Naciones Unidas A/75/590

Asamblea General

Distr. general
10 de noviembre de 2020
Español
Original: inglés

Septuagésimo quinto período de sesiones
Tema 70 b) del programa
Eliminación del racismo, la discriminación racial, la xenofobia y las formas conexas de intolerancia: aplicación y seguimiento generales de la Declaración y el Programa de Acción de Durban

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

Nota del Secretario General

La Secretaría tiene el honor de transmitir a la Asamblea General el informe de la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia, E. Tendayi Achiume, preparado de conformidad con la resolución 74/137 de la Asamblea General.

* Este informe se presenta con retraso debido a circunstancias ajenas a la voluntad de la Relatora Especial.

Informe de la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia

Resumen

Los gobiernos y los organismos de las Naciones Unidas están desarrollando y utilizando las nuevas tecnologías digitales de manera particularmente experimental, peligrosa y discriminatoria en el contexto de las medidas de control de las fronteras y de la inmigración. Al hacerlo, vulneran los derechos humanos de los refugiados, migrantes, apátridas y otras personas y obtienen de ellos grandes cantidades de datos en condiciones de explotación que los privan de su capacidad de acción y dignidad humanas fundamentales.

En el presente informe se resalta la forma en que se están desplegando tecnologías digitales para promover ideologías xenófobas y racialmente discriminatorias que han llegado a ser tan prevalentes, en parte debido a determinadas percepciones generalizadas de que los refugiados y los migrantes constituyen por sí mismos una amenaza para la seguridad nacional. En otros casos, la discriminación y la exclusión se producen aunque no exista una animadversión expresa, sino como resultado de la búsqueda de la eficiencia burocrática y humanitaria sin mantener las necesarias salvaguardias de los derechos humanos. En el informe también se señala que los enormes beneficios económicos asociados a la securitización de las fronteras y la digitalización del control fronterizo son una parte importante del problema.

Índice

I. Introducción

1. En el presente informe la Relatora Especial continúa el análisis iniciado en su informe más reciente al Consejo de Derechos Humanos, titulado “La discriminación racial y las tecnologías digitales emergentes: un análisis de los derechos humanos”[1]. En ese informe, la Relatora Especial introdujo un enfoque de la gobernanza de las nuevas tecnologías digitales en materia de derechos humanos que se basaba en el criterio de la igualdad y ponía énfasis en la discriminación racial resultante del diseño y la utilización de esas tecnologías. Instó a los agentes estatales y no estatales a superar las estrategias de “daltonismo racial” o “neutralidad racial”, que ignoraban las repercusiones de sesgo racial y étnico de las nuevas tecnologías digitales, y a encarar directamente las formas intersectoriales de discriminación que se derivaban de la adopción generalizada de esas tecnologías y se veían exacerbadas por ellas. Ese informe se centró en las personas que eran objeto de discriminación principalmente por motivos de raza y origen étnico, incluida la condición de indígena, y destacó los efectos del género, la religión y la discapacidad. El presente informe a la Asamblea General aporta un matiz adicional pues se centra en los efectos xenófobos y racialmente discriminatorios de las nuevas tecnologías digitales en los migrantes, los apátridas, los refugiados y otros no ciudadanos, así como en los nómadas y otros pueblos para los que las tradiciones migratorias son fundamentales. El término “refugiados” incluye a los solicitantes de asilo que cumplen los criterios de la definición de refugiados, pero cuya condición de refugiados aún no ha sido reconocida oficialmente por ningún Estado.

2. Aunque el empleo de las nuevas tecnologías digitales ya es común en la gobernanza de todos los aspectos de la sociedad, existen preocupaciones particulares en el contexto de las fronteras y la inmigración que obedecen a, por lo menos, dos razones. En la mayoría, si no en todos los marcos de gobernanza nacional:

a) Los no ciudadanos, los apátridas y los grupos afines tienen menos derechos y protecciones legales contra el abuso del poder del Estado y pueden ser objeto de formas singulares de violencia xenófoba privada;

b) El ejecutivo y otros poderes de gobierno conservan amplias facultades discrecionales, no revisables, en el ámbito de la aplicación de la normativa de fronteras e inmigración, que no están sujetan a las limitaciones sustantivas y de procedimiento habituales, garantizadas a los ciudadanos en la constitución y por otros medios.

3. Como se resalta en el presente informe, los gobiernos y los agentes no estatales están desarrollando e implantando nuevas tecnologías digitales de manera singularmente experimental, peligrosa y discriminatoria en el contexto de la aplicación de medidas de control de fronteras e inmigración. Al hacerlo, vulneran los derechos humanos de los refugiados, migrantes, apátridas y otras personas y obtienen de ellos grandes cantidades de datos en condiciones de explotación que los privan de su capacidad de acción y dignidad humanas fundamentales. Aunque el presente informe se centra en innovaciones tecnológicas relativamente recientes, muchas de ellas tienen antecedentes históricos en las tecnologías de gobernanza colonial con sesgo racial, aplicadas incluso mediante los controles de la migración. No se trata solamente de que la tecnología no es neutral, sino de que su diseño y utilización suelen reforzar las tendencias sociales, políticas y económicas dominantes. Como se ha resaltado en informes anteriores, el resurgimiento del populismo etnonacionalista en todo el mundo ha tenido graves consecuencias xenófobas y discriminatorias para los refugiados, los migrantes y los apátridas[2]. En el presente informe se resalta la forma

[1] A/HRC/44/57.

[2] Véase, por ejemplo, A/73/312.

en que se están desplegando tecnologías digitales para promover ideologías xenófobas y racialmente discriminatorias que han llegado a ser prevalentes, en parte debido a determinadas percepciones generalizadas de que los refugiados y los migrantes constituyen por sí mismos una amenaza para la seguridad nacional. En otros casos, la discriminación y la exclusión se producen aunque no exista una animadversión expresa, sino como resultado de la búsqueda de la eficiencia burocrática y humanitaria sin mantener las necesarias salvaguardias de los derechos humanos. En el informe también se resalta cómo la securitización en curso de las fronteras y los enormes beneficios económicos conexos constituyen una parte importante del problema.

4. Los refugiados, migrantes y apátridas son objeto de las violaciones enumeradas en el presente informe debido a su origen nacional, raza, etnia y religión y otros motivos inadmisibles. Esas violaciones no pueden descartarse como distinciones aceptables entre ciudadanos y no ciudadanos. A este respecto, la Relatora Especial apunta a su anterior informe sobre la discriminación racial sobre la base de la ciudadanía, la nacionalidad y la situación migratoria, en el que pone de relieve las tendencias discriminatorias y la aplicación de las normas internacionales de derechos humanos en lo que respecta a esas violaciones[3].

5. Muchos de los mismos factores destacados en el informe de la Relatora Especial al Consejo de Derechos Humanos son antecedentes esenciales del presente informe, por lo que recomienda que se lea conjuntamente con el informe mencionado anteriormente[4]. Su informe anterior es especialmente útil, entre otras razones, para explicar los mecanismos que causan la discriminación racial a través de las nuevas tecnologías digitales y para resaltar las fuerzas económicas, políticas y sociales de otro tipo que impulsan la expansión del uso discriminatorio de esas tecnologías. La Relatora Especial reitera que, pese a la sensación generalizada de que las tecnologías digitales emergentes son neutrales y objetivas en su funcionamiento, la raza, el origen étnico y nacional y la ciudadanía determinan el ejercicio y disfrute de los derechos humanos en todos los campos en los que esas tecnologías hoy se aplican ampliamente. Los Estados tienen la obligación de prevenir y combatir esta discriminación racial y ofrecer recursos para corregirla, y los agentes privados, como las empresas, tienen la responsabilidad conexa de hacer otro tanto. En el contexto de la aplicación de la ley en materia de fronteras e inmigración, como en otros contextos, para prevenir las violaciones de los derechos humanos tal vez sea necesario prohibir del todo o abolir el uso de tecnologías si resultara imposible controlar o mitigar sus efectos.

6. En la preparación del informe, la Relatora Especial aprovechó las aportaciones valiosas de: las reuniones de grupos de expertos 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 la UCLA, el Institute on Statelessness and Inclusion, y el Migration and Technology Monitor; entrevistas con investigadores y con apátridas, migrantes y refugiados; y comunicaciones recibidas de diversas partes interesadas en respuesta a una convocatoria pública de presentación de comunicaciones. Las comunicaciones no confidenciales se podrán consultar en el sitio web de la Relatoría.

[3] A/HRC/38/52.
[4] A/HRC/44/57.

II. El auge de las fronteras digitales

7. La tecnología siempre ha formado parte de la aplicación de las medidas de control fronterizo y de inmigración, y se entiende debidamente que instrumentos que van desde los pasaportes hasta las barreras fronterizas físicas son elementos característicos de esta tecnología. El presente informe se centra concretamente en el uso creciente de las tecnologías digitales para aplicar las medidas de control fronterizo y de inmigración, en tal magnitud que algunos comentaristas se refieren correctamente al auge de las "fronteras digitales", expresión que en este informe se refiere a las fronteras cuyas infraestructuras y procesos dependen cada vez más del aprendizaje automático, los sistemas automatizados de adopción de decisiones sobre la base de algoritmos, los análisis predictivos y las tecnologías digitales conexas[5]. Estas tecnologías se integran en los documentos de identificación, los sistemas de reconocimiento facial, los sensores terrestres, los vehículos aéreos de vigilancia no tripulados, las bases de datos biométricos, los procesos de adopción de decisiones en materia de asilo y muchas otras facetas de la aplicación de las leyes sobre fronteras e inmigración.

8. En general, las tecnologías digitales usadas en el control de las fronteras refuerzan regímenes de control fronterizo paralelos que segregan la movilidad y migración de los diferentes grupos en función del origen nacional y la categoría, entre otras cosas. Los controles de fronteras automatizados son un ejemplo del uso de esos regímenes paralelos. En una comunicación se ofreció el ejemplo de "eGates", sistema implantado en los puertos de entrada irlandeses, como el aeropuerto de Dublín, donde los titulares de pasaportes electrónicos de la Unión Europea y el Espacio Económico Europeo y Suiza podían pasar por la ventanilla eGates, en régimen de "autoservicio", para realizar el control de inmigración[6]. En la comunicación se señala que "solo ciertas nacionalidades pueden emplear método de 'autoservicio', y las nacionalidades incluidas son las naciones ricas y blancas (con excepción del Japón)". Quienes no sean ciudadanos de la Unión Europea y el Espacio Económico Europeo o de Suiza y arriben a Irlanda por aire o por mar deben presentarse a un oficial de inmigración a su llegada.

9. Una de las facetas de las fronteras digitales es el uso generalizado de los datos biométricos o el "reconocimiento automatizado de las personas basado en sus características biológicas y de comportamiento"[7]. Entre los datos biométricos figuran las huellas dactilares y los datos obtenidos mediante el escaneo de retina y el reconocimiento facial o con métodos menos conocidos como el reconocimiento del patrón de venas y vasos capilares, la forma de la oreja y el movimiento al andar, entre otros. Los datos biométricos se utilizan para establecer, registrar y verificar la identidad de los migrantes y refugiados. Las Naciones Unidas, por ejemplo, han reunido los datos biométricos de más de 8 millones de personas, la mayoría de las cuales huían de conflictos o necesitaban asistencia humanitaria[8]. Los investigadores han documentado los orígenes raciales de las tecnologías biométricas[9], así como su funcionamiento discriminatorio contemporáneo sobre la base de la raza, el origen

[5] 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 (enero de 2007), págs. 71 a 92.

