Carlos Manuel Lancho Bances

POLÍTICAS DE DATOS Y GOBERNANZA ALGORÍTMICA DE PERSONAS REFUGIADAS Y MIGRANTES EN EL CONTEXTO EUROPEO

UNIVERSIDAD D CÓRDOBA

TRABAJO DE FIN DE MÁSTER

Dirigido por:

Dr. Carlos Arce Jiménez y Dr. Javier Sánchez Monedero

UNIVERSIDAD DE CÓRDOBA

Máster de Cultura de Paz, Conflictos, Educación y Derechos Humanos

Cátedra Unesco de Resolución de Conflictos

Córdoba 2022

A Paz, Agatha y Tristán,

Por enseñarme a creer.

ÍNDICE

Resumen

El presente trabajo de fin de máster estudia el empleo de herramientas de extracción y procesamiento de datos en población refugiada y migrante. A través de tres capítulos se plantea, primero, presentar y describir los sistemas informáticos biométricos que se emplean en fronteras, como los casos de EURODAC y PRIMES. Segundo, se profundizará en el marco normativo-jurídico nacional, comunitario e internacional para comprender los límites actuales que tienen este tipo de herramientas y el valor intrínseco que tiene la figura del refugio como un derecho humano. Tercero, se desarrollarán los conceptos de «extractivismo», «datificación» y «tecno-colonialismo» para entender las bases de lo que en esta investigación se interpreta como una infraestructura digital que contribuye al contexto de discriminación, criminalización e hipervigilancia de los solicitantes de asilo. Nuestra hipótesis apunta a que el uso de estas herramientas de datos contribuye a construir una gobernanza algorítmica sobre la población refugiada, cuya información privada tiene usos secundarios para los diversos actores que están involucrados: agencias de ayuda humanitaria, empresas privadas y estados.

Palabras clave

Gobernanza algorítmica, biometría, tecno-colonialismo, política de datos, datificación, extractivismo, refugiados.

Agradecimientos

Este TFM está dedicado a todas las personas que siguen luchando por encontrar un espacio más seguro y hacer prevalecer sus derechos fundamentales de acceso a un estatus de refugio digno y seguro.

El cuestionario de las entrevistas es el producto de una colaboración con el grupo de investigación de Security Flows. En especial, se contó con el apoyo de la Dra. Ana Valdivia.

INTRODUCCIÓN

El uso de las nuevas tecnologías como método para recolectar datos, a menudo personales o privados, de población vulnerable es una expresión contemporánea de discriminación. La datificación es un fenómeno socioeconómico que se basa en la cuantificación automatizada a través de información digital del que dependen cada vez más esferas de la vida social y que supone una fractura con los derechos humanos de los individuos que se encuentran en situación de refugio.

En la raíz de este problema contemporáneo se encuentran elementos del pasado colonial, cuestión que se puede comprender bajo el concepto de «tecnocolonialismo». Como afirman diversos estudios de migración y diásporas, el fenómeno de la datificación se puede entender en la dinámica del poscolonialismo, en tanto se entiende que las poblaciones vulnerables de los países del hemisferio sur son rentables desde un punto de vista económico.

Una de las expresiones de este fenómeno se encuentra en las organizaciones de cooperación internacional. La evidencia sugiere que diversas oenegés, con el fin de mejorar sus sistemas de reparto o localización de refugiados basan sus programas de ayuda en tecnología biométrica, que a su vez se obtiene a partir de contratos con grandes empresas. En este sentido, el sentido ético de la ayuda humanitaria queda rezagada a un segundo plano, pesando más la cuantificación de los individuos para propósitos de financiación.

Esta situación no se escapa a otras cuestiones como la política migratoria, que ya utiliza tecnología biométrica para la gestión de refugiados. En este sentido, la automatización y la cuantificación se han convertido en el nuevo paradigma de las políticas fronterizas, dejando a miles de refugiados a merced de un análisis y resultado computacional basados en factores recogidos en la extracción de datos: color de piel, procedencia, género, etc.

Como ruta metodológica, se proponen técnicas basadas en un método mixto, propio de las investigaciones sobre migración y diásporas. Partiendo de la amplia bibliografía científica, se realizará una combinación de entrevistas y encuestas, utilizando técnicas cualitativas y de etnografía como base. Por los límites de este trabajo, las entrevistas no se han realizado en contextos de fronteras, sino en espacios ofrecidos por la Cruz Roja de Córdoba.

ASPECTOS METODOLÓGICOS

1. Hipótesis

El uso de herramientas basadas en algoritmos como método para recolectar, procesar y analizar los datos personales de población refugiada es una expresión de discriminación y criminalización que supone, a toda luz, una fractura con determinados derechos fundamentales. Tres agentes interactúan en este escenario: las grandes empresas de tecnología, que crean las herramientas, las agencias de ayuda humanitaria, que las emplean en sus campos de trabajo y los estados nacionales, que usan estos datos para satisfacer sus objetivos en materia de política migratoria.

En la raíz de este problema contemporáneo se encuentran algunos fundamentos que hemos estructurado en nuestro marco conceptual y que son la clave para comprender este fenómeno de la era digital: el pasado colonial, que se expresa a través de la noción de «tecno-colonialismo», la «datificación» como forma de gobernanza a través de los datos y el «extractivismo», como sistema de apropiación de la materia prima que constituye los datos personales de millones de refugiados. Este marco conceptual permite comprender el funcionamiento de la gobernanza algorítmica de refugiados.

2. Objetivos

1. Aportar, a través de la realización de entrevistas semiestructuradas, las experiencias de la población refugiada en cuanto a los procesos de extracción de sus datos personales. Empleando una metodología cualitativa, se pretende profundizar en las historias de vida de una muestra pequeña localizada en la ciudad de Córdoba.
2. Analizar los sistemas informáticos de gran escala que se utilizan para la extracción y procesamiento de datos personales de personas demandantes de asilo y refugiadas, en particular aquellos de naturaliza biométrica. Estos son básicamente dos: EURODAC y PRIMES. A partir de ello, se explicará el funcionamiento de la gobernanza algorítmica en el contexto de las migraciones y asilo.

3. Conocer el marco normativo jurídico que existe para señalar la incompatibilidad de los derechos fundamentales con los métodos de extracción, procesamiento y utilización de los datos personales de refugiados llevados a cabo por los agentes antes mencionados.

4. Demostrar, mediante el estudio de la literatura científica, la presencia de determinados elementos que evidencian el trasfondo de discriminación y criminalización en los métodos de extracción y procesamiento de datos. Todo esto se argumentará mediante la explicación de algunos conceptos como tecno-colonialismo, datificación y extractivismo.

3. Técnicas de investigación

En el presente TFM se realizarán entrevistas semiestructuradas a un grupo de población refugiada. La elección de esta técnica de investigación en concreto se debe a su valor como método íntimo y directo para conocer las perspectivas de los entrevistados. La guía, incluida en el anexo II, contiene las preguntas que se han preparado previamente mediante consultas con otros grupos de investigación con experiencia en este tema en particular. No obstante, las entrevistas contarán con la flexibilidad necesaria para atender y profundizar en las respuestas que puedan surgir de los diferentes individuos.

Esta muestra demográfica es de diez personas aproximadamente. Los encuentros se realizarán entre los meses de junio, julio y agosto presencialmente en la ciudad de Córdoba y virtualmente a través de videollamadas. La población es de origen saharaui, maliense, senegalés, salvadoreño y venezolano. La información proporcionada será recogida, trascrita y tratada de manera anónima. En concreto, las entrevistas se llevarán a cabo con el apoyo técnico de la Oficina de Refugiados de la Cruz Roja Española.

La técnica planteada permite profundizar, de forma cualitativa, en los procesos de extracción de datos personales de la población refugiada. En este sentido, las preguntas estarán dirigidas para conocer de manera específica las experiencias, percepciones, opiniones y sensaciones positivas o negativas de los solicitantes de asilo. Se evitará, en la medida de lo posible, entrar en detalles personales, e irrelevantes para esta investigación, acerca de las experiencias traumáticas que los entrevistados puedan haber tenido en sus países de origen o en sus viajes para entrar en la Unión Europea.

