derechos humanos de las personas migrantes, refugiadas y apátridas, entre otras;

b) Adoptar y reforzar los enfoques jurídicos y de política de igualdad racial y no discriminación basados en los derechos humanos para el uso de las tecnologías digitales en el control y la administración de las fronteras y de la inmigración. En la actualidad no existe un marco regulador integrado de gobernanza global para el uso de las tecnologías automatizadas y otras tecnologías digitales, lo que no hace más que resaltar la importancia de respetar las obligaciones jurídicas internacionales existentes en materia de derechos humanos en la regulación del diseño y el uso de estas tecnologías;

c) Adoptar las medidas recomendadas por el Comité para la Eliminación de la Discriminación Racial en su recomendación general núm. 36 (2020), relativa a la prevención y la lucha contra la elaboración de perfiles raciales por los agentes del orden,

¹⁸¹ Véase <https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf>.

¹⁸² *Ibid.*

¹⁸³ Véase <https://files.institutesi.org/PRINCIPLES.pdf>.

¹⁸⁴ Instituto Zolberg sobre Migración y Movilidad *et al.*, “Principles of Protection for Migrants, Refugees, and Displaced People During COVID-19”, (2020).

en particular las recomendaciones sobre la adecuación del uso de la inteligencia artificial al derecho internacional de los derechos humanos;

d) Garantizar, tanto a nivel nacional como internacional, que el control y la administración de las fronteras y la inmigración estén sujetos a obligaciones legales vinculantes para prevenir, combatir y recurrir la discriminación racial y xenófoba en el diseño y el uso de las tecnologías digitales en las fronteras. Esas obligaciones incluyen, entre otras, las siguientes:

i) Medidas rápidas y eficaces para prevenir y mitigar el riesgo del uso y el diseño racialmente discriminatorio de las tecnologías digitales en las fronteras, entre otras cosas, estableciendo como condición *sine qua non* la realización de una evaluación de su impacto en la igualdad racial y en el principio de no discriminación para el despliegue público de los sistemas. Estas evaluaciones de impacto deben incorporar oportunidades significativas para que los representantes de los grupos marginados racial o étnicamente, incluidas las personas refugiadas, migrantes, apátridas y otras personas, puedan participar en el diseño y la aplicación de las tecnologías. No bastará con la adopción de un enfoque puro o primordialmente voluntario para la realización de las evaluaciones de los efectos sobre la igualdad: será esencial un enfoque obligatorio;

ii) Una moratoria inmediata para la adquisición, la venta, la transferencia y el uso de tecnología de vigilancia, hasta que se establezcan sólidas salvaguardias de derechos humanos para regular dichas prácticas. Esas salvaguardias incluyen una diligencia debida en materia de derechos humanos que cumpla con las prohibiciones de la legislación internacional sobre derechos humanos por lo que respecta a la discriminación racial, la supervisión independiente, las leyes estrictas de privacidad y protección de datos, y la plena transparencia sobre el uso de herramientas de vigilancia como las grabaciones de vídeo y la tecnología de reconocimiento facial. En algunos casos, será necesario imponer prohibiciones absolutas a las tecnologías que no puedan cumplir las normas consagradas en los marcos jurídicos internacionales de derechos humanos que prohíben la discriminación racial;

iii) Transparencia y rendición de cuentas en el uso de las tecnologías digitales en las fronteras por parte de los sectores público y privado, y posibilidades de efectuar un análisis y una supervisión independientes, entre otras cosas utilizando únicamente sistemas que puedan ser auditados;

iv) Obligaciones legales para que las empresas privadas prevengan, combatan y proporcionen vías de recurso en los casos de discriminación racial y xenófoba resultante del uso de las tecnologías de las fronteras digitales;

v) Alianzas público-privadas para el suministro y el uso de tecnologías digitales en las fronteras que sean transparentes y estén sujetas a una supervisión independiente en lo que respecta a los derechos humanos, y que no se traduzcan en una renuncia de los Gobiernos a sus responsabilidades en materia de derechos humanos.

63. La Relatora Especial tuvo la oportunidad de celebrar consultas con representantes del ACNUR y de la OIM sobre el uso que hacen de las tecnologías digitales en las fronteras. Sobre la base de esas consultas, recomienda que ambas entidades adopten y apliquen mecanismos para la participación y la toma de decisiones sostenidas y genuinas de las personas migrantes, refugiadas y apátridas en la implantación, el uso y la revisión de las tecnologías digitales en las fronteras.

64. Además, recomienda que la OIM:

a) Incorpore y refuerce las obligaciones y los principios internacionales en materia de derechos humanos, especialmente los relativos a la igualdad y la no discriminación, en su uso y supervisión de las tecnologías digitales en las fronteras digitales, en particular en todas sus alianzas con entidades públicas y privadas. Para ello es necesario no limitarse a un enfoque restringido a las preocupaciones de

privacidad relacionadas con el intercambio de datos y la protección de datos y obligar a aplicar protecciones de igualdad y no discriminación, en lugar de recomendar su aplicación;

b) Adopte políticas y prácticas obligatorias para el análisis sistémico de los efectos potencialmente dañinos y discriminatorios de las tecnologías digitales en las fronteras antes de la adopción de esas tecnologías, y prohíba la adopción de tecnologías que no puedan demostrar que cumplen los requisitos de igualdad y no discriminación. Debería proporcionar directrices más claras y concretas, basadas en los derechos humanos, sobre los criterios para la designación de tecnologías digitales de una “opción cero” y garantizar la aplicación de dichas directrices;

c) Adopte protocolos obligatorios de evaluación continua de los derechos humanos en relación con las tecnologías digitales en las fronteras una vez implantadas.

65. En comparación con la OIM, el ACNUR ha tomado más medidas para comprometerse con las normas de igualdad y no discriminación en sus marcos de orientación relativos a las tecnologías digitales en las fronteras, pero también tiene que hacer un trabajo adicional significativo para garantizar que esas normas se lleven a la práctica. Al respecto, la Relatora Especial recomienda al ACNUR que:

a) Garantice la aplicación efectiva de sus políticas y prácticas para el análisis sistémico de los efectos potencialmente perjudiciales y discriminatorios de las tecnologías digitales en las fronteras antes de su adopción y prohíba la adopción de tecnologías que no puedan demostrar que cumplen los requisitos de igualdad y no discriminación. Debería proporcionar directrices más claras y concretas, basadas en los derechos humanos, sobre los criterios para la designación de tecnologías digitales de una “opción cero” y garantizar la aplicación de dichas directrices;

b) Garantice el uso y la aplicación de protocolos obligatorios de evaluación continua de los derechos humanos para las tecnologías digitales en las fronteras una vez implantadas.

66. La Relatora Especial recomienda a la OIM y el ACNUR que:

a) Creen mecanismos para la supervisión independiente de los derechos humanos en su uso de las tecnologías digitales en las fronteras y apliquen reformas para garantizar una mayor transparencia en la forma en que se toman las decisiones para adoptar estas tecnologías;

b) Proporcionen a las personas migrantes, refugiadas, apátridas y otras personas mecanismos para que rindan cuentas directamente de las violaciones de sus derechos humanos derivadas del uso de las tecnologías digitales en las fronteras.

67. Todos los organismos humanitarios y afines de las Naciones Unidas deberían poner en práctica las recomendaciones antes mencionadas dirigidas a la OIM y al ACNUR.