[6] Comunicación del Immigrant Council of Ireland.

[7] Véase https://www.biometricsinstitute.org/what-is-biometrics/.

[8] Estos enormes conjuntos de datos son extremadamente difíciles de rastrear y también pueden incluir datos antiguos actualizados con datos biométricos recién recopilados. Véase, por ejemplo, http://humanitarian-congress-berlin.org/2018/.

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

étnico y el género[10]. En un informe reciente sobre la tecnología de reconocimiento facial desplegada en cruces de fronteras, como los aeropuertos, se señala que la frecuencia de error de incluso los mejores algoritmos en el reconocimiento de las mujeres negras es veinte veces mayor que en el reconocimiento de los hombres blancos; pese a ello, el uso de esas tecnologías está aumentando en todo el mundo[11]. Como se señala en ese informe, "cuando se aplica el reconocimiento facial como tecnología de control de acceso, los viajeros quedan excluidos de los mecanismos de control fronterizo por motivos de raza, género y otras características demográficas (por ejemplo, el país de origen)". Este trato diferencial suele redundar en que se perpetúan los estereotipos negativos, e incluso la discriminación prohibida, lo que para los solicitantes de asilo puede conducir a la devolución.

10. Los ejemplos que figuran a continuación muestran que la recopilación de datos biométricos de refugiados y migrantes por los gobiernos y agentes humanitarios está vinculada a graves violaciones de los derechos humanos de esos grupos, a pesar de las justificaciones burocráticas y humanitarias en que se basa la reunión de esos datos. Además, no está claro qué sucede con los datos biométricos recogidos y si los grupos afectados tienen acceso a sus propios datos. El Programa Mundial de Alimentos (PMA), por ejemplo, ha sido criticado por haberse asociado a la empresa de minería de datos Palantir Technologies mediante un contrato de 45 millones de dólares de los Estados Unidos, pues ello supone riesgos para el procesamiento y la seguridad de los datos de 92 millones de receptores de ayuda que administra el PMA y la responsabilidad conexa[12]. Empresas privadas como Palantir han sido proveedores indispensables de la tecnología que utilizan los programas de detención y deportación del Servicio de Inmigración y Control de Aduanas y el Departamento de Seguridad Nacional de los Estados Unidos, lo que plantea preocupaciones justificadas acerca de la complicidad corporativa en las violaciones de derechos humanos asociadas a estos programas[13]. Todavía no está claro qué mecanismo de rendición de cuentas sobre el intercambio de datos se establecerá durante la asociación entre el Programa Mundial de Alimentos y Palantir o si los interesados podrán optar por no aportar sus datos[14]. La reunión de datos no es un ejercicio apolítico, especialmente en los casos en que agentes poderosos del Norte Global reúnen información sobre poblaciones vulnerables, sin métodos que regulen la supervisión y la rendición de cuentas[15]. La recopilación cada vez más entusiasta de datos sobre poblaciones de migrantes ha sido criticada por que entraña la posibilidad de que se vulnere de manera significativa la privacidad de las personas y suscita preocupaciones en materia de derechos humanos[16].

11. La historia ofrece muchos ejemplos de la utilización discriminatoria e incluso letal de datos de grupos marginados. La Alemania nazi reunió estratégicamente enormes cantidades de datos sobre las comunidades judías para facilitar el

[10] Véase A/HRC/44/57.

[11] Tamir Israel, "Facial recognition at a crossroads: transformation at our borders and beyond" (septiembre de 2020).

[12] Véase www.thenewhumanitarian.org/news/2019/02/05/un-palantir-deal-data-mining-protection-concerns-wfp.

[13] Véase www.technologyreview.com/2018/10/22/139639/amazon-is-the-invisible-backbone-behind-ices-immigration-crackdown/.

[14] Véase www.devex.com/news/opinion-the-wfp-and-palantir-controversy-should-be-a-wake-up-call-for-humanitarian-community-94307.

[15] Dragana Kaurin, "Data protection and digital agency for refugees", documento de investigación núm. 12 del World Refugee Council (mayo de 2019), que puede consultarse en www.cigionline.org/publications/data-protection-and-digital-agency-refugees.

[16] Véase www.chathamhouse.org/2018/03/beware-notion-better-data-lead-better-outcomes-refugees-and-migrants.

Holocausto, en gran medida en asociación con una empresa privada: la IBM[17]. Otros genocidios también aprovecharon el rastreo sistemático de grupos, como el registro de tutsis basado en tarjetas de identidad étnica, que contribuyó a la magnitud del genocidio en Rwanda en 1994[18]. Después del 11 de septiembre, los Estados Unidos experimentaron con varias modalidades de reunión de datos sobre poblaciones marginadas a través del Sistema de Registro de Entradas y Salidas del Departamento de Seguridad Nacional, que recopiló fotografías, datos biométricos e incluso datos de entrevistas directas con más de 84.000 personas, procedentes en su mayoría de Estados árabes que habían sido marcados por el sistema[19]. En todos esos casos, diferentes actores, incluidos los gobiernos, explotaron las ideas sobre la neutralidad o la necesidad no prejudicial de la reunión de datos de grupos marginados y luego dieron a esos grupos un trato selectivo de manera discriminatoria.

12. Para vigilar y asegurar los espacios fronterizos también se utilizan cada vez más las tecnologías autónomas. Por ejemplo, la Agencia Europea de la Guardia de Fronteras y Costas (Frontex), ha estado probando diversos vehículos aéreos no tripulados de uso militar en los mares Mediterráneo y Egeo para vigilar e interceptar embarcaciones de migrantes y refugiados que desean llegar a las costas europeas[20]. Una investigación conjunta de Bellingcat, *Lighthouse Reports*, *Der Spiegel*, TV Asahi y *Report Mainz* generó pruebas creíbles en octubre de 2020 de que Frontex había sido cómplice en los rechazos[21] o los retornos forzados de refugiados y migrantes a través de las fronteras, sin tener en cuenta las circunstancias individuales y sin ofrecer la posibilidad de solicitar asilo o de apelar decisiones. Esos rechazos probablemente violan las obligaciones de no devolución previstas en el derecho internacional y se ven favorecidos por las tecnologías de vigilancia. En una comunicación se destacaron ciertas novedades jurídicas que se habían producido en Grecia y que permitían a la policía utilizar drones para vigilar la migración irregular en las regiones fronterizas, pero sin garantizar la protección jurídica necesaria de los derechos humanos de las personas sometidas a esa vigilancia[22].

13. El uso de tecnologías autónomas militares o cuasimilitares refuerza el nexo entre la inmigración, la seguridad nacional y el impulso creciente hacia la penalización de la migración y el uso de taxonomías basadas en el riesgo para definir y señalar los casos [23]. Los Estados, en particular los que tienen fronteras a las que arriba un gran número de refugiados y migrantes, han venido utilizando diversos medios para adelantarse a quienes tratan de solicitar asilo legalmente y disuadirlos. Este cambio normativo hacia la penalización del asilo y la migración sirve para justificar tecnologías cada vez más radicales e invasivas como los vehículos aéreos no tripulados y diversos mecanismos de control fronterizo como los sensores remotos y las torres fijas integradas con cámaras de luz infrarroja (llamadas torres de vigilancia autónomas) para mitigar el “entorno de riesgo” en las fronteras[24]. Estas

[17] Edwin Black, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America’s Most Powerful Corporation* (Dialog Press, 2012).

[18] Véase www.theengineroom.org/dangerous-data-the-role-of-data-collection-in-genocides/.

[19] Véase www.aclu.org/issues/immigrants-rights/immigrants-rights-and-detention/national-security-entry-exit-registration.

[20] Petra Molnar, “Technological testing grounds: migration management experiments and reflections from the ground up” (noviembre de 2020).

[21] Véanse www.bellingcat.com/news/2020/10/23/frontex-at-fault-european-border-force-complicit-in-illegal-pushbacks y www.spiegel.de/international/europe/eu-border-agency-frontex-complicit-in-greek-refugee-pushback-campaign-a-4b6cba29-35a3-4d8c-a49f-a12daad450d7.

[22] Comunicación de Homo Digitalis.

[23] Comunicación de Dimitri van den Meerssche.

[24] Raluca Csernatoni, “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.

tecnologías pueden generar resultados dramáticos. Si bien se ha dicho que las llamadas tecnologías de “fronteras inteligentes” son una alternativa más humana a otros regímenes de control, en los estudios se ha documentado que las tecnologías de ese tipo empleadas en la frontera entre los Estados Unidos y México, por ejemplo, en realidad han aumentado el número de muertes de migrantes y han desviado las rutas de migración hacia territorios más peligrosos, a través del desierto de Arizona[25]. Chambers y otros han determinado que las muertes de migrantes han aumentado en más del doble desde que se introdujeron esas nuevas tecnologías[26], creando una “tierra de tumbas a cielo abierto”[27].

14. Es probable que el uso de esas tecnologías por las autoridades de seguridad fronteriza aumente en el “complejo tecnológico militarizado” del espacio fronterizo, sin las debidas consultas públicas, marcos de rendición de cuentas y mecanismos de supervisión[28]. En una comunicación se presentó un ejemplo de la zona desmilitarizada de la península de Corea, donde la República de Corea había desplegado armas semiautónomas estacionarias operadas por control remoto[29]. El Gobierno de la República de Corea declaró que no tenía intención de desarrollar o adquirir sistemas de armas autónomas letales[30]. Debido a la falta de transparencia, a menudo es difícil determinar la situación del despliegue de sistemas de armas autónomos en las fronteras. En previsión del despliegue de sistemas de este tipo, es fundamental que los Estados den cuenta de los efectos desproporcionados, desde el punto racial, étnico y nacional, que las armas plenamente autónomas tendrían en los grupos vulnerables, especialmente los refugiados, los migrantes, los solicitantes de asilo, los apátridas y los grupos conexos, y que procuren evitarlos.

15. Los Estados Miembros de las Naciones Unidas y múltiples órganos de la Organización dependen cada vez más del análisis de macrodatos para fundamentar sus políticas. Por ejemplo, la Matriz de Seguimiento de los Desplazamientos de la Organización Internacional para las Migraciones (OIM) vigila a las poblaciones en movimiento para predecir mejor las necesidades de las personas desplazadas, utilizando registros de llamadas de teléfonos móviles y etiquetado geográfico, así como análisis de la actividad en los medios sociales[31]. En los Estados Unidos de América también se están utilizando los análisis de macrodatos para predecir los probables resultados satisfactorios del reasentamiento de refugiados sobre la base de sus vínculos comunitarios anteriores[32]. En un entorno mundial que es cada vez más antiinmigrante, han surgido críticas en el sentido de que los datos sobre migración también se han interpretado erróneamente y se han tergiversado con fines políticos, por ejemplo para afectar la distribución de la ayuda. Los datos incorrectos también pueden utilizarse para avivar el miedo y la xenofobia, como indican la caracterización del grupo de migrantes que intenta solicitar asilo en la frontera entre los Estados Unidos y México[33] o la incitación de sentimientos contra los migrantes en la región

[25] Samuel Norton Chambers y otros, “Mortality, surveillance and the tertiary ‘funnel effect’ on the U.S.-Mexico border: a geospatial modeling of the geography of deterrence”, *Journal of Borderlands Studies* (2019).