Así mismo, se plantea realizar una revisión bibliográfica sobre la problemática planteada, la cual ha sido abordada desde la interdisciplinaridad. Por un lado, desde los estudios de migración y diásporas, y, por otro lado, desde los estudios de ciencias de la comunicación. En este sentido, el marco teórico parte del trabajo de otros académicos que ya han investigado sobre las nociones que se proponen como marco conceptual.

4. Universo de análisis

La selección de las personas refugiadas se hizo en coordinación con la Oficina de Refugiados de la Cruz Roja en Córdoba. Por un lado, se buscó una representación geográficamente variada, que permitiera una mayor diversidad de testimonios. Por ese motivo, aunque la mayoría de las personas provienen de África Occidental, también se han realizado encuentros con ciudadanos provenientes de El Salvador y Venezuela por su proximidad sociocultural con España.

Los refugiados son en su mayoría hombres, mayores de edad, solteros, casados o con hijos. En cuanto a las edades, varían entre los 20 y 40 años aproximadamente. Los grados de educación también son distintos, ya que se incluyen desde jóvenes estudiantes hasta profesionales con grado de instrucción superior. Toda la población registra su llegada a España entre los años 2021 y 2022, con lo cual sus experiencias son recientes y responden a políticas migratorias vigentes.

CAPÍTULO I

DECODIFICANDO EL ALGORITMO

En el siglo XIX, en la Inglaterra victoriana, el investigador Francis Galton ideó un sistema que permitía analizar cientos de huellas digitales para propósitos de investigación policial. Ya en su obra *Fingerprints*, Galton sugería la existencia de patrones únicos e irremplazables en las huellas dactilares de los seres humanos. Aunque sus investigaciones se basaban en el trabajo de otros científicos de la época, no cabe duda de que su trabajo supuso una auténtica revolución en el campo de la criminología y un precedente en el desarrollo de los estudios biométricos.

El trabajo de Galton sugiere que la extracción y el procesamiento de datos biométricos no es nuevo en la historia. Así como en el siglo XIX se utilizaron en las investigaciones policiales, en la actualidad la tecnología biométrica tiene diversos usos en la práctica. Desde el reconocimiento facial en los móviles, pasando por el desbloqueo a través de huellas digitales, hasta la lectura de iris que está reemplazando a los primeros como sistema preferente de reconocimiento de identidad.

No obstante, estos usos cotidianos solo representan el lado más visible de la biometría, ya que su empleo de esta ha encontrado un nicho importante en la política fronteriza de muchos países, sobre todo del hemisferio norte. Con el aumento exponencial de la población refugiada debido a los conflictos, hambrunas y violencia, la biometría se emplea sobre la población migrante y, sobre todo, en los solicitantes de asilo.

Los objetivos de la biometría siguen siendo los mismos: la obtención masiva de datos que permitan la identificación lo más exacta posible de los individuos. Pero, de forma similar al siglo XIX, en la base de muchos algoritmos se encuentra un propósito criminalizador. En la carrera por obtener la mayor cantidad exacta de datos personales, subyace una intención: identificar a la persona refugiada y garantizar su vigilancia y control.

1. La infraestructura de la hipervigilancia

Antes de adentrarnos en los mecanismos específicos del extractivismo biométrico[1] es importante entender sus estructuras fundamentales. Es decir, la lógica que existe detrás de su funcionamiento práctico. Para ello, partimos de la tesis de Latonero y Kift, quienes explican que la lógica del control de movimiento se articula en una infraestructura, dentro de la cual se desenvuelven las ciencias biométricas. Así, esta infraestructura vendría a ser el esquema lógico bajo el cual la tecnología trabaja[2].

Pero los autores dan un paso más, reemplazando la idea de la «infraestructura» por «pasaje» (*passage*). Este «pasaje digital» o *digital passage* se refiere, por un lado, al acto, permiso o libertad de cruzar de un lugar a otro, y, por otro lado, a toda la arquitectura limitante que restringe el intercambio de información, bienes o personas. En esta «ambigüedad del espacio», los refugiados no solamente se enfrentan a límites físicos como fronteras, vallas o puestos de control, sino a toda la infraestructura digital que condiciona su tránsito. Por ello, a la hora de hablar del extractivismo biométrico es inevitable hacer referencia a las infraestructuras digitales que dificultan los canales de migración[3].

Así mismo, en este pasaje o infraestructura, existen diferentes actores que trabajan de manera simultánea: traficantes, empresas, gobiernos y organizaciones humanitarias. Mientras que los primeros lucran de manera ilícita de los límites que impone la infraestructura del extractivismo y la hipervigilancia, las empresas privadas son las principales proveedoras de la tecnología biométrica que hacen realidad estos obstáculos y que son parte de algunas políticas migratorias de determinados países o entidades supranacionales como la Unión Europea[4].

En cuanto a los medios digitales, que también forman parte de esta gran infraestructura, estos se han convertido en un vehículo idóneo para el extractivismo de datos. Los mapas, aplicaciones, zonas *wi-fi* y redes sociales forman parte del pasaje digital que utilizan las organizaciones no gubernamentales y los gobiernos para conseguir datos personales de la población refugiada. Estas cuestiones de

[1] El concepto de extractivismo lo define Mirca Madianou (ver referencia 20), apoyándose en Mezzara y Neilson, como la «minería de datos» y otras formas inmateriales de trabajo. Cuestión que es una de las bases de su tesis del tecno-colonialismo.
[2] Mark Latonero y Paula Kift, «On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control,» *Social Media and Society* 4, no. 1 (2018): 3.
[3] Latonero and Kift, «On digital passages and Borders,» 3.
[4] Latonero and Kift, «On digital passages and Borders,» 4-6.

desarrollan detenidamente en este capítulo, pero por el momento basta con tener en cuenta que existe una colaboración entre los estudios de medios digitales y los estudios sobre inmigración[5].

En paralelo, como subrayan Nedelcu y Soysüren, toda la infraestructura de vigilancia que ofrecen determinadas tecnologías de extracción de datos obedece a la política de seguridad establecida a partir de los atentados del 11/9. Así, tanto Estados Unidos como la Unión Europea y otras naciones han creado un régimen de hipervigilancia en sus fronteras. En este sentido, como explican los autores, las tecnologías de la inmigración se prestan a restringir la circulación de la migración, así como limitar los derechos de personas refugiadas, o como último objetivo, limitar la entrada de ciudadanos provenientes del sur global[6].

En este sentido, a la hora de examinar estas nuevas tecnologías de la inmigración, debemos partir de la premisa de que, como explica Ponzanesi, la revolución digital no elimina las relaciones de poder o fortalece la democratización de la información, sino que, en realidad, impacta de manera desigual sobre las comunidades más vulnerables. En el caso de los inmigrantes y en especial los solicitantes de asilo, los mecanismos de extracción de datos son utilizados con fines discriminatorios y criminalizadores[7].

En cuanto al proceso de extractivismo en sí, podríamos decir que la datificación ocurre de forma diferente dependiendo de las fuentes y del estado migratorio de los refugiados. Obedeciendo al esquema que ofrece Sánchez Monedero, los datos provienen de, en primer lugar, de reportes acerca del país del que proviene el refugiado que condiciona la solicitud de asilo; en segundo lugar, de la identificación de los refugiados en campos de refugio; en tercer lugar, del viaje a través de los distintos países; en cuarto lugar, de las fronteras y evaluación del país de acogida y, finalmente, de la vigilancia o seguimiento de cada refugiado[8].

2. Sistemas informáticos a gran escala

La necesidad de agrupar la ingente cantidad de datos de personas refugiadas obedece a una necesidad y a una obligación legal para los estados que han firmado y/o ratificado los convenios y tratados que defienden los derechos fundamentales de los solicitantes de asilo. El caso de la Unión Europea no es

[5] Latonero and Kift, «On digital passages and Borders,» 2-3.
[6] Mihaela Nedelcu and Ibrahim Soysüren, «Precarious Migrants, Migration Regimes and Digital Technologies: The Empowerment-Control Nexus,» *Journal of Ethnic and Migration Studies* 48, no. 8, 1821-1837 (2020): 2.
[7] Sandra Ponzanesi, «Digital Diasporas: Postcoloniality, Media and Affect,» *Interventions* 22, no. 8 (2020): 982.
[8] Javier Sánchez-Monedero, «The Datafication of Borders and Management of Refugees in the Context of Europe,» *Data Justice Project* (2018): 2.

ajeno. La entrada de miles de refugiados anuales, sobre todo a partir de la mal llamada "crisis de refugiados" del 2015, compele a los estados a depender de bancos de data para procesar, organizar y retener la información de los solicitantes. Pero, sobre todo, la ley es clara cuando se trata de la recepción de personas refugiadas. De conformidad con los artículos 10 y 11 del Tratado de Dublín, el primer estado de la unión al que llegue un refugiado será responsable, con las excepciones establecidas en el documento, de realizar los exámenes y acoger a la persona solicitante.

Si bien estas cuestiones se desarrollarán en el segundo capítulo, es importante entender que el derecho internacional establece de manera clara los derechos y deberes, tanto de los estados hacia los refugiados, así como los de estos últimos hacia los estados.

2.1. Eurodac

La regulación Eurodac establece la creación de un repositorio central europeo en el que se encuentran todas las huellas digitales y datos para el reconocimiento facial obtenidas de solicitantes de asilo. El objetivo primordial de esta base de datos es darle herramientas a lo establecido en la Convención de Dublín, es decir, hacer lo más efectiva posible la norma que obliga a los solicitantes de asilo a permanecer en el primer país de acogida de la Unión de Europea, sin la posibilidad de solicitar más de un permiso de refugio.

No obstante, más allá de una simple herramienta que otorga facultades a un convenio internacional, Eurodac también cumple con una función que se puede interpretar como criminalizadora. Como bien apunta Latonero, esta base de datos acumula también todos los intentos de cruces fronterizos ilegales[9]. Así, como el propio reglamento europeo estipula, "la información recopilada es necesaria para la prevención, detección o investigación de las posibles ofensas terroristas"[10].

Así mismo, la evidencia señala que Eurodac está en colaboración con instituciones de seguridad, como, por ejemplo, Europol o la Oficina de Policía Europea, entre otras instituciones de seguridad, con el propósito de contrastar las huellas digitales obtenidas de los solicitantes de asilo con expedientes criminales[11]. Es más, como señalan Metcalfe y Dencik, existen importantes críticas que se deben tener

[9] Latonero and Kift, «On digital passages and Borders,» 6.
[10] Reglamento (UE) 603/2013 del Parlamento Europeo y del Consejo de 26 de junio de 2013, relativo a la creación del sistema «Eurodac».
[11] Sánchez-Monedero, «The Datafication of Borders,» 13.

en cuenta en lo referente al uso que se le da a Eurodac, ya que los solicitantes de asilo son considerados desde un primer momento como criminales potenciales. Así, la obligación de solicitar huellas digitales, conducta usualmente asociada con la criminalidad en Europa, es parte integral de la Convención de Dublín y de Eurodac y demuestra la prevalencia de la gobernanza basada en la «datificación» y en la criminalización de personas desplazadas[12].

Así mismo, en el uso de estas tecnologías no existe un auténtico consentimiento de los solicitantes de asilo a entregar datos personales. Esto se debe a diversos motivos. Por un lado, los solicitantes se sienten obligados a dar lo que las autoridades les pidan por temor a ser rechazados y devueltos a sus países de origen, por lo que las entrevistas se realizan en un contexto de extrema desconfianza. Por otro lado, existe una sensación de obligación y agradecimiento por parte de los solicitantes, lo que genera un clima de gratitud hacia el benefactor que ofrece la ayuda humanitaria[13]. Por ejemplo, en las entrevistas que se realizaron a personas refugiadas de Centro América y África Occidental, existe un consenso de buenos tratos por parte de las autoridades migratorias. Solo uno de los entrevistados, que trabajaba como informático en su país de origen, declaró estar en desacuerdo con la entrega de sus datos personales.

El solo hecho de que la información personal de los refugiados, en este caso sus huellas digitales, estén a disposición de las fuerzas de seguridad sugiere una criminalización inicial. En la práctica, se busca criminalizar el derecho al refugio y crear toda una infraestructura que facilite la hipervigilancia de determinados sujetos. En este sentido, Eurodac no solo se trata de un repositorio de información de refugiados, sino, una herramienta más al servicio de las políticas migratorias. La evidencia sugiere que, sobre todo a partir del último flujo migratorio ocasionado por la invasión de Rusia a Ucrania, existe una jerarquización discriminadora de personas refugiadas. Mientras que ucranianas y ucranianos han accedido a solicitudes exprés, hay quienes llevan esperando meses y hasta años para conseguir un permiso de refugio[14]. Así, Eurodac, siendo capaz de compartimentar los datos de refugiados, se ha

[12] Metcalfe, P., & Dencik, L. «The politics of big borders: Data (in)justice and the governance of refugees». *First Monday*, (2019): 24(4).
[13] Mirca Madianou, Jonathan Corpus Ong, Liezel Longboan, Jayeel Cornelio, «The Appearance of Accountability: Communication Technologies and Power Asymmetries in Humanitarian Aid and Disaster Recovery,» *Journal of Communication* 66, no. 6 (2016): 28.
[14] «EURODAC: un sistema biométrico para categorizar y criminalizar a esos migrantes y refugiados que no queremos,» Algorace, 20 de abril de 2022, https://algorace.org/2022/04/20/eurodac-un-sistema-biometrico-para-categorizar-y-criminalizar-a-esos-migrantes-y-refugiados-que-no-queremos/

convertido en una herramienta capaz de discriminar de manera automática, dando prioridad a unos sobre otros. No es difícil observar que detrás de este uso indebido se hayan razones puramente raciales.

2.2. PRIMES

PRIMES es el ecosistema de herramientas y datos para la gestión y control de personas refugiadas desarrollado por la Agencia de la ONU para los Refugiados (ACNUR). El Ecosistema de Registro de Identidad de la Población funciona como una gran estructura que sostiene todas las herramientas y aplicaciones que se utilizan para procesar e identificar los casos que gestiona ACNUR. Así, como iremos desglosando en los siguientes párrafos, dentro de Primes funciona el sistema ProGres, BIMS, Rapp, entre otros.

A diferencia de Eurodac, PRIMES no funciona a nivel supraestatal, sino que responde a ACNUR, una de las organizaciones más importantes en cuanto a gestión de personas refugiadas en el mundo. Para entender su funcionamiento, es importante comprender que las tecnologías de extracción de datos biométricos son transversales, en tanto se utilizan para fines de políticas migratorias, como también para los fines de organizaciones sin ánimos de lucro.

Desde su lanzamiento en el año 2017, PRIMES ha acelerado de manera exponencial el ritmo de recopilación de datos biométricos. Por ejemplo, en su primer año de implementación, se logró extraer y recolectar los datos biométricos de más de 7,1 millones de personas en más de 60 países. De esta población, 8 de cada 10 eran personas refugiadas gestionadas por ACNUR[15]. Otras agencias de las Naciones Unidas también están siguiendo los mismos pasos, como es el ejemplo del the World Food Program (WFP).

Como defiende Madianou, el uso de PRIMES refleja el vuelco ideológico que han dado las organizaciones de ayuda humanitaria al adoptar el discurso del sector privado. Es decir, según las agencias el uso de esta infraestructura se defiende por tres razones: en primer lugar, se busca empoderar a los refugiados a través de actividades económicas basadas en la web (por ejemplo, la adquisición de productos mediante reconocimiento de iris); en segundo lugar, fortalecer las capacidades de los estados para gestionar las solicitudes de asilo y, en tercer lugar, mejorar la oferta de

[15] Mirca Madianou, «The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies» *Television & New Media* 20, no 6, pp. 581-599 (2019): 15

ayuda a través de una optimización de la eficiencia[16]. Esta última cuestión es quizá la más interesante porque saca a la luz la doble intención de utilizar herramientas digitales para extraer datos biométricos: por un lado, reducir el fraude, pero, por otro lado, satisfacer las expectativas de los inversionistas o donantes, lo que explicaría la transición de las agencias hacia el modelo de mercado que demanda eficacia y rentabilidad[17].