[26] *Ibid.*

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

[28] Raluca Csernatoni, “Constructing the EU’s high-tech borders: Frontex and dual-use drones for border management”.

[29] Comunicación de Campaign to Stop Killer Robots.

[30] *Ibid.*

[31] Véase https://dtm.iom.int/about.

[32] Véase https://news.stanford.edu/2018/01/18/algorithm-improves-integration-refugees/.

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

del Mediterráneo, incluida la propuesta reciente de instalar barreras flotantes[34]. A nivel de la sociedad, ese temor se utiliza para justificar respuestas extremistas que contravienen las normas internacionales de derechos humanos[35]. Como se señala en una comunicación, en contextos políticos polarizados, antiinmigrantes e incluso xenófobos, “los datos utilizados para alimentar los algoritmos de aprendizaje automático en las fronteras o los utilizados en campañas políticas o para elaborar legislación pueden contener errores, y en un entorno de sesgo estructural contra las minorías esa tergiversación de los datos puede avivar la desinformación, el discurso de odio y la violencia”[36].

16. Para evaluar el panorama de los derechos humanos en las fronteras digitales es fundamental tener en cuenta el papel de las empresas privadas, cuyo afán de lucro ha sido decisivo para impulsar la expansión de las tecnologías digitales en el control de la inmigración y las fronteras, a menudo en forma de asociaciones que permiten a los gobiernos abdicar de su responsabilidad por las violaciones que puedan derivarse del uso de esas tecnologías. Se ha empleado el término “complejo industrial fronterizo” para describir “el nexo entre el control y la vigilancia de las fronteras, la militarización y los intereses financieros”[37], pues los gobiernos recurren cada vez más al sector privado para gestionar la migración mediante nuevas tecnologías, aplicando criterios predominantes de seguridad nacional que pasan por alto los derechos humanos fundamentales[38]. Las tendencias que nutren el complejo industrial fronterizo son la externalización, la militarización y la automatización de las fronteras.[39] En los Estados Unidos, el presupuesto para la aplicación del control de las fronteras y la inmigración ha aumentado en más de un 6.000 % desde 1980[40]. El presupuesto de la Unión Europea para la gestión de las fronteras exteriores, la migración y el asilo en 2021-2027 se multiplicará por 2,6 y ascenderá a más de 34.900 millones de euros, frente a los 13.000 millones de euros presupuestados para 2014-2020[41]. Según indican estudios de mercado recientes, la tasa compuesta de crecimiento anual de este mercado de seguridad fronteriza mundial se situará entre el 7,2 % y el 8,6 % (65.000 a 68.000 millones de dólares) en 2025[42].

17. Entre las nuevas tecnologías digitales implantadas en el complejo industrial fronterizo, son fundamentales los vehículos aéreos no tripulados empleados en la vigilancia de las fronteras y los datos biométricos que ayudan a erigir “fronteras inteligentes”[43]. Las grandes empresas que son proveedores y beneficiarios del sector de servicios de vigilancia fronteriza son principalmente empresas militares del Norte Global, algunas de las cuales, como Lockheed Martin, se encuentran entre los mayores vendedores de armas del mundo[44]. Las empresas de tecnología de la información, como IBM, son también agentes importantes del sector, incluso en las funciones de reunión y procesamiento de datos[45]. Muchos de esos agentes

[34] Véase www.dezeen.com/2020/02/10/greece-floating-sea-border-wall-news/.
[35] Véanse también Ana Beduschi, “International migration management in the age of artificial intelligence”, *Migration Studies* (2020); y la comunicación de Ana Beduschi.
[36] Comunicación de Minority Rights Group International.
[37] Véase www.aljazeera.com/opinions/2019/11/1/why-climate-action-needs-to-target-the-border-industrial-complex/.
[38] Comunicación de Dhakshayini Sooriyakumaran y Brami Jegan.
[39] *Ibid.*
[40] *Ibid.*
[41] Véase https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4106.
[42] Véanse www.issuewire.com/border-security-system-industry-projected-to-garner-usd-6781-billion-by-2025-flir-systems-lockhee-1631530966252699 y www.marketresearchfuture.com/reports/border-security-market-1662.
[43] Comunicación de Dhakshayini Sooriyakumaran y Brami Jegan.
[44] *Ibid.*
[45] *Ibid.*

empresariales ejercen una gran influencia en la adopción de decisiones, a nivel nacional e internacional, sobre la gobernanza de la industria de las fronteras digitales[46]. La "puerta giratoria" entre la función pública y las empresas privadas hace que se reduzca y se difumine la separación entre el gobierno (control de fronteras, sector militar) y la industria (empresas de seguridad y consultoría)[47]. Las empresas también están vinculadas con los gobiernos mediante empresas mixtas. Según una comunicación, por ejemplo, en 2016 la empresa público-privada francesa Civipol creó bases de datos de huellas dactilares para Malí y el Senegal[48]. Esos proyectos, financiados 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, tienen como objetivo identificar a los refugiados que llegan a Europa desde esos dos países y deportarlos[49]. Francia es propietaria del 40 % de las acciones de Civipol, mientras que los productores de armas Airbus, Safran y Thales detentan cada uno más del 10 % de las acciones[50]. Este ejemplo ilustra mejor la manera en que los países del Norte Global emplean la ayuda internacional para promover sus programas fronterizos en el Sur Global.

18. Un investigador ha señalado la preocupación apremiante que suscita el auge del "tecnocolonialismo", que pone de relieve "el papel constitutivo que tienen los datos y la innovación digital en el afianzamiento de las desigualdades entre los refugiados y los organismos humanitarios y, en última instancia, las desigualdades en el contexto mundial"[51], intensificadas en parte por los beneficios de las empresas y por el hecho de que los gobiernos abdican de su responsabilidad en materia de derechos humanos. Esas desigualdades se afianzan mediante experimentos tecnológicos, la extracción de datos y valores y las formas directas e indirectas de discriminación descritas en la sección III del presente documento.

19. En resumen, muchas tecnologías digitales aplicadas en las fronteras sustituyen o contribuyen a los procesos humanos de adopción de decisiones, a veces en formas que suscitan profunda inquietud en materia de derechos humanos. Esas tecnologías también amplían el poder y el control que los gobiernos y los agentes privados pueden ejercer sobre los migrantes, los refugiados, los apátridas y otras personas, al tiempo que protegen ese poder de las restricciones jurídicas y judiciales. Es decir, amplían las posibilidades de que se cometan abusos graves de los derechos humanos y lo hacen de manera que se eluden las protecciones sustantivas y de procedimiento que normalmente son indispensables en el contexto de la aplicación de la ley en las fronteras. En la sección III se pone de relieve la gama de violaciones discriminatorias de los derechos humanos facilitadas por los mecanismos y la infraestructura tecnológica digital en las fronteras y se llama la atención sobre esa expansión de las competencias y reducción de las restricciones.

[46] *Ibid.*, en el que se cita a https://www.escr-net.org/corporateaccountability/corporatecapture.

[47] Comunicación de Dhakshayini Sooriyakumaran y Brami Jegan.

[48] Mark Akkerman, "Expanding the fortress: the policies, the profiteers and the people shaped by EU's border externalisation programme" (2018).

[49] *Ibid.*, en el que se cita a https://ec.europa.eu/trustfundforafrica/sites/euetfa/files/eutf_2016_annual_report_final_en.pdf.

[50] Véanse https://privacyinternational.org/news-analysis/4290/heres-how-well-connected-securitycompany-quietly-building-mass-biometric y www.afronline.org/?p=42722.

[51] Mirca Madianou, "Technocolonialism: digital innovation and data practices in the humanitarian response to refugee crises, *Social Media + Society* (abril de 2019).

III. Inventario de la discriminación racial y xenófoba en la aplicación de tecnologías digitales en los controles de fronteras y de inmigración

A. Discriminación directa e indirecta

1. Plataformas en línea

20. En las consultas con migrantes, refugiados y apátridas se resaltó que plataformas de medios sociales como Facebook, Twitter y WhatsApp se usaban para difundir el odio racista y xenófobo, y algunos informaron de que habían recibido mensajes personales directos en esas plataformas. En Malasia, por ejemplo, participantes en las consultas denunciaron que a raíz de la pandemia de enfermedad por coronavirus (COVID-19) habían aumentado la apología del racismo y la xenofobia en las plataformas de medios sociales. En algunos casos, los usuarios habían publicado fotografías de migrantes y refugiados que consideraban "ilegales", lo que suscitaba grave inquietud ante la posibilidad de que esas personas sufrieran ataques en el mundo real, además de abusos en línea.

21. En una comunicación se mencionaba a Canary Mission, un sitio web de listas negras administrado anónimamente, que de manera tendenciosa atacaba a estudiantes, profesores y activistas que habían defendido en público los derechos de los palestinos y se centraba de manera desproporcionada en las personas de ascendencia árabe. Según la comunicación, la información publicada en Canary Mission ha sido utilizada por funcionarios de inmigración israelíes en el contexto de la administración y aplicación del control de las fronteras israelíes y las fronteras del territorio palestino ocupado, incluso para denegar la entrada a ellos[52]. Esas prácticas vulneran los derechos de igualdad y no discriminación, así como las protecciones de la libertad de expresión, y las personas cuyos derechos son vulnerados suelen disponer de escasas vías de reparación.

2. Elaboración de perfiles raciales

22. En las consultas con migrantes, refugiados y apátridas también se puso de relieve el papel de las tecnologías digitales en la elaboración de perfiles raciales y étnicos empleados en el control de las fronteras. Los participantes expresaron su preocupación por el empleo de perfiles étnicos de los romaníes en las fronteras de Macedonia del Norte. En 2017, un caso de elaboración de perfiles raciales de romaníes reveló que los funcionarios almacenaban en una lista de vigilancia los datos biométricos de las personas a las que se les impedía cruzar esas fronteras[53]. Se plantearon preocupaciones válidas en el sentido de que ese tipo de listas incluía un número desproporcionadamente elevado de romaníes, de quienes se elaboraban perfiles étnicos; además, los romaníes tenían recursos limitados para impugnar su presencia en esas listas.

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

23. Los Estados están exigiendo cada vez más la recopilación amplia de datos biométricos de los no ciudadanos, y causa preocupación que la reunión y el uso de esos datos constituyan formas directas e indirectas de discriminación por motivos de raza, origen étnico y nacional, ascendencia e incluso religión. Como ya se ha

[52] Comunicación de Palestine Legal.

[53] Véase www.errc.org/uploads/upload_en/file/5209_file1_third-party-intervention-kham-delchevo-and-others-v-north-macedonia-5-february-2020.pdf.

mencionado, en la mayoría de los casos los refugiados, migrantes y apátridas no tienen ningún control sobre la forma en que se comparten los datos obtenidos de ellos. Según una comunicación, la India ha establecido la reunión obligatoria de datos biométricos de los no ciudadanos, datos que se emplean de manera discriminatoria y selectiva en la detención y deportación de personas, incluidos refugiados como los rohinyá[54]. Otra preocupación planteada en el contexto de la India es la utilización de la tarjeta Aadhaar como medio para excluir de facto a los no ciudadanos de los servicios básicos vitales que dependen de sistemas automatizados[55]. Dado que a los refugiados sin permiso de residencia se les prohíbe tener tarjetas Aadhaar, se les discrimina y se les niega el acceso a los servicios básicos y el disfrute de "derechos que aseguren que tengan un refugio digno en la India"[56]. Según esa comunicación, incluso a los niños refugiados se les ha negado el acceso a la enseñanza primaria por no tener la tarjeta Aadhaar[57].

24. En lo que respecta a los apátridas en particular, los participantes en las consultas dijeron que la expansión de los sistemas de identificación digital estaba destruyendo los medios informales de supervivencia que esos grupos habían desarrollado al no contar con la debida documentación y el reconocimiento de los Estados en que residían. Los apátridas, que pertenecen sobre todo a minorías raciales y étnicas, son excluidos sistemáticamente de las bases de datos y no se les entregan documentos de identidad digitales. Los sistemas centralizados de identificación biométrica contradicen de múltiples formas el marco reconocido internacionalmente de la nacionalidad y la ciudadanía. Entre los problemas clave figuran la adopción de decisiones con ayuda de algoritmos y el paso de la adopción de decisiones sobre el estatuto jurídico de las manos de los funcionarios de gobierno a las máquinas o los funcionarios de registros que administran los kits de datos biométricos. Esto puede conllevar una desnaturalización de facto, sin las debidas garantías procesales o salvaguardias. Las mismas consideraciones clave que deben tenerse en cuenta en toda decisión de privación de nacionalidad, como la no discriminación, la evitación de la apatridia, la prohibición de la arbitrariedad, la proporcionalidad, la necesidad y la legalidad[58], también deben estar presentes al examinar la implantación de sistemas centralizados de identificación biométrica. Con la introducción de estructuras de gobernanza digital se corre el riesgo de privar de la nacionalidad por medios indirectos, sin el debido proceso, de manera deliberada o como resultado de sistemas de registro civil incompletos o deficientes[59]. Durante las consultas, participantes de las comunidades nubia y somalí de Kenya y de las comunidades rohinyá, por ejemplo, informaron de que sistemáticamente enfrentaban dificultades para conseguir la identificación digital, lo que luego afectaba su capacidad de acceso al empleo formal y a otros servicios básicos. En algunos casos, los sistemas de identificación digital parecían exacerbar la apatridia pues causaban la exclusión completa y el no reconocimiento de los grupos étnicos minoritarios.

4. Reconocimiento del habla

25. Aunque los sistemas de registro automatizado se implanten con el fin de aumentar la eficiencia burocrática, su tecnología puede producir resultados discriminatorios. Según una comunicación, la Oficina Federal para la Migración y los

[54] Comunicación de Anubhav Dutt Tiwari y Jessica Field.
[55] *Ibid.*
[56] *Ibid.*
[57] *Ibid.*
[58] Institute on Statelessness and Inclusion y otros, Principios sobre la privación de la nacionalidad como medida de seguridad nacional (2020), que pueden consultarse en https://files.institutesi.org/PRINCIPLES_Spanish.pdf.
[59] *Ibid.*, principio 10.

Refugiados de Alemania utiliza TraLitA, un programa de transliteración automática, para registrar los nombres árabes con el alfabeto latino[60]. Sin embargo, el sistema es más propenso a errores al procesar los nombres de solicitantes procedentes de la región del Magreb, en cuyo caso la tasa de registro correcto es del 35 %, frente a una tasa de entre el 85 % y el 90% en el procesamiento de los nombres de solicitantes iraquíes o sirios. Los solicitantes de habla árabe también pueden ser sometidos a un análisis del dialecto al registrarse. La Oficina Federal para la Migración y los Refugiados utiliza programas informáticos para analizar una muestra del habla del solicitante y determinar la verosimilitud del origen nacional declarado. El programa informático se basa en el dialecto levantino del árabe[61], y la comunicación plantea la gran preocupación de que la "susceptibilidad del programa informático a los errores nunca se ha comprobado mediante un control supervisado y especializado y no puede ser comprendida por agentes externos sin acceso a los algoritmos utilizados"[62]. Es evidente que se corre el riesgo de que los hablantes de dialectos árabes no representados en el programa sean considerados erróneamente no creíbles y que, por tanto, se les nieguen las protecciones legales y de otro tipo sobre una base discriminatoria.

5. Extracción de datos móviles e información de medios sociales de los migrantes y refugiados

26. Los gobiernos utilizan cada vez más los dispositivos electrónicos de los migrantes y refugiados como medio de verificar la información que proporcionan a las autoridades fronterizas y de inmigración. Los funcionarios pueden hacerlo porque emplean herramientas de extracción de datos móviles de los teléfonos inteligentes incluidos contactos, datos de llamadas, mensajes de texto, archivos guardados, información de localización y otros[63]. En algunos casos, los funcionarios llegan incluso a privar a los migrantes y refugiados de sus dispositivos personales. En una comunicación se informó de que "las autoridades croatas despojan regularmente a los migrantes interceptados de sus pertenencias, en particular los pasaportes y otras formas de identificación, teléfonos celulares y cargadores portátiles, y los expulsan sumariamente a Bosnia y Herzegovina"[64].

27. En Alemania, Austria, Bélgica, Dinamarca, Noruega y el Reino Unido de Gran Bretaña e Irlanda del Norte, las leyes permiten incautar los teléfonos móviles de los solicitantes de asilo o de trámites migratorios, de los que se extraen datos que luego se utilizan como parte de los procedimientos de asilo[65]. Estas prácticas constituyen una injerencia grave y desproporcionada en el derecho de los migrantes y refugiados a la privacidad, sobre la base de su condición de inmigrantes y, de hecho, de su origen nacional. Por otra parte, es errónea la presunción de que los datos obtenidos de los dispositivos digitales arrojan necesariamente pruebas fiables[66]. Los gobiernos también han recurrido a la inteligencia de los medios sociales, es decir, las técnicas y tecnologías que permiten a las empresas o los gobiernos vigilar los sitios de redes sociales, como Facebook o Twitter[67]. Algunas de estas actividades las realizan directamente los propios funcionarios gubernamentales, pero en algunos casos los

[60] Comunicación de Geselleschaft für Freiheitsrechte.
[61] *Ibid.*
[62] *Ibid.*
[63] *Ibid.*; y comunicación de Privacy International y otros.
[64] Comunicación de Border Violence Monitoring Network.
[65] Comunicación de Privacy International y otros.
[66] Comunicación de Geselleschaft für Freiheitsrechte.
[67] Comunicación de Privacy International y otros.

gobiernos piden a las empresas que les proporcionen las herramientas o los conocimientos técnicos o ambos para realizar esa vigilancia[68].

28. En una comunicación se detallaban las prácticas usuales en Alemania[69]. De conformidad con el artículo 15 de la Ley de Asilo enmendada, los solicitantes de asilo que no puedan presentar un pasaporte válido o un documento equivalente deberán entregar todos los dispositivos portadores de datos —no solo los teléfonos móviles, sino también las computadoras portátiles, las memorias USB e incluso las pulseras inteligentes— junto con la información de acceso a ellos para que la Oficina Federal para la Migración y los Refugiados los "lea" a fin de confirmar su identidad o nacionalidad[70]. La Ley sobre una Mejor Aplicación de la Obligación de Abandonar el País también faculta a la Oficina a compartir los datos con otros organismos gubernamentales, como las autoridades de seguridad y los servicios de inteligencia[71]. Si se determina que es necesario, la lectura de los dispositivos ocurre antes de la audiencia de solicitud de asilo, a petición de la Secretaría de Procedimientos de Asilo y con el consentimiento y la firma del solicitante, aunque en la comunicación se señala que los solicitantes están sometidos "a una presión excepcional para aceptar las peticiones gubernamentales" pues temen a las consecuencias negativas que podrían derivarse de su procedimiento de asilo[72,73]. Esta práctica rutinaria afectó a más de la mitad de todas las personas que solicitaron asilo por primera vez en los últimos dos años[74] y a ciertas nacionalidades más que a otras, lo que suscitó gran preocupación sobre la discriminación de facto por el origen nacional.

29. Esta extracción invasiva de datos de dispositivos personales en Alemania no tiene precedentes y está dirigida únicamente a los solicitantes de asilo; la legalización de esas medidas se basó en supuestos racistas y xenófobos en el discurso político[75]. En la comunicación se destaca además que se ha comprobado que las evaluaciones de los portadores de datos no son idóneas para verificar la identidad o el origen nacional del solicitante de asilo con cierto grado de certeza ni para prevenir el uso indebido de los procedimientos de asilo[76]. Alrededor de una cuarta parte de los intentos de lectura fallan por motivos técnicos; incluso cuando la lectura es satisfactoria, la mayoría de los informes de evaluación son inutilizables porque el conjunto de datos examinados es demasiado pequeño o no es concluyente[77]. De los 21.505 teléfonos móviles cuyos datos se leyeron con éxito en 2018 y 2019, solo unos 118 casos, es decir, el 0,55 %, indicaron una contradicción[78]. Además, como el público no conoce los algoritmos ni los datos de capacitación de los evaluadores, los jueces y otras autoridades decisorias no pueden evaluar correctamente su fiabilidad[79].

30. Aunque disposiciones como el Reglamento General de Protección de Datos de la Unión Europea tratan de proteger los datos y la privacidad, algunos Estados establecen excepciones en la aplicación de las leyes de inmigración. En dos comunicaciones se señalaron las excepciones a la aplicación del Reglamento General de Protección de Datos recogidas en la Ley de Protección de Datos de 2018 del Reino

[68] *Ibid.*
[69] Comunicación de Geselleschaft für Freiheitsrechte.
[70] *Ibid.*
[71] *Ibid.*
[72] *Ibid.*
[73] *Ibid.*
[74] *Ibid.*
[75] *Ibid.*
[76] *Ibid.*
[77] *Ibid.*
[78] *Ibid.*
[79] *Ibid.*

Unido[80]. En virtud de una “excepción por motivos de inmigración”, la entidad facultada para procesar datos, conocida como “controlador de datos”, puede eludir su obligación de respetar los derechos fundamentales de una persona en relación con el acceso a los datos si de no hacerlo “se perjudica el control efectivo de la inmigración”[81]. Esos derechos incluyen el derecho de una persona a poner objeciones al procesamiento de sus propios datos y a limitarlo y el derecho a que se supriman sus datos personales[82]. La excepción también libera a los responsables de los datos de su responsabilidad de informar a las personas interesadas cuando se obtienen datos de otras fuentes, como una escuela, un empleador o una autoridad local[83]. En el Reino Unido, la Ley de Policía enmendada faculta no solo a la policía sino también a los funcionarios de inmigración a examinar los teléfonos móviles y otros dispositivos electrónicos de los solicitantes de asilo[84]. La Ley sobre Delincuencia y Tribunales de 2013 del Reino Unido va más allá incluso de la evaluación de los portadores de datos permitida en Alemania, pues permite a la policía y los funcionarios de inmigración realizar operaciones de vigilancia secreta, colocar dispositivos de escucha y piratear y registrar teléfonos móviles y computadoras[85]. Las personas afectadas por esas prácticas serán objeto de una atención desproporcionada por motivos de origen nacional, aunque el origen nacional no debería servir nunca como base para disminuir el derecho a la privacidad y otros derechos.