Mientras que el uso de la biometría se justifica en el nombre de la eficacia, existen también riesgos inherentes en el uso de este tipo de tecnología. Como explica un informe realizado por Oxfam, cuestiones como la «fiabilidad» y la «reusabilidad» son importantes de tener en cuenta. En primer lugar, la posibilidad de que los algoritmos arrojen falsos negativos o falsos positivos en la identificación de individuos, como sería el caso de las huellas digitales, que presentan un margen de error considerable. En segundo lugar, los algoritmos tampoco pueden asegurar que terceros actores, como los gobiernos de los estados anfitriones o los gobiernos de los estados de origen no accedan a los bancos de datos para reutilizarlos para sus propios fines[18]. En ambos casos, el peligro de que la biometría no funcione correctamente o que se pueda utilizar de manera poco fiable es una cuestión que se debe tener en cuenta al momento de presentar a este tipo de tecnología como infalible.

PRIMES funciona como una infraestructura, o, en palabras de Latonero, como un «digital passage», dentro del cual funcionan varias herramientas para la recolección de datos biométricos. Estos son: ProGres v4, Rapp, Dataport, BIMS, RAIS, IrisGuard, GDT, entre otras. En la siguiente imagen se puede apreciar cómo se organiza y funciona esta estructura:

[16] Madianou, «The Biometric Assemblage,» 15.
[17] Madianou, «The Biometric Assemblage,» 21.
[18] Carly Nyst, Zara Rahman, Paola Verhaert y Anna Kondakhchyan, eds., *Biometrics in the Humanitarian Sector* (Oxford: Oxfam, 2018), 9.

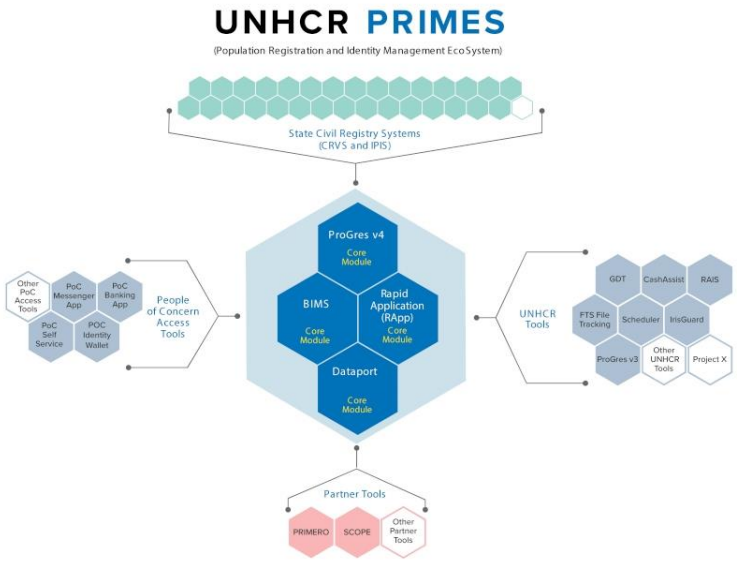

Ilustración 1: Ecosistema de herramientas de PRIMES (Fuente: UNHCR https://www.unhcr.org/ primes.html)

2.2.1. ProGres v4

ACNUR define Progres v4 como su «aplicación de software corporativa, centralizada y basada en la web para gestión de casos [la cual] admite funciones operativas que incluyen desde el registro de individuos hasta una amplia gama de funciones de gestión de casos como asistencia, gestión de casos de protección, intervenciones de protección y el otorgamiento de documentación y asistencia basada en efectivo»[19]. ACNUR describe esta aplicación como clave en su trabajo en terreno con población refugiada, haciendo de esta herramienta una parte fundamental del funcionamiento de operaciones.

Como cuestión interesante, la empresa responsable de construir Progres v4 fue Microsoft, a través de su herramienta Microsoft Dynamics 365 para construir sistemas de gestión de relaciones con clientes alojados en la nube de la empresa. Como se verá más adelante, existe una relación entre agencias de ayuda humanitaria (como ACNUR o WFP) empresas y estados. En este «trinomio de la discriminación», la tecnología de extracción de datos biométricos es diseñada por empresas privadas, como Microsoft o IBM, mientras que los beneficiarios son los propios estados[20].

[19] «Guía sobre registro y gestión de identidad: planificación y preparación de los sistemas de registro y gestión de identidad», ACNUR, https://www.unhcr.org/registration-guidance/es/chapter3/registration-tools/
[20] Mirca Madianou, «Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises,» *Social Media and Society* 5, no. 3 (2019): 5.

Así mismo, ProGres puede ser utilizado por ACNUR, pero también por los propios estados para gestionar los datos extraídos de sus solicitantes de asilo[21]. El objetivo de la aplicación es conseguir un alcance global, de manera que los datos de refugiados puedan servir a los socios de ACNUR. Como explica la propia agencia, se «ha adaptado esta poderosa herramienta para crear un sistema de gestión de casos verdaderamente global. ProGres v4 permite a ACNUR otorgar acceso a socios, incluidos los gobiernos de acogida, garantizando una plataforma común para la colaboración»[22].

Incluso, ProGres permite que el cifrado de extremo a extremo transmita los datos registrados a entidades financieras que participen en los programas de ayuda. Así, por ejemplo, cuando se requiera la asistencia en efectivo para determinados solicitantes de asilo, los bancos pueden tener acceso a parte de los datos, como en el caso de los biométricos, para realizar la autenticación de personas. En una auditoría de las herramientas de ACNUR se concluía que no había mecanismos de protección que impidieran a los socios, incluyendo empresas, con acceso a estas herramientas recopilar y reutilizar los datos para otros fines[23].

En esta misma línea, ProGres, al no ser precisamente una herramienta para datos biométricos, está diseñada para ser compatible y trabajar en colaboración con otras aplicaciones que sí integran estos datos, como es el caso de BIMS (*Biometric Database*) pero también otras herramientas de distribución de alimentos o analíticas de datos como GDT (*food and assistance distribution*), Data Port (*reporting and data analysis*)[24] y, como ya se ha mencionado, con aplicaciones de distribución monetaria de entidades financieras.

En una entrada de blog publicada en 2017, ACNUR hacía hincapié en las bondades de ProGres, en especial en su aplicación en territorio bielorruso, a través de su organización socia, Refugee Counseling Service[25]. Esta cuestión abre la puerta a muchas interrogantes. Si ProGres es compatible con otras herramientas de extracción biométrica y está abierta a ser compartida con agencias estatales, existe el peligro de que un estado con pobres credenciales democráticas y de derechos humanos pueda acceder a los datos de miles de solicitantes de asilo.

---

[21] Sánchez-Monedero, «The Datafication of Borders,» 4.
[22] ACNUR, «Guía sobre registro y gestión de identidad».
[23] TriLateral Research and Consulting and the Office of the United Nations High Commissioner for Refugees, *Privacy Impact Assessment of UNHCR Cash Based Interventions.* New York, NY: UN Headquarters, 2015.
[24] Sánchez-Monedero, «The Datafication of Borders,» 4.
[25] «proGres version 4 is now live in Belarus», ACNUR, Oct 26, 2017, https://www.unhcr.org/blogs/progres-version-4-is-now-live-in-belarus/.

Ese es el caso ejemplar de los refugiados durante el genocidio contra la población Rogingya en Myanmar, que en el año 2017 huyeron a la vecina Bangladesh. Las Naciones Unidas, en colaboración con el gobierno de Daca, recolecto miles de datos biométricos (huellas digitales y fotografías) para identificar a las personas refugiadas y darles acceso a ayuda humanitaria. Toda esta información sensible quedó en manos de las autoridades bangladesas que tiempo después inició conversaciones con el gobierno de Myanmar para el retorno de los refugiados[26]. O, como en el caso del primer ejemplo, en el invierno de 2021-22, cuando las autoridades de Bielorrusia utilizaron población refugiada en su frontera oeste para presionar a la Unión Europea.