B. Estereotipos discriminatorios

31. En su informe al Consejo de Derechos Humanos, la Relatora Especial ofreció ejemplos de la forma en que el diseño y la utilización de diferentes tecnologías digitales emergentes podían combinarse de forma deliberada e involuntaria y generar estructuras discriminatorias desde el punto de vista racial, que de manera holística o sistemática socavaban el disfrute de los derechos humanos de determinados grupos por motivos de raza u origen étnico o nacional, en combinación con otras características. La Relatora instó a que, en lugar de considerar únicamente que las nuevas tecnologías digitales podían afectar el acceso y el disfrute de determinados derechos humanos, se entendiera que también podían crear y mantener la exclusión racial y étnica en términos sistémicos o estructurales. En esta subsección, la Relatora Especial destaca las formas en que los migrantes, los refugiados, los apátridas y los grupos conexos están siendo objeto de intervenciones tecnológicas que los exponen a una amplia gama de violaciones reales y potenciales de sus derechos sobre la base de su origen nacional o de su condición, real o presunta, de inmigrantes.

1. Humanitarismo de vigilancia y vigilancia en el proceso de asilo

32. Los analistas han advertido del aumento del “humanitarismo de vigilancia”[86], según el cual una mayor dependencia de las tecnologías digitales en la prestación de servicios y en otros procesos burocráticos tiene como resultado no intencionado que los refugiados y los solicitantes de asilo se ven privados de acceso a servicios que atiendan sus necesidades básicas esenciales, como los alimentos[87]. El humanitarismo

[80] *Ibid.*; y comunicación de la Plataforma para la Cooperación Internacional para Inmigrantes Indocumentados.
[81] Comunicación de la Plataforma para la Cooperación Internacional para Inmigrantes Indocumentados.
[82] *Ibid.*
[83] *Ibid.*
[84] Comunicación de Geselleschaft für Freiheitsrechte.
[85] *Ibid.*
[86] Véase www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.
[87] Comunicación de Ana Beduschi.

acompañado de prácticas de vigilancia se refiere al despliegue de “sistemas de reunión de enormes cantidades de datos por las organizaciones de ayuda que, involuntariamente, aumentan la vulnerabilidad de las personas necesitadas en situación de emergencia”[88]. Incluso un nombre mal escrito puede crear un “caos burocrático” y dar lugar a acusaciones de proporcionar información falsa, retrasando el proceso de asilo, que ya de por sí es lento[89]. Suele estar latente la posibilidad de que se afecte la privacidad de los datos y que ello incluso cause violencia en las zonas de conflicto, donde el acceso no autorizado a los datos o su filtración a una facción beligerante podrían dar lugar a represalias contra quienes sean considerados partidarios de la otra parte en el conflicto[90].

33. A este respecto, en una comunicación se destacan los peligros que entraña que la Oficina del Alto Comisionado de las Naciones Unidas para los Refugiados (ACNUR) utilice cada vez más las tecnologías digitales para gestionar la distribución de la ayuda[91]. En los campamentos de refugiados del Afganistán, el ACNUR estableció el registro mediante el escaneo del iris de los refugiados afganos que regresaban como requisito previo para recibir asistencia[92]. Aunque el ACNUR justifica la recopilación, digitalización y almacenamiento de las imágenes del iris de los refugiados en el Sistema Biométrico de Gestión de la Identidad como medio para detectar y prevenir el fraude[93], los efectos del procesamiento de esos datos sensibles pueden ser graves cuando los sistemas son deficientes o se utilizan indebidamente[94]. También se ha documentado que esos instrumentos de vigilancia biométrica han provocado una aversión al sistema y la pérdida de acceso a bienes y servicios necesarios para la supervivencia[95]. En esa comunicación se señalaban, por ejemplo, los fallos de la tecnología en los campamentos de refugiados rohinyá en Bangladesh, que provocaron la denegación de raciones de alimentos a los refugiados[96].

34. La reunión de enormes cantidades de datos sobre migrantes y refugiados crea graves problemas y posiblemente produce violaciones de los derechos humanos relacionados con el intercambio de datos y el acceso a ellos, sobre todo en lugares como los campamentos de refugiados, donde las diferencias de poder entre los organismos de las Naciones Unidas, las organizaciones no gubernamentales internacionales y las comunidades afectadas ya son muy marcadas. Aunque se suele plantear que compartir datos sobre las crisis humanitarias o identificar mediante datos biométricos constituyen formas de aumentar la eficiencia y la cooperación entre instituciones y entre Estados, los beneficios que reporta la reunión de datos no son iguales para todos. La reunión de datos y el uso de nuevas tecnologías, especialmente en contextos caracterizados por grandes diferencias de poder, plantean problemas relacionados con el consentimiento informado y la posibilidad de optar por no aportar datos. En diversos contextos de migración forzosa y ayuda humanitaria, como en Mafraq (Jordania), se están utilizando tecnologías biométricas como el escaneo del iris, en lugar de tarjetas de identidad, para entregar raciones de alimentos[97]. Sin

[88] Véase www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.
[89] Mark Latonero y otros, “Digital identity in the migration and refugee context: Italy case study” (Data & Society, abril de 2019).
[90] Véase www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.
[91] Comunicación de Amnistía Internacional.
[92] *Ibid.*
[93] *Ibid.*
[94] *Ibid.*, en el que se cita a A/HRC/39/29.
[95] Comunicación de Amnistía Internacional.
[96] *Ibid.*
[97] Fleur Johns, “Data, detection, and the redistribution of the sensible in international law”, *American Journal of International Law*, vol. 111, núm. 1 (2017). Véase también https://medium.com/unhcr-innovation-service/managing-risk-to-innovate-in-unhcr-91fe9294755b.

embargo, condicionar el acceso a los alimentos a la reunión de datos supone que los refugiados quedan sin posibilidad de elección o sin autonomía, pues no se puede dar el consentimiento libremente cuando la alternativa es la inanición. De hecho, una investigación realizada en el campo de refugiados de Azraq[98] reveló que la mayoría de los refugiados entrevistados se sentían incómodos con tales experimentos tecnológicos, pero sentían que no podían negarse si querían comer. El objetivo o la promesa de mejorar la prestación de servicios no puede justificar los niveles de coerción implícita que subyacen a regímenes como este[99].

35. En las consultas se puso de relieve la preocupación de los refugiados rohinyá en Bangladesh y la India de que sus datos se compartieran de manera tal que aumentara su riesgo de devolución, o se compartieran con el Gobierno de Myanmar, lo que aumentaría su vulnerabilidad a las violaciones de los derechos humanos en caso de devolución o de otras formas de retorno de esos grupos a su país de origen. En este contexto causa profunda inquietud la "deriva funcional", práctica que supone que los datos reunidos en un contexto (por ejemplo, en la vigilancia de los fraudes de bajo nivel) se comparten y se reutilizan con propósitos diferentes (por ejemplo, para añadirlos a registros de posibles sospechosos de terrorismo), sin que existan protecciones procesales y sustantivas que amparen a las personas cuyos datos se comparten y reutilizan[100].

36. En algunos casos, la propia naturaleza de la reunión de datos puede arrojar resultados profundamente discriminatorios. Desde agosto de 2017, más de 742.000 refugiados apátridas rohinyá han cruzado a Bangladesh huyendo del genocidio en Myanmar[101]. El sistema de registro del ACNUR y el Gobierno de Bangladesh no ofrecía el término "rohinyá" como una opción de identidad étnica; en cambio, se utilizaba el término "nacionales de Myanmar". Este es un término que Myanmar no reconoce y que no capta la realidad de que los rohinyá son apátridas porque se les ha privado arbitrariamente de su derecho a la nacionalidad de Myanmar[102]. Como señala una de las comunicaciones, la categorización mediante un término irreconocible en las tarjetas de identidad que deben portar y utilizar los rohinyá equivale a una forma de "aniquilación simbólica"[103].

37. La exclusión de los refugiados y los solicitantes de asilo de los servicios básicos esenciales mediante sistemas de tecnología digital también se produce fuera de los campamentos de refugiados. En una comunicación se presenta el ejemplo de Alemania, donde, en virtud de la Ley de Prestaciones a los Solicitantes de Asilo, las personas indocumentadas tienen el mismo derecho a la atención médica que los solicitantes de asilo[104]. Sin embargo, la oficina de bienestar social que administra la atención médica de los indocumentados está obligada a comunicar sus datos personales a las autoridades de inmigración en virtud del artículo 87 de la Ley de Residencia, que rige la "transferencia de datos e información a las autoridades extranjeras" por parte de todas las autoridades públicas[105]. Esto significa que el acceso legal a la atención médica puede dar lugar a la aplicación de controles de inmigración,

[98] Véase www.irinnews.org/analysis/2016/05/18/eye-spy-biometric-aid-system-trials-jordan.

[99] Véanse www.unhcr.org/innovation/wp-content/uploads/2020/04/Space-and-imagination-rethinking-refugees%E2%80%99-digital-access_WEB042020.pdf; y Dragana Kaurin, "Data protection and digital agency for refugees".

[100] Comunicación de Mirca Madianou.

[101] Véase www.acnur.org/emergencia-rohingyas.html.

[102] Mirca Madianou, "Technocolonialism: digital innovation and data practices in the humanitarian response to refugee crises".

[103] Comunicación de Mirca Madianou.

[104] Comunicación de la Plataforma para la Cooperación Internacional para Inmigrantes Indocumentados.

[105] *Ibid.*

lo que probablemente inhiba el uso de servicios de atención médica, incluso de emergencia, por los migrantes y refugiados.

2. Experimentación tecnológica

38. En las comunicaciones recibidas para la elaboración del presente informe se plantea una gran preocupación por la experimentación tecnológica que de manera generalizada practican los agentes estatales y no estatales con los refugiados, los migrantes y los apátridas. Esta experimentación consiste en ensayos de diversos productos tecnológicos en circunstancias en que los grupos destinatarios tienen medios limitados para dar su consentimiento informado, o carecen de ellos, y en que las consecuencias de dichos ensayos y experimentos para los derechos humanos son negativas o desconocidas. Por lo general, los refugiados, los migrantes y los apátridas tienen muy poco o ningún recurso para impugnar esa experimentación tecnológica y las posibles violaciones de los derechos humanos conexas. Además, el origen nacional y la situación migratoria o de ciudadanía es lo que expone a los refugiados, migrantes y apátridas a esos experimentos, lo que plantea serias preocupaciones sobre la presencia de estructuras de vulnerabilidad discriminatorias.

39. En una comunicación se destacó el sistema iBorderCtrl (sistema inteligente portátil de control fronterizo), que forma parte del programa Horizonte 2020 de la Unión Europea y que "tiene por objeto facilitar un control fronterizo más rápido y riguroso de los nacionales de terceros países que cruzan las fronteras terrestres de los Estados miembros de la Unión Europea"[106]. El sistema iBorderCtrl utiliza equipo y programas informáticos con tecnologías que procuran automatizar la vigilancia de las fronteras[107] y, entre otras funciones, realiza la detección automática de mentiras[108]. La Unión Europea ha puesto a prueba este detector de mentiras en aeropuertos de Grecia, Hungría y Letonia[109]. Según se ha informado, en 2019 se hizo una prueba del iBorderCtrl en la frontera serbo-húngara, que resultó fallida[110]. Este sistema ilustra la tendencia de experimentar las tecnologías de vigilancia y de otro tipo con los solicitantes de asilo, con arreglo a premisas científicamente dudosas[111]. El sistema iBorderCtrl, que se sustenta en la controvertida teoría de la "ciencia del reconocimiento de la expresión emocional", sustituye a los guardias de fronteras por un sistema de reconocimiento facial que busca anomalías faciales al escanear el rostro del viajero mientras responde a una serie de preguntas[112]. Otros países, como Nueva Zelandia, también están experimentando con la tecnología de reconocimiento facial automatizado para identificar a futuros "agitadores", lo que ha llevado a organizaciones de la sociedad civil a presentar demandas judiciales por motivos de discriminación y uso de perfiles raciales[113].

40. Los Estados experimentan actualmente con la automatización de diversos aspectos de la toma de decisiones en materia de inmigración y asilo. Por ejemplo, desde por lo menos 2014, el Canadá ha utilizado alguna forma de adopción de

[106] Comunicación de Privacy International y otros.

[107] Para obtener información general sobre el proyecto, véase Comisión Europea, "Smart lie-detection system to tighten the EU's busy borders" (24 de octubre de 2018), que puede consultarse en https://ec.europa.eu/research/infocentre/article_en.cfm?artid=49726.

[108] Comunicación de Privacy International y otros.

[109] Comunicación de Maat for Peace, Development and Human Rights. Véase también Petra Molnar, "Technology on the margins: AI and global migration management from a human rights perspective" (2019); y comunicación de Minority Rights Group International.

[110] Comunicación de Privacy International y otros.

[111] *Ibid.*

[112] Comunicación de Minority Rights Group International.

[113] Véase www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12026585.

decisiones automatizada en su sistema de inmigración y refugiados[114]. En un informe de la Universidad de Toronto de 2018 se examinaron los riesgos que entrañaba para los derechos humanos el uso de la inteligencia artificial para remplazar o ampliar las decisiones en materia de inmigración y se señaló que esos procesos constituían un laboratorio donde se realizaban experimentos de alto riesgo dentro de un sistema que de por sí era muy discrecional y poco transparente[115]. La adopción de decisiones automatizada tenía ramificaciones de gran alcance en el contexto de la inmigración y los refugiados. Aunque el Gobierno del Canadá ha confirmado que este tipo de tecnología se emplea únicamente para intensificar la adopción de decisiones por seres humanos y se reserva solo para determinadas solicitudes de inmigración, no existe ningún mecanismo jurídico que proteja los derechos procesales de los no ciudadanos e impida que se produzcan abusos de los derechos humanos. En el Reino Unido ya se utilizan algoritmos similares para la concesión de visados, lo que ha sido impugnado en los tribunales debido a su potencial discriminatorio[116]. El Canadá, el Reino Unido y Suiza también utilizan la adopción de decisiones automatizada o basada en algoritmos "para la selección y el reasentamiento de refugiados"[117]. La introducción de nuevas tecnologías repercute tanto en los procesos como en los resultados asociados a las decisiones que, de otro modo, adoptarían los tribunales administrativos, funcionarios de inmigración, agentes de fronteras, analistas jurídicos y otros funcionarios encargados de administrar los sistemas de inmigración y de refugiados, aplicar las leyes relativas a las fronteras y gestionar la respuesta a los refugiados. Hay una grave falta de claridad en cuanto a la forma en que los tribunales interpretarán los principios de derecho administrativo, como la justicia natural, la equidad procesal y las normas de revisión cuando se trate de un sistema de toma de decisiones automatizado o un uso poco transparente de la tecnología.

41. En algunos contextos, se practican experimentos tecnológicos al reunir datos genéticos, con fines que se justifican por motivos poco convincentes, pero que plantean preocupaciones serias y concretas en materia de derechos humanos. En una comunicación se describía el Sistema Combinado de Índices de ADN (CODIS), una base de datos genéticos forenses de los Estados Unidos mediante la cual los distintos estados y el Gobierno federal reúnen, almacenan y comparten información genética[118]. Desde enero de 2020, el Gobierno federal ha venido reuniendo datos del ADN de todas las personas detenidas por motivos migratorios[119]. Esto significa que "por primera vez, el CODIS almacenará, con fines de detección de delitos, los datos genéticos de personas que no han sido acusadas de ningún delito", lo cual elimina el requisito establecido desde hace mucho tiempo de que la recogida de ADN debe ir precedida de una conducta delictiva previa[120]. Los no ciudadanos que se encuentran detenidos por motivos migratorios por regla general no son delincuentes[121]. De hecho, la gran mayoría de las infracciones de inmigración por las que se detiene a un inmigrante son de carácter civil[122]. En lo que respecta a los solicitantes de asilo, que

[114] Petra Molnar y Lex Gill, "Bots at the gate: a human rights analysis of automated decision-making in Canada's immigration and refugee system", Citizen Lab and International Human Rights Program, Facultad de Derecho, Universidad de Toronto, informe de investigación núm. 114 (septiembre de 2018).

[115] *Ibid.*

[116] Véase www.foxglove.org.uk/news/home-office-says-it-will-abandon-its-racist-visa-algorithm-nbsp-after-we-sued-them.

[117] Comunicación de Maat for Peace, Development and Human Rights; y comunicación de Ana Beduschi, en la que cita a Petra Molnar y Lex Gill, "Bots at the gate: a human rights analysis of automated decision-making in Canada's immigration and refugee system".

[118] Comunicación de Daniel I. Morales, Natalie Ram y Jessica L. Roberts.

[119] *Ibid.*

[120] *Ibid.*

[121] *Ibid.*

[122] *Ibid.*

constituyen una proporción cada vez mayor de los no ciudadanos detenidos, tanto las leyes internacionales como las nacionales permiten expresamente que entren en los Estados Unidos para reclamar el derecho de refugio[123]. En la comunicación se señala acertadamente que la nueva política de inmigración que amplía el CODIS orienta a los Estados Unidos hacia la construcción de un "edificio panóptico genético", cuyos propósitos y efectos bien pueden ser discriminatorios. Se corre el riesgo de que el CODIS se convierta en una herramienta distópica de vigilancia genética que incluirá "a toda persona que se encuentre dentro de las fronteras de los Estados Unidos, entre ellas estadounidenses comunes y corrientes que no hayan sido condenados ni sean siquiera sospechosos de conducta delictiva", lo que supone una amenaza para la democracia y los derechos humanos[124], en particular sobre la base del origen nacional.

42. Dado que la COVID-19 ha alentado y legitimado aún más la vigilancia y el uso de otras tecnologías dirigidas a los refugiados y migrantes, estos grupos han sido objeto de una mayor experimentación[125]. Un ejemplo de ello es la implantación en África Occidental, a título experimental, de un pasaporte de inmunidad denominado "COVI-Pass"[126]. Esta iniciativa digital, producto de la asociación entre Mastercard y la Alianza Gavi, una alianza público-privada para el fomento de la vacunación, combina datos biométricos, la localización de contactos, los pagos sin dinero en efectivo, la identificación nacional y la aplicación de la ley[127]. Las tecnologías de ese tipo no solo funcionan al margen de las evaluaciones de los efectos y los reglamentos en materia de derechos humanos; también es posible que pongan en peligro el ejercicio de determinados derechos humanos, como la libertad de circulación, el derecho a la privacidad, el derecho a la autonomía física y el derecho a la igualdad y la no discriminación, especialmente en el caso de los refugiados y los migrantes[128].

3. Externalización de las fronteras

43. La externalización de las fronteras, es decir, el desplazamiento de las fronteras nacionales y regionales fuera del territorio correspondiente, hacia otras regiones geográficas, a fin de evitar la llegada de migrantes y refugiados, se ha convertido en un instrumento habitual de aplicación de la ley en las fronteras de muchos países y regiones. Las violaciones de los derechos humanos asociadas a la externalización de las fronteras están bien documentadas[129]. La externalización de las fronteras no afecta por igual a todas las nacionalidades o grupos de origen nacional. Esta práctica tiene efectos desproporcionados en las personas de África, América Central y del Sur y Asia Meridional, y en muchas regiones se ve impulsada por políticas de cariz racial, xenófobo y etnonacionalista que tratan de excluir a ciertos grupos nacionales y étnicos de determinadas regiones sobre bases discriminatorias. Los Estados y los bloques regionales han venido recurriendo cada vez más a las tecnologías digitales para llevar a la práctica la externalización de las fronteras, consolidando y ampliando así los regímenes discriminatorios y excluyentes.

44. En una comunicación se destacó el Sistema Europeo de Vigilancia de Fronteras (EUROSUR), un programa que utiliza tecnologías de macrodatos para predecir, controlar y vigilar el tráfico a través de las fronteras exteriores de la Unión Europea[130].

---

[123] *Ibid.*
[124] *Ibid.*
[125] Comunicación de Amnistía Internacional.
[126] *Ibid.*
[127] *Ibid.*
[128] *Ibid.*
[129] Véanse, por ejemplo, A/HRC/23/46, A/HRC/29/36 y A/72/335.
[130] Comunicación de Maat for Peace, Development and Human Rights, en la que se cita a 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).

El sistema despliega drones en el mar Mediterráneo con el fin de notificar a la guardia costera de Libia para que intercepte embarcaciones de refugiados y migrantes y devuelva a los migrantes a ese país[131]. Aunque la Comisión Europea insiste en que los drones solo se usan con fines de vigilancia civil[132], la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos se ha pronunciado en contra de los rechazos coordinados de migrantes y refugiados y la negativa a prestarles asistencia en el Mediterráneo, que lo convierte en una de las rutas migratorias más mortales del mundo[133]. Las tecnologías de vigilancia son esenciales para la coordinación en ese contexto.

45. En otra comunicación se informó de que 13 naciones europeas participaban en el proyecto ROBORDER, un "sistema de vigilancia de fronteras totalmente funcional y autónomo"[134], que consiste en robots móviles no pilotados capaces de funcionar de forma autónoma o en enjambres en diversos entornos: aéreos, acuáticos, submarinos y terrestres[135]. Esta propuesta de aumentar el uso de vehículos aéreos no pilotados para vigilar las fronteras de Europa intensifica la descentralización de las zonas fronterizas en varias capas de vigilancia verticales y horizontales, suspende el poder del Estado en el espacio aéreo, y extiende la frontera visual y virtualmente, convirtiendo a las personas en objetos de seguridad y puntos de datos que deben analizarse, almacenarse, reunirse y hacerse inteligibles[136]. El uso de tecnologías autónomas militares o cuasimilitares también refuerza la conexión entre la inmigración, la seguridad nacional y el impulso creciente hacia la penalización de la migración y el uso de taxonomías basadas en el riesgo para definir y señalar los casos[137]. A nivel mundial, los Estados, en particular los que tienen fronteras a las que arriba un gran número de migrantes, han venido utilizando diversos medios para adelantarse a quienes tratan de solicitar asilo legalmente y disuadirlos. Este tipo de política de disuasión es palpable en España, Grecia e Italia[138], países que se encuentran en las fronteras geográficas exteriores de Europa y que recurren cada vez más a políticas de disuasión violenta y de "rechazo".