2.2.2. RApp – The Rapid Application

En cuanto a Rapp, también parte de la infraestructura de PRIMES, se trata de una aplicación diseñada especialmente para dispositivos móviles y computadoras portátiles que permite ingresar datos relacionados con la identidad de la persona y geolocalización. La herramienta funciona de manera *offline*, lo cual permite que se pueda utilizar en cualquier momento y sin conexión a internet. A través de esta, se puede extraer datos biográficos (como nombre, edad o sexo) o incluso biométricos (fotografías)[27]. Luego de subirse, los datos obtenidos a través de Rapp se pueden sincronizar con otras aplicaciones de PRIMES, como ProGres o BIMS para reforzar la información acerca de un individuo, una familia o incluso las relaciones que un refugiado pueda tener con otro.

2.2.3. BIMS: Sistema de Gestión de Identidad Biométrica

Como lo indica su nombre, BIMS se trata de la herramienta para gestionar los datos biométricos de los solicitantes de asilo. Funciona a través de la extracción de las 10 huellas dactilares y la lectura de ambos iris. Según explica la propia ACNUR, la recopilación de huellas e iris hace mucho más "eficiente" la identificación de cada individuo, reduciendo la posibilidad de suplantación o errores en

[26] Elise Thomas «Tagged, tracked and in danger: How the Rohingya got caught in the UN's risky biometric database». Wired, March 12, 2018, http://www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh.
[27] ACNUR, «Guía sobre registro y gestión de identidad».

la representación de individuos. Lo que permite es la comprobación de la identidad en tiempo real en todos los sitios de ACNUR en donde se utilice el sistema[28].

Según la propia agencia se trata de un sistema rápido y que se puede utilizar en el terreno, incluso sin conexión a internet. Así, BIMS es capaz de analizar datos de los usuarios y dar resultados en cuestión de segundos (cinco para ser exactos). La aplicación funciona desde el año 2010 y se utilizó por primera en el año 2013, en Malawi. Al igual que las otras herramientas, BIMS está integrada en PRIMES y permite integrarse con ProGres o con RApp, de manera que los datos se complementen[29].

2.2.4. GDT: La Herramienta de Distribución Global

GDT está relacionada con BIMS. Utiliza el banco de datos biométricos de esta última para optimizar la entrega de alimentos y otros servicios a usuarios en los campamentos de refugiados. En otras palabras, utiliza la biometría para mejorar las operaciones que requieran un esfuerzo de distribución de recursos. De acuerdo con ACNUR se trata de una herramienta rápida, eficiente, que evita fraude y ayuda al trabajo de gestión.

La herramienta no solo se puede integrar con BIMS, sino también con ProGres, de manera que los informes se actualizan automáticamente y se puede conocer en tiempo real qué individuos o familias han hecho uso de determinados recursos. Además, permite conocer la cantidad de recursos que se han consumido. En este sentido, se trata de una completa digitalización de la distribución de alimentos.

2.2.5. IrisGuard

De manera similar a BIMS, IrisGuard se trata de una herramienta biométrica mediante la cual se obtienen los datos de iris de los individuos. Según ACNUR, IrisGuard se utiliza principalmente para optimizar la gestión de identidad e integrarla dentro de operaciones de ACNUR o terceras partes como bancos. Por ejemplo, en algunos campos de refugiados, los usuarios pueden acceder a supermercados, cajeros automáticos e incluso a entrevistas para reasentamiento a través de este sistema[30]. Así, un refugiado o refugiada puede acceder a los bancos de comida situando su ojo en los dispositivos de

[28] ACNUR, «Guía sobre registro y gestión de identidad».
[29] Sánchez-Monedero, «The Datafication of Borders,» 7.
[30] Mirca Madianou, «The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies» *Television & New Media* 20, no 6, pp. 581-599 (2019).

IrisGuard. El acceso a la ayuda humanitaria queda supeditada a la entrega "voluntaria" de estos datos biométricos[31].

Hasta el momento, la herramienta se ha utilizado sobre todo en los campamentos de Jordania, en población siria. Como se ilustrará en el estudio de casos más adelante, estos datos pueden tener un uso perverso. Si esta tecnología está al alcance de los estados, por ejemplo, el de Jordania, basta con acceder a PRIMES para saber qué personas estuvieron en los campamentos de refugiados, vigilarlos, restringir su movimiento o incluso denegar la entrada o retorno de estas personas. ACNUR defiende que IrisGuard es parte fundamental de sus operaciones en Medio Oriente, por lo que se podría deducir que su uso se podría externalizar a otras regiones.

2.2.6. RAIS: Sistema de Información de Asistencia a Refugiados

RAIS funciona como una plataforma en la cual los datos de refugiados sirven para mejorar la rendición de cuentas de ACNUR, por lo que los usuarios finales son los socios y donantes. Aunque, cabe decir que la herramienta está siendo usada únicamente en la región de Medio Oriente y Norte de África (MENA), por lo que, a diferencia de otras aplicaciones, no está muy extendida. No obstante, lo interesante de esta aplicación es la dimensión financiera que tiene y que en el fondo también justifica el uso de las otras herramientas del ecosistema PRIMES. Es decir, optimizar la rendición de cuentas para la seguridad de quienes aportan los fondos que utiliza ACNUR. A fin de cuentas, se trata de una herramienta con fines económicos.

3. Empresas, agencias y fronteras: el trinomio de la discriminación

Existe un robusto consenso académico de que la biometría y otros tipos de tecnología de procesamiento de datos pueden tener consecuencias negativas en cuanto a su uso. Aunque sería apresurado concluir que los diseñadores de algoritmos o las instituciones que los emplean tienen malas intenciones, en la práctica la evidencia indica que en las fronteras o en los campamentos de refugiados existen fuertes indicios de discriminación en el uso de estas herramientas. Como señala la Relatora Especial sobre racismo y la discriminación racial de las Naciones Unidas, el diseño y uso de la tecnología biométrica reproduce de manera intencional o inintencional estructuras racialmente

[31] ACNUR, «Guía sobre registro y gestión de identidad».

discriminatorias que, de manera sistemática, interfieren con determinados derechos fundamentales de ciertos grupos debido a la raza, etnicidad, nacionalidad etc.[32].

Para comprender los peligros en los que puede incurrir la automatización de datos, es importante tener en cuenta a los actores que están detrás de su puesta en práctica. Cuando hablamos de políticas de fronteras, en el caso de Eurodac, o en campañas humanitarias, en el caso en PRIMES, quienes están detrás del diseño y construcción de las aplicaciones y herramientas biométricas, son empresas privadas, gigantes tecnológicos como Microsoft, Accenture, IBM, entre otras[33]. Detrás de todo esto, yace una «lógica capitalista»[34], que se basa en una estrecha colaboración entre el sector privado y el público. El primero (las empresas) obtiene una ventaja económica, mientras que el segundo (agencias y estados) consigue información para desarrollar sus proyectos de ayuda humanitaria o sus políticas fronterizas. La pregunta clave es la siguiente: ¿qué sucede con los datos obtenidos? Si las empresas son quienes se encargan de diseñar la tecnología, ¿no tendrían acceso a los bancos de datos que se generan a partir de esta?[35].

Los tres actores interactúan entre sí y se retroalimentan[36]. Las empresas crean el producto, las agencias humanitarias lo incorporan en su trabajo de campo y los estados tienen acceso a estos bancos de datos de los solicitantes de asilo y los utilizan poner desarrollar sus políticas fronterizas. Obsérvese, por ejemplo, el caso ya mencionado de los refugiados rohingyas en Bangladesh. Al mismo tiempo, las empresas de tecnología, que también trabajan directamente con los estados, utilizan a la población refugiada para probar sus nuevos productos[37] y comercializarlos en el cada vez más competitivo mercado de la tecnología digital[38].