46. En una comunicación se destacó que Croacia empleaba tecnologías financiadas por la Unión Europea para detectar, aprehender y devolver a los refugiados y migrantes que viajaban por la ruta de los Balcanes, desde Bosnia y Herzegovina y Serbia a través de Croacia para llegar a las fronteras de la zona Schengen[139]. En esa comunicación se alegan cientos de abusos de los derechos humanos ocurridos en los últimos tres años, entre ellos "rechazos ilegales" que reflejan "divisiones inherentemente racistas"[140]. Las tecnologías de vigilancia, como los drones y los helicópteros con reflectores automatizados "se han convertido en armas contra las

[131] Comunicación de Familia Franciscana Internacional, en la que se cita a www.middleeastmonitor.com/20190819-eu-using-israel-drones-to-track-migrant-boats-in-the-med/.

[132] Comunicación de Familia Franciscana Internacional, en la que se cita a www.europarl.europa.eu/doceo/document/E-9-2019-003257-ASW_EN.pdf.

[133] Véase https://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=25875&LangID=S.

[134] Comunicación de Homo Digitalis. Véase también https://roborder.eu/. Los Estados participantes son Alemania, Bélgica, Bulgaria, España, Estonia, Finlandia, Grecia, Hungría, Italia, Portugal, el Reino Unido de Gran Bretaña e Irlanda del Norte, Rumania y Suiza.

[135] *Ibid.*

[136] Raluca Csernatoni, "Constructing the EU's high-tech borders: Frontex and dual-use drones for border management".

[137] Comunicación de Dimitri van den Meerssche.

[138] Véanse 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/ y www.efadrones.org/countries/italy/.

[139] Comunicación de Border Violence Monitoring Network.

[140] *Ibid.*

personas en movimiento, facilitan su detección y agravan su vulnerabilidad y los peligros a los que se enfrentan”[141].

47. La externalización discriminatoria de las fronteras también se logra mediante programas transnacionales de intercambio de datos biométricos entre múltiples países. En una comunicación se informó de un programa de intercambio de datos biométricos establecido por los Gobiernos de México y los Estados Unidos[142]. Hasta agosto de 2018, México había desplegado el programa financiado por los Estados Unidos en sus 52 puestos de procesamiento de migrantes[143]. Este programa bilateral utiliza datos biométricos para examinar a los migrantes detenidos en México que presuntamente han tratado de cruzar la frontera de los Estados Unidos o pertenecen a una banda delictiva[144]. Sin embargo, cuando recibió solicitudes de acceso a la información, el Instituto Nacional de Migración de México negó haber procesado datos biométricos de esa forma[145].

4. Vigilancia de la inmigración[146]

48. En una comunicación se informó de que en la frontera entre los Estados Unidos y México se estaba construyendo “una red de 55 torres equipadas con cámaras, sensores termográficos, sensores de movimiento, sistemas de radar y un sistema de GPS”[147]. Este sistema de vigilancia fronteriza también vigila la reserva de la nación tohono o’odham, situada en Arizona a un kilómetro y medio de la frontera aproximadamente[148]. Este sistema “inteligente” de vigilancia sustituye a otro anterior, que, según estudios realizados, no había logrado impedir el cruce de la frontera sin documentos, sino que había desviado las rutas de migración, aumentando así la vulnerabilidad de los migrantes a las lesiones, el aislamiento, la deshidratación, la hipertermia y el agotamiento, así como el número de muertes[149]. En otra comunicación se señala que los investigadores y las organizaciones de la sociedad civil se han opuesto a esas tecnologías fronterizas porque “exacerbarían la desigualdad racial y étnica en la vigilancia policial y la aplicación de la ley en materia de inmigración, además de limitar la libertad de expresión y el derecho a la privacidad”[150]. En otras comunicaciones también se destacó que estaba en funcionamiento otra infraestructura autónoma de inteligencia artificial de vigilancia en la frontera entre los Estados Unidos y México, que incluía drones concebidos para detectar la presencia humana y alertar a los agentes de control fronterizo[151]. El Comité para la Eliminación de la Discriminación Racial ha expresado su preocupación a la Asamblea General por “los viajes cada vez más precarios que hacen los solicitantes de asilo, los refugiados y los migrantes en busca de seguridad y dignidad, lo que causa

[141] *Ibid.*
[142] Comunicación de Privacy International y otros.
[143] *Ibid.*
[144] *Ibid.*
[145] *Ibid.*
[146] Anil Kalhan, “Immigration surveillance”, *Maryland Law Review*, vol. 74, núm. 1 (2014) (en que se define la vigilancia de la inmigración como el producto de una ampliación espectacular de la identificación, el seguimiento y el control de la movilidad y el intercambio de información, así como de la evasión de las protecciones jurídicas sustantivas y procesales tradicionales en las que se ha confiado habitualmente para proteger a los no ciudadanos de diversos abusos de los derechos humanos).
[147] Comunicación de Campaign to Stop Killer Robots.
[148] *Ibid.*
[149] Samuel Norton Chambers y otros, “Mortality, surveillance and the tertiary ‘funnel effect’ on the U.S.-Mexico border: a geospatial modeling of the geography of deterrence”.
[150] Comunicación de Minority Rights Group International.
[151] Comunicación de Mijente y comunicación de Iván Chaar-López.

muertes y sufrimientos innecesarios”[152],[153]. Como ya se ha mencionado, hay pruebas de que la llamada tecnología de “fronteras inteligentes” obliga a los migrantes a emprender esos viajes cada vez más precarios, lo que tiene efectos desproporcionados en grupos de determinado origen nacional, étnico y racial.

49. En los Estados Unidos se vigilan las comunicaciones de los inmigrantes detenidos con sus familiares y amigos[154]. El modelo comercial de las empresas proveedoras de la tecnología consiste en ofrecer a los inmigrantes detenidos y sus familiares “comodidad en forma de llamadas, videoconferencias, mensajes de correo de voz, intercambio de fotografías y mensajes de texto, mientras que sus verdaderos clientes”, los funcionarios de inmigración, obtienen datos de los usuarios[155]. El programa informático de vigilancia basado en la web, que se ofrece de manera gratuita a los funcionarios gubernamentales con cada instalación, “incluye análisis de patrones de llamadas, análisis de relaciones y herramientas de visualización de datos”[156].

50. Otra faceta de la vigilancia de inmigración es el análisis de los medios sociales. Desde abril de 2019, el Departamento de Estado de los Estados Unidos exige a los solicitantes de visado que revelen información sobre sus cuentas en los medios sociales durante los últimos cinco años previos a la fecha de solicitud[157]. En septiembre de 2019, el Departamento de Seguridad Nacional propuso obligar a revelar esa información a los no ciudadanos que ya estuvieran presentes e incluso residieran en el país y que solicitaran hacer trámites de inmigración, por ejemplo de naturalización, residencia permanente y asilo[158]. Como se pone de relieve en la comunicación, este enfoque amplio de la verificación de antecedentes en los medios sociales es especialmente preocupante debido a que se ha demostrado que las autoridades de inmigración estadounidenses ya han utilizado la información de los medios sociales de una manera que perjudica desproporcionadamente a los miembros de grupos raciales, étnicos y religiosos minoritarios[159]. El Departamento de Seguridad Nacional ha acusado falsamente a jóvenes negros y latinos de pertenecer a pandillas y ha utilizado sus conexiones en los medios sociales como base para su detención o deportación o para denegar sus solicitudes de trámites migratorios[160]. El Servicio de Inmigración y Control de Aduanas de los Estados Unidos, organismo que forma parte del Departamento de Seguridad Nacional, rastrea con frecuencia los medios sociales para obtener información que apoye las acusaciones de pertenencia a pandillas[161]. En una ocasión, el Departamento de Seguridad Nacional ofreció como prueba de su alegación una foto publicada en Facebook de un joven inmigrante con una gorra de los Chicago Bulls. El tribunal de inmigración le denegó la fianza y rechazó tanto su solicitud de asilo como la de residencia permanente, deportándolo a un país en el que temía por su vida[162], en contravención de las prohibiciones de no devolución previstas en el derecho internacional.

51. Además, el escrutinio de los medios sociales ha agravado el riesgo desproporcionado que corren las personas de fe musulmana o de ascendencia árabe,

[152] Comunicación de Familia Franciscana Internacional.
[153] Véase A/72/18.
[154] Comunicación de Mijente, en la que se cita a www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.
[155] *Ibid.*
[156] *Ibid.*
[157] Comunicación de Harvard Immigration and Refugee Clinical Program.
[158] *Ibid.*, en la que se cita a www.govinfo.gov/content/pkg/FR-2019-09-04/pdf/2019-19021.pdf.
[159] Comunicación de Harvard Immigration and Refugee Clinical Program.
[160] *Ibid.*, en que se cita a www.ilrc.org/sites/default/files/resources/deport_by_any_means_nec-20180521.pdf.
[161] Comunicación de Harvard Immigration and Refugee Clinical Program.
[162] *Ibid.*

real o presunta, pues “crea una infraestructura plagada de inferencias erróneas y de culpabilidad por asociación”[163]. Por ejemplo, en 2019, la Oficina de Aduanas y Protección Fronteriza de los Estados Unidos, otro organismo bajo la égida del Departamento de Seguridad Nacional, denegó a un estudiante universitario palestino la entrada en el país basándose en las publicaciones de sus amigos en Facebook, en las que expresaban sus opiniones políticas contra los Estados Unidos, aunque él no había publicado sus propias opiniones[164]. Además de las obligaciones directas que imponen a los no ciudadanos, los requisitos ampliados que los obligan a proporcionar al Gobierno de los Estados Unidos información sobre los medios sociales probablemente afecten a las libertades de expresión y asociación de esas personas.

52. La Oficina de Investigaciones de Seguridad Nacional, que es el órgano de investigaciones del Servicio de Inmigración y Control de Aduanas de los Estados Unidos, ya había ensayado la elaboración automatizada de perfiles en los medios sociales en 2016[165], lo que había reforzado su capacidad de utilizar los medios sociales de código abierto para verificar los antecedentes de los solicitantes y titulares de visados antes y después de su llegada a los Estados Unidos[166]. En las comunicaciones también se plantearon inquietudes acerca del examen por el Gobierno de los Estados Unidos de tecnologías cuyo objetivo era “determinar mediante medios automatizados” si era probable que una persona que solicitaba o tenía un visado de los Estados Unidos se convertiría en un “miembro que contribuiría de manera positiva a la sociedad” o si tenía la intención de “cometer delitos o atentados terroristas”[167]. En una comunicación se señaló en particular que los Estados Unidos empleaban instrumentos de evaluación de riesgos para adoptar decisiones sobre la detención de inmigrantes, incluido uno que utilizaba un algoritmo establecido para recomendar siempre la detención del inmigrante, independientemente de sus antecedentes penales[168]. Este es un ejemplo de cómo la tecnología ha sido adaptada para aplicar medidas punitivas en materia de inmigración basadas en la visión racista, xenófoba y etnonacionalista de la inmigración que ha sido promovida por el Gobierno del Presidente Donald Trump.

53. Todo ello apunta a una tendencia en la vigilancia de la inmigración según la cual los modelos predictivos utilizan la inteligencia artificial para predecir si las personas que no tienen vínculos con una actividad delictiva cometerán delitos en el futuro. Sin embargo, estos modelos predictivos son propensos a crear y reproducir bucles de retroalimentación racialmente discriminatorios[169]. Además, el sesgo racial ya está presente en los conjuntos de datos en los que se basan estos modelos[170]. Cuando los conjuntos de datos discriminatorios se consideran aportaciones neutrales, dan lugar a modelos de delincuencia incorrectos que “perpetúan la desigualdad racial y contribuyen a la selección y el control excesivo de los no ciudadanos”[171].