Como trasfondo de esta «lógica capitalista», es fundamental entender el concepto de datificación, cuestión que se abordará con mayor detenimiento en el tercer capítulo, pero que por el momento basta con definirlo como la categorización automatizada de sujetos a partir del procesamiento de datos

[32] United Nations Human Rights Council, Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis*. New York, NY: UN Headquarters, 2020: 12.
[33] Mirca Madianou, «Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises,» *Social Media and Society* 5, no. 3 (2019): 5.
[34] Madianou, «Technocolonialism: Digital Innovation and Data Practices,» 5.
[35] Madianou, «Technocolonialism: Digital Innovation and Data Practices,» 5.
[36] Mirca Madianou, «The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies» *Television & New Media* 20, no 6, pp. 581-599 (2019): 19.
[37] Christina to Nedden, C y Dongus, A. «Tested on millions Non-volunteers / Getestet an Millionen Unfreiwilligen». *ACNUR* (2017, December 17). https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/01/article_1.pdf.
[38] Madianou, «Technocolonialism: Digital Innovation and Data Practices,» 5.

con el objetivo de construir sociedades determinadas por el control algorítmico[39]. Como defiende Madianou, los datos se han convertido en la nueva divisa para las organizaciones humanitarias, la clave en el desarrollo de sus campañas. Sin embargo, no es descabellado asumir que, para los estados, los datos también han adquirido un valor importante para sus políticas migratorias. En la hiperactividad por obtener más y mejores datos, no solo existe una notoria ausencia de derechos básicos en el trato de los datos de población refugiada, sino que, detrás de la datificación, hay una acción extractivista reforzada por las estructuras poscoloniales que se ejercen de norte a sur[40].

En esta dinámica de poder, control y mercantilización, las víctimas son percibidas en cuanto a su valor como proveedores de información personal. El estudio de Crawford y Finn recuerda que durante los días que siguieron al terremoto de Haití de 2010, miles de mensajes de texto que contenían información privada fueron difundidos sin el consentimiento de los afectados que habían utilizado sus teléfonos móviles para brindar información sobre los daños ocasionados[41]. Los voluntarios de la llamada «Misión 4636» traducían estos mensajes y se los enviaban a las entidades de asistencia (sobre todo a los militares de Estados Unidos). Esto no sirvió de ayuda para quienes habían emitido los mensajes, que quedaron en un segundo plano como simples informantes, pero sí para quienes estaban interesados en recoger y procesar estos bancos de datos. Es más, como se esfuerzan en señalar los autores, esta cuestión no hizo más que reproducir ciertas estructuras sociales entre quienes se encontraban en situación de vulnerabilidad (los haitianos pobres), quienes trabajaban en agencias de ayuda humanitaria (los voluntarios internacionales) y quienes financiaban la ayuda (el ejército de Estados Unidos)[42].

En este sentido, el libre consentimiento se trata de un concepto vacío cuando hablamos del extractivismo de datos. Para los solicitantes de asilo no existe la posibilidad de negarse a dar sus datos privados, ya sean biométricos o de otro tipo, porque el riesgo de que sus solicitudes sean denegadas o dilatadas en el tiempo es considerable. Por lo tanto, a pesar de que las agencias humanitarias o los gobiernos se esfuercen en señalar la voluntariedad de la información obtenida, se trata de un

[39] Nick Couldry and Ulises A. Mejias, «Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject,» *Television and New Media* 20, no. 4 (2019): 11, https://doi.org/10.1177/1527476418796632.
[40] Mirca Madianou, «The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies» *Television & New Media* 20, no 6, pp. 581-599 (2019): 20.
[41] Kate Crawford and Megan Finn, "The Limits of Crisis Data: Analytical and Ethical Challenges of Using Social and Mobile Data to Understand Disasters," *GeoJournal* 80, no. 4 (2015): 494.
[42] Crawford and Finn, «The Limits of Crisis Data, » 494.

formalismo sin sustento ni lógica. En el fondo, ya sea en fronteras o en los campamentos de refugiados, existen motivaciones que trascienden los objetivos de la ayuda humanitaria.

En las entrevistas que se realizaron a personas refugiadas de Mali, Sahara Occidental, Senegal, El Salvador y Venezuela existe un consenso de que el trato de las autoridades migratorias fue positivo. A pesar de que el origen geográfico era distinto y las motivaciones de la solicitud de asilo eran diferentes, los entrevistados recalcaron el buen trato al momento de la recolección de datos personales. A tenor del trabajo de campo más minucioso y directo que se ha llevado a cabo en campos de refugiados y en fronteras por parte de otros investigadores, se pueden extraer algunas conclusiones.

La primera, en consonancia con lo previamente expuesto, existe un clima de agradecimiento hacia los benefactores, en este caso las autoridades migratorias, por haberles concedido la «oportunidad» de conseguir protección en suelo europeo, cuando en realidad se trata de un derecho reconocido a nivel internacional. El segundo motivo es una deducción lógica: los refugiados y refugiadas tienen como principal objetivo conseguir asilo, por lo que la entrega de datos personales de cualquier índole, y a través de cualquier tipo de tecnología, es una cuestión secundaria. Esta segunda cuestión quedó plasmada en algunas respuestas de quienes respondieron a la pregunta «¿Pudiste decidir qué datos personales entregabas y cuáles no?»[43].

Existe un tercer motivo igual de importante que es, al mismo tiempo, una cuestión estructural en esta investigación. La mayoría de las personas refugiadas, al igual que gran parte de los usuarios de internet, no tienen un conocimiento previo acerca de la transferencia de datos ni tampoco sobre las herramientas biométricas que se usan para determinados fines. Esto no quiere decir que haya un desconocimiento de los derechos que atañen al estatus de solicitante de asilo, sino que no hay una cultura de datos lo suficientemente sólida que permita generar una verdadera respuesta por parte de la población.

De las entrevistas realizadas, solamente en una, la que se realizó a un ciudadano salvadoreño que llegó a España con su familia en 2021, hubo un esfuerzo de reflexión sobre las posibles consecuencias negativas de la extracción de datos personales. A las preguntas «¿Cómo te hubiera gustado que hubiera sido el proceso de recolección datos personales?» y «¿Cuál sería tu preferencia con relación a dar o no dar datos personales?[44]» la persona respondió que efectivamente había información muy sensible que

[43] Ver anexo II.
[44] Ver anexo II.

él hubiera preferido no aportar al momento de solicitar el asilo, pero además aseveró la preocupación de no saber en dónde podía terminar sus datos y los de su familia. En su caso, el temor se debía a la persecución y violencia que había sufrido en su país de origen. La diferencia en este caso fue la profesión del entrevistado, que ejercía como informático en su país de origen.

En la dinámica del extractivismo de datos, hay poca posibilidad de que los datos recolectados sean borrados en el futuro. Muchas de las bases de datos, como Eurodac o PRIMES, estipulan un tiempo de almacenamiento de diez años, pero la probabilidad que después de ese tiempo los datos biométricos de esta población vulnerable desaparezcan resulta difícil de predecir debido a las múltiples vías de externalización que existen en el escenario digital. Sobre todo, teniendo en cuenta que los datos biométricos de agencias de ayuda humanitaria son susceptibles de caer en manos de terceros, como las empresas que crearon la tecnología o los gobiernos que ocasionalmente pueden tener acceso a esta información.

En la dinámica de estos tres agentes, los individuos pasan a un segundo plano, al igual que las reglas que establecen los derechos de los refugiados o el derecho internacional humanitario. Para los primeros, las agencias como ACNUR, el argumento de la eficacia en la gestión de la ayuda humanitaria no tiene una justificación coherente ni corroborable. En realidad, pareciera ser que la obtención de datos son una forma de rentabilizar el humanitarismo y rendir cuentas sobre sus actividades para la satisfacción de los donantes de los fondos[45]. Mientras que, para los segundos, es decir, los estados u organizaciones supraestatales, como la Unión Europea, los datos de refugiados sirven para restringir la libre circulación o directamente impedir el ingreso de población no deseada. Para los últimos, las empresas de tecnología, el juego del humanitarismo no es más que una actividad comercializable en el juego de la lógica capitalista[46].