[163] *Ibid.*
[164] *Ibid.*
[165] Comunicación de Mijente, en la que se cita a 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 (2019).
[166] Comunicación de Mijente, en la que se cita a www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.
[167] *Ibid.*
[168] Comunicación de Minority Rights Group International.
[169] Comunicación de Mijente.
[170] *Ibid.*
[171] *Ibid.*

IV. Recomendaciones

54. **En su informe al Consejo de Derechos Humanos, la Relatora Especial presentó a los Estados un enfoque estructural e intersectorial basado en el derecho de los derechos humanos en relación con la discriminación racial en el diseño y la utilización de las nuevas tecnologías digitales. En el informe se explicaban las obligaciones internacionales de derechos humanos aplicables y se destacaban:**

a) El alcance de la discriminación racial prohibida legalmente, pero presente en el diseño y la utilización de las nuevas tecnologías digitales;

b) La obligación de prevenir y combatir la discriminación racial en el diseño y la utilización de las nuevas tecnologías digitales;

c) La obligación de ofrecer vías de recurso efectivo ante la discriminación racial en el diseño y la utilización de las nuevas tecnologías digitales.

55. **La Relatora Especial explicó los conceptos y doctrinas de la discriminación racial directa, indirecta y estructural recogidos en las normas internacionales de derechos humanos y resumió las obligaciones que estas imponían a los Estados con respecto a las nuevas tecnologías digitales. Señaló que esas obligaciones también tenían repercusiones para los agentes no estatales, incluidas las empresas, que en muchos aspectos ejercían más control sobre esas tecnologías que los propios Estados. La Relatora reitera el análisis y las recomendaciones de ese informe e insta a los Estados a que los examinen junto con las recomendaciones que formula en el presente informe, que se centran en el cumplimiento de las obligaciones en materia de derechos a la igualdad y la no discriminación destacadas en el informe al Consejo de Derechos Humanos en el contexto específico del control de las fronteras y la inmigración.**

56. **Los Estados Miembros deben encarar las ideologías y estructuras racistas y xenófobas que han ido conformando cada vez más la aplicación y administración del control de las fronteras y la inmigración. Los efectos de la tecnología son en gran parte producto de fuerzas sociales, políticas y económicas subyacentes que impulsan el diseño y la utilización de la tecnología. Si no se produce un cambio fundamental de los enfoques políticos de la gestión de las fronteras de corte racista, xenófobo, antimigrantes, antiapátridas y antirrefugiados no se podrán corregir los efectos discriminatorios de las fronteras digitales destacados en el presente informe. Los Estados deben cumplir las obligaciones internacionales en materia de derechos humanos para prevenir la discriminación racial en la aplicación de las leyes de fronteras e inmigración y aplicar las recomendaciones que figuran en el informe de la Relatora Especial titulado "La discriminación racial y las tecnologías digitales emergentes: un análisis de los derechos humanos" (A/HRC/44/57). Los Estados también deben seguir la orientación proporcionada por intervenciones como los Principios sobre la privación de la nacionalidad como medida de seguridad nacional[172] y los Principios de protección para personas migrantes, refugiadas y otras personas desplazadas durante la pandemia de COVID-19[173], en los que se articulan las obligaciones que incumben a los Estados, incluso con respecto a la igualdad y la**

[172] Institute on Statelessness and Inclusion y otros, Principios sobre la privación de la nacionalidad como medida de seguridad nacional.

[173] Zolberg Institute on Migration and Mobility y otros, "Movilidad y derechos humanos durante la pandemia de COVID-19: Principios de protección para personas migrantes, refugiadas y otras personas desplazadas", (2020).

no discriminación, de garantizar los derechos humanos de los migrantes, los refugiados, los apátridas y los grupos conexos.

57. **Los Estados Miembros deben adoptar y reforzar los enfoques jurídicos y normativos de igualdad racial y no discriminación basados en los derechos humanos con respecto al uso de las tecnologías digitales en el control y la administración de las fronteras y la inmigración. En la actualidad, no existe un marco global integrado de políticas de gobernanza del uso de las tecnologías automatizadas y otras tecnologías digitales, por lo que las obligaciones jurídicas internacionales vigentes en materia de derechos humanos resultan sumamente importantes para regular el diseño y la utilización de esas tecnologías.**

58. **Tanto en el plano nacional como en el internacional, los Estados Miembros deben velar por que el control y la administración de las fronteras y la inmigración estén sujetos a obligaciones jurídicas vinculantes para prevenir y combatir la discriminación racial y xenófoba en el diseño y la utilización de las tecnologías relativas a las fronteras digitales y ofrecer recursos a quienes la sufran. Estas obligaciones incluyen, entre otras, las siguientes:**

a) Adoptar medidas rápidas y eficaces para prevenir y mitigar el riesgo que suponen el empleo y diseño racialmente discriminatorios de las tecnologías digitales en el control de las fronteras, incluso estableciendo como requisito que para adoptar sistemas y antes de que se desplieguen públicamente deberán hacerse evaluaciones de su impacto en el goce de los derechos humanos a la igualdad racial y la no discriminación. Estas evaluaciones de impacto deben constituir una oportunidad valiosa para el diseño y la implantación conjunta, junto con representantes de grupos marginados por motivos raciales o étnicos, incluidos los refugiados, migrantes, apátridas y grupos afines. No bastará con aplicar un enfoque las evaluaciones del impacto sobre la igualdad que sea solo o incluso principalmente voluntario; es esencial que se exija su cumplimiento obligatorio;

b) Imponer una moratoria inmediata de la adquisición, venta, transferencia y utilización de tecnologías de vigilancia hasta que se establezcan salvaguardias sólidas de los derechos humanos que permitan regular esas prácticas. Estas salvaguardias consisten en actuar con la debida diligencia en el sentido de respetar las prohibiciones establecidas en el derecho internacional de los derechos humanos con respecto a la discriminación racial y aplicar la supervisión independiente, las leyes estrictas de protección de la privacidad y los datos y la plena transparencia en el uso de instrumentos de vigilancia como las grabaciones de imágenes y la tecnología de reconocimiento facial. En algunos casos, será necesario prohibir de manera absoluta las tecnologías que no cumplan las normas consagradas en los marcos jurídicos internacionales de derechos humanos que prohíben la discriminación racial;

c) Asegurar la transparencia y la rendición de cuentas en el uso de las tecnologías digitales para el control de las fronteras por las entidades públicas y privadas, y facilitar el análisis y la supervisión independientes, incluso utilizando únicamente sistemas que sean auditables;

d) Imponer a las empresas privadas obligaciones jurídicas para prevenir y combatir la discriminación racial y xenófoba causada por el uso de las tecnologías digitales en el control de las fronteras y ofrecer recursos a quienes la sufran;

e) Asegurar que las asociaciones que se establezcan entre el sector público y el privado para suministrar y utilizar tecnologías digitales en las fronteras sean transparentes y estén sujetas a una supervisión independiente en

relación con los derechos humanos, y que no den lugar a la abdicación de la responsabilidad de los gobiernos de rendir cuenta en materia de derechos humanos.

59. **La Relatora Especial tuvo la oportunidad de celebrar consultas con representantes del ACNUR y la OIM acerca de la utilización de diferentes tecnologías digitales de control fronterizo. Sobre la base de esas consultas, recomienda que ambos organismos adopten y apliquen mecanismos que permitan que los migrantes, los refugiados y los apátridas participen de manera sostenida y productiva en la toma de decisiones sobre la adopción, el uso y el examen de las tecnologías digitales de control de las fronteras. La Relatora Especial formula las recomendaciones que figuran a continuación.**

60. **La OIM debe:**

a) Incorporar y fortalecer las obligaciones y los principios internacionales de derechos humanos, especialmente los relativos a la igualdad y la no discriminación, al utilizar tecnologías digitales en el control de las fronteras y al supervisar su uso, incluso en todas sus asociaciones con entidades privadas y públicas. Para ello es necesario dejar de centrarse únicamente en las preocupaciones sobre la privacidad en el intercambio y la protección de datos y, en lugar de recomendar, establecer por mandato la protección de la igualdad y la no discriminación;

b) Adoptar políticas y prácticas obligatorias para realizar un análisis sistémico de los posibles efectos perjudiciales y discriminatorios de las tecnologías digitales en el control de las fronteras antes de que se adopten, y prohibir la adopción de tecnologías sobre las cuales no se pueda demostrar que cumplen los requisitos de igualdad y no discriminación. Proporcionar directrices más claras y concretas y basadas en los derechos humanos sobre los criterios para la designación de tecnologías digitales de "opción cero" y garantizar la aplicación de esas directrices;

c) Adoptar protocolos de obligatorio cumplimiento para evaluar de manera constante la situación de los derechos humanos en la aplicación de las tecnologías digitales una vez desplegadas en el control de las fronteras;

d) Crear mecanismos de supervisión independiente de la situación de los derechos humanos con respecto al uso por la OIM de las tecnologías digitales en el control fronterizo y aplicar reformas para asegurar una mayor transparencia en la forma en que se adoptan las decisiones de implantación de esas tecnologías;

e) Proporcionar a los migrantes, refugiados, apátridas y grupos conexos mecanismos que les permitan exigir cuentas directamente a la OIM cuando se vulneren sus derechos humanos como resultado del empleo de tecnologías digitales en el control fronterizo.

61. **El ACNUR, en comparación con la OIM, ha adoptado medidas de más alcance para incorporar las normas de igualdad y no discriminación en sus marcos de orientación sobre las tecnologías digitales en el control de las fronteras, pero también tiene que trabajar más para asegurar que esas normas se apliquen en la práctica. A ese respecto, la Relatora Especial formula las recomendaciones que figuran a continuación.**

62. **El ACNUR debe:**

a) Adoptar políticas y prácticas obligatorias para realizar un análisis sistémico de los posibles efectos perjudiciales y discriminatorios de las tecnologías digitales en el control de las fronteras antes de que se adopten, y

prohibir la adopción de tecnologías sobre las cuales no se pueda demostrar que cumplen los requisitos de igualdad y no discriminación. Proporcionar directrices más claras y concretas y basadas en los derechos humanos sobre los criterios para la designación de tecnologías digitales de "opción cero" y garantizar la aplicación de esas directrices;

b) Adoptar protocolos de obligatorio cumplimiento para evaluar de manera constante la situación de los derechos humanos en la aplicación de las tecnologías digitales una vez desplegadas en el control de las fronteras;

c) Crear mecanismos de supervisión independiente de la situación de los derechos humanos con respecto al uso por el ACNUR de las tecnologías digitales en el control fronterizo y aplicar reformas para asegurar una mayor transparencia en la forma en que se adoptan las decisiones de implantación de esas tecnologías;

d) Proporcionar a los migrantes, refugiados, apátridas y grupos conexos mecanismos que les permitan exigir cuentas directamente al ACNUR cuando se vulneren sus derechos humanos como resultado del empleo de tecnologías digitales en el control fronterizo.

63. **Todos los organismos humanitarios y conexos de las Naciones Unidas deben aplicar las recomendaciones anteriores dirigidas a la OIM y al ACNUR.**