4. La gobernanza algorítmica de refugiados

Kasapoglu, Masso y Calzati definen «gobernanza algorítmica» como una estrategia de poder y dominación que produce diferencias sociales al reproducir categorizaciones basadas en el

[45] Mirca Madianou, Jonathan Corpus Ong, Liezel Longboan, Jayeel Cornelio, «The Appearance of Accountability: Communication Technologies and Power Asymmetries in Humanitarian Aid and Disaster Recovery,» *Journal of Communication* 66, no. 6 (2016): 29.
[46] Madianou, «The Appearance of Accountability» 29.

procesamiento de datos cuyas consecuencias son proyectadas en determinadas poblaciones[47]. Esta conceptualización es particularmente interesante porque nace de una reflexión sobre las teorías de Foucault, es especial de su famoso seminario *Technologies of the self,* en el que acuña la noción de *governmentality* para explicar la relación entre las «tecnologías del poder», siendo estas aquellas que determinan el comportamiento de los individuos y los someten a estructuras de dominio, y las «tecnologías del ser», es decir, aquellas técnicas empleadas por cada persona para obtener determinado beneficio físico, mental o espiritual[48].

Estas consideraciones son fundamentales para los objetivos de esta investigación, ya que cuando hablamos acerca del uso de algoritmos en la categorización de población refugiada, ya sea para fines de lucro, para propósitos humanitarios o para el desarrollo de políticas fronterizas, nos encontramos precisamente ante una expresión más contemporánea de la *governmentality* de Foucault. La gobernanza algorítmica de los refugiados se produce a partir del uso de la tecnología que se emplea para la extracción, procesamiento y categorización automatizada de información privada que más adelante se utiliza para ejercer algún tipo de control o dominio. En el caso de la biometría, los algoritmos son la pieza clave porque permiten la estandarización de los rasgos faciales, dactilares u oculares que más tarde van a ser extraídos de los solicitantes de asilo.

Este concepto servirá para entender los siguientes capítulos. Primero, para entender cómo la gobernanza algorítmica encuentra sus límites en los marcos normativo-jurídico nacionales e internacionales que protegen los derechos fundamentales de la privacidad y el olvido. Segundo, para comprender la relación fundamental que tiene el gobierno a partir de los algoritmos en el contexto contemporáneo de la poscolonización, sobre todo en lo que concierne al concepto de «tecno-colonialismo». En este último se retomará la gobernanza algorítmica para explicar las expresiones de discriminación y criminalización que se manifiestan a través de las estructuras de poder y las dinámicas de control en las políticas de datos.

[47] Tayfun Kasapoglu, Anu Masso, and Stefano Calzati, "Unpacking Algorithms as Technologies of Power: Syrian Refugees and Data Experts on Algorithmic Governance," *Digital Geography and Society* 2 (2021): 1.
[48] Tayfun «Unpacking Algorithms as Technologies of Power,» 2.

CAPÍTULO II

EL DERECHO EN LOS PREDIOS DE LA ERA DIGITAL

Para entender la repercusión del uso de algoritmos en la extracción de datos de poblaciones vulnerables, como es el caso de los solicitantes de asilo es necesario tener en cuenta los aspectos legales que son determinantes en la defensa de los derechos humanos. Para examinar esta cuestión, es fundamental atender a las normas que se han establecido en el nuevo contexto digital, así como el estado actual de los tratados y leyes que defienden la figura del refugio. También, es necesario estudiar detenidamente lo recientemente trabajado en relación con la protección de datos, sobre todo en el entorno europeo.

Por un lado, los derechos digitales. Como se explicará más adelante, se trata de una cuestión poco desarrollada, no porque haya una falta de intención, sino por el vertiginoso avance de la tecnología digital en las últimas dos décadas. También, no sería apresurado sostener que existe una presión por parte de los gigantes tecnológicos para mantener el *estatus quo* que los sostiene, es decir, pocos impuestos y poca regulación.

Por otro lado, en cuanto al derecho de asilo, sí existe un corpus robusto y bastante amplio. Desde tratados internacionales, hasta regulaciones internas de cada país. No obstante, a pesar de este escudo legal, en los últimos años—sobre todo a partir de los atentados del 11 de septiembre de 2001–, existe un esfuerzo por parte de los países más desarrollados de evitar el ingreso de población refugiada proveniente del sur global. Detrás de las múltiples violaciones al derecho internacional de los Derechos Humanos, se esconden justificaciones racistas, xenófobas y nacionalistas, que usualmente abanderan los no tan nuevos partidos de ultraderecha.

En el caso concreto de la Unión Europea, estos ámbitos presentan un notable avance. Por un lado, el artículo 18[49] de la Carta de Derechos Fundamentales de la UE rescata, haciendo eco a lo establecido en la Convención de Ginebra, su Protocolo, y en el Estatuto de Refugiados, el derecho del asilo. Por otro lado, en su artículo 8[50], establece que toda persona tiene derecho a la protección de sus datos personales, así como a poner los límites en el uso de estos. En este sentido, el club comunitario ha

[49] European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2000/C 364/12
[50] European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2000/C 364/10

sido un referente en cuanto a legislación de protección de información personal en lo referente al Reglamento General de Protección de Datos (RGPD).

No obstante, como se ha revisado en el primer capítulo, la evidencia en el uso de algoritmos para la extracción de datos biométricos sugiere que, en el espacio europeo, existe una creciente dificultad para los solicitantes de asilo para entrar y circular libremente por el espacio comunitario. Mientras que las fronteras interiores no existen para los ciudadanos, para quienes llegan como refugiados salir del país de acogida pone en peligro sus permisos de refugio. Como varios autores se esfuerzan en señalar, no solo a la entrada, sino también durante la estadía, los refugiados son criminalizados y puestos bajo una estricta vigilancia[51]. Los fallos en estos dos ámbitos legales crean un coctel pernicioso para quienes se atreven a entrar en el territorio de la Unión Europea y solicitar asilo.

1. El concepto jurídico-normativo del refugio

Según los datos más recientes de ACNUR, en el mundo existen 89,3 millones de personas desplazadas. De estos, 27,1millones son personas refugiadas, mientras que 53,2 millones son población desplazada interna y 4,6 millones son solicitantes de asilo. Curiosamente, el 83% de estas personas son acogidas en países de renta baja o media, contrariamente a lo que se suele creer. Turquía, Colombia y Uganda encabezan la lista de los países que más refugiados han acogido hasta el momento[52]. El aumento de esta cifra se debe al incremento de las hambrunas, de las guerras, la violencia interna y la pobreza que sufren los países del sur global. Como recuerda Galtung, detrás de este desastre humanitario se encuentran graves desequilibrios sociales que se traducen en una violencia estructural rampante en todo el mundo[53].

A partir de los desastres que ocasionaron los conflictos bélicos en la primera mitad del siglo XX, ha existido un esfuerzo por regular los derechos fundamentales intrínsecos al ser humano. El Derecho Internacional Humanitario y el Derecho Internacional de los Derechos Humanos se han encargado de nutrir los derechos que protegen a los asilados.

[51] Ver capítulo 3, apartado 2: Los refugiados como sujetos de datificación
[52] «Datos básicos,» ACNUR, https://www.acnur.org/datos-basicos.html
[53] Vicente Hueso, «Johan Galtung. La Transformación de Los Conflictos Por Medios Pacíficos,» *Cuadernos de Estrategia* 111 (2000): 130.

En 1951, apenas seis años después del fin de la Segunda Guerra Mundial, la recién formada Organización de Naciones Unidas en la Convención de Ginebra elaboró y firmó el Estatuto de los Refugiados, un tratado internacional que tiene como objetivo dotar de derechos a las personas que, por motivo de persecución, se veían en la obligación de solicitar asilo en un tercer país.

Lo curioso de este encuentro fue la intención por la cual se reunieron los países que formaban la ONU. El Estatuto de los Refugiados fue creado, en primera instancia, por y para ayudar a los desplazados europeos que huían de los horrores de la guerra. Es más, el propio documento original define a un refugiado como:

> «[Una persona que debido a los]…acontecimientos ocurridos antes del 1.º de enero de 1951 y debido a fundados temores de ser perseguida por motivos de raza, religión, nacionalidad, pertenencia a determinado grupo social u opiniones políticas, se encuentre fuera del país de su nacionalidad y no pueda o, a causa de dichos temores, no quiera acogerse a la protección de tal país; o que, careciendo de nacionalidad y hallándose, a consecuencia de tales acontecimientos, fuera del país donde antes tuviera su residencia habitual, no pueda o, a causa de dichos temores, no quiera regresar a él»[54].

Conocer el argumento inicial del estatuto de refugiado es importante para entender las contradicciones que ocurren en los desplazamientos contemporáneos. Mientras que Europa occidental se ha alejado de la violencia de su pasado, ahora los refugiados son las personas que llegan huyendo de las guerras y el hambre causadas por los conflictos que las potencias coloniales provocaron en un principio. No obstante, 70 años después de que el mundo presenciara las grandes diásporas europeas, son los descendientes de estos mismos los que se esfuerzan en poner trabas para ayudar a los más vulnerables.

A pesar de que el concepto de refugio cambió a partir del Protocolo sobre el Estatuto de Refugiados de 1967, en el cual se ampliaron las bases geográficas y temporales del protocolo inicial– y que existe una sólida base legal que ha servido para crear una importante jurisprudencia–, en los últimos años la evidencia indica un notable incremento en las violaciones o impedimentos al derecho de asilo. Por más que los conceptos que nutren el derecho de los refugiados sean claros, la intención política de respetarlos es muy pobre.

Como sostiene Rodríguez-Villasante, en la actualidad existe una abundancia de tratados y legislación interna que defienden a los solicitantes de asilo. Por lo tanto, se ha de suponer que el problema no

[54] Asamblea General de las Naciones Unidas, *Convención sobre el Estatuto de los Refugiados*, 28 de julio de 1951, Serie de Tratados de las Naciones Unidas, vol. 189, pág. 2.

radica en una falta de reglas, sino en la voluntad política de los gobiernos para aplicarlas y hacerlas efectivas. Esta observación no podría ser más precisa, si tenemos en cuenta las constantes infracciones de los derechos de los solicitantes de asilo por parte de países firmantes[55].

Como veremos más adelante, la discriminación que impera en el uso de algoritmos en fronteras no es casualidad. Detrás de esta tendencia yace una discriminación estructural que trastoca todas las políticas fronterizas. La criminalización en los procesos migratorios no es nueva, sino que se lleva cultivando desde hace varias décadas. Por ello, no sorprende observar el mismo patrón en la frontera sur europea con el empleo de herramientas biométricas para evitar la entrada de más refugiados.

Esta falta de intención que defiende Rodríguez-Villasante es evidente, por ejemplo, en los países mediterráneos como Grecia, España o Italia. A pesar de las obligaciones que establece el Tratado de Dublín, la práctica sugiere que, en el caso de estos países mediterráneos, existe un notable esfuerzo, a través de herramientas tecnológicas, por evitar el ingreso de solicitantes de asilo[56]. Por ejemplo, en el caso de España, existe un esfuerzo por «impermeabilizar» las fronteras externas de la Unión Europea, a través de una externalización de las políticas fronterizas con los acuerdos de «buena vecindad», como es el caso con Marruecos. También, con el objetivo de desincentivar la migración legal o la recepción de solicitudes de asilo, las autoridades fronterizas incurren en mecanismos de devolución o retención[57].

El Tratado de Dublín no es el único que garantiza los derechos de las personas refugiadas. En el contexto europeo, y por ende, el español, es importante rescatar que la Carta de los Derechos Fundamentales de la Unión Europea estipula en su artículo 18 la garantía del derecho de asilo «dentro del respeto de las normas de la Convención de Ginebra de 28 de julio de 1951 y del Protocolo de 31 de enero de 1967 sobre el Estatuto de los Refugiados y de conformidad con el Tratado de la Unión Europea y con el Tratado de Funcionamiento de la Unión Europea»[58].

Es importante anotar que una parte de los solicitantes de asilo tienen conocimiento sobre los derechos fundamentales que los protegen. Uno de los entrevistados, procedente del Sahara Occidental, declaró

---

[55] José Luis Rodríguez-Villasante y Prieto «La protección de los refugiados y desplazados internos por el derecho internacional», en *Migraciones en el siglo XXI: riesgos y oportunidades: XXIV Curso Internacional de Defensa*, Academia General Militar (Zaragoza) (dir.), Universidad de Zaragoza (dir.) (Jaca, 2016), 1.

[56] United Nations Human Rights Council, Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial and Xenophobic Discrimination and the Use of Digital Technologies in Border and Immigration Enforcement*, New York, NY: UN Headquarters, 2021: 1–24.

[57] Virginia Rodríguez y Gonzalo Fanjul. *La industria del control migratorio ¿Quién gana en España con las políticas fronterizas de la Unión Europea?* Madrid: Porcausa, 2017: 11.

[58] European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2000/C 364/18.

estar consciente de su estatus migratorio y de las leyes nacionales y europeas que lo amparaban. Es más, su caso era particularmente interesante, dado que su lugar de procedencia no es reconocido como un estado independiente, menos aún después de los cambios en política extranjera entre España y Marruecos en cuanto al reconocimiento del Sahara Occidental. No obstante, se deben hacer dos aclaraciones. Por un lado, que los casos particulares no pueden generalizarse, ya que buena parte de la población refugiada llega a la Unión Europa sin conocer realmente los derechos que tienen e incluso, como algunos encuestados declararon, solo se enterar acerca de estos al momento de acudir a las autoridades migratorias. Por otro lado, el conocimiento sobre el marco normativo jurídico que los protege en cuanto a su condición de solicitante no se aplica en materia de derechos digitales. Como se verá a continuación, la materia en cuanto a esta cuestión aún se está desarrollando y no goza del debido conocimiento por parte de los usuarios de internet y menos aún de la población refugiada.

2. El nuevo contexto digital

La era digital es la materialización de lo que Zygmunt Bauman explicaba como modernidad líquida. La ruptura del mundo analógico y el desarrollo cada vez más rápido de la tecnología digital ha resultado en un cambio de paradigma en cuanto a la percepción subjetiva de la ciudadanía[59]. Tomando el pensamiento de Bauman como punto de partida, nuestra cotidianidad viene perdiendo los elementos «sólidos» que la caracterizaban, para adoptar nuevas costumbres más «gaseosas» o «etéreas». En la era de la globalización, lo digital ha encontrado el perfecto caldo de cultivo para desarrollarse.

En la nueva sociedad globalizada y tecno-digital, existe una escisión en el concepto de ciudadanía. Como acierta en señalar Arce, el «yo analógico» se contrapone al «yo digital», no sugiriendo con esto que exista un dominio del uno sobre el otro, sino un desdoblamiento. En este sentido, hay un cambio de paradigma en cuanto a la forma en que se ejerce la ciudadanía, así como los marcos legales, normativos y jurisprudenciales le dan forma en la sociedad[60].

La inteligencia artificial, a la que la ciencia ficción se encargó de dotarla de impresiones futuristas y analógicas, se desarrolla a través de una infraestructura «invisible». En esta nueva realidad, los datos personales se han convertido en una nueva materia prima y, por lo tanto, en una nueva fuente de riqueza. En esta nueva forma de mercantilización de datos, el *big data*, a través del desarrollo de algoritmos, ha conseguido la automatización en el procesamiento de esta información. En lo que atañe

[59] Carlos Arce Jiménez, *¿Una nueva ciudadanía para la era digital?* (Madrid: Dykinson, 2022), 14.
[60] Arce Jiménez, *¿Una nueva ciudadanía para la era digital?,* 15.

a la presente investigación, la capacidad para datificar de manera automática la información personal de millones de individuos adquiere un matiz peligroso si se emplea en población vulnerable, como es el caso de los refugiados. Cuestiones como el racismo, la discriminación y el extractivismo neocolonial son componentes que, en la nueva realidad digital, encuentran canales de amplificación.

Ya sea para el sector privado o para la administración pública, los algoritmos ya son parte de los mecanismos de gestión. Por ejemplo, empresas como Oracle o Microsoft ofrecen herramientas de CRM que se encargan, a través de determinados algoritmos, de agilizar las relaciones comerciales con clientes[61]. Para las instituciones públicas, los algoritmos son el *modus operandi* sin los cuales el trabajo burocrático sería insostenible.

Sin embargo, no es posible afirmar que las herramientas algorítmicas son neutras, en el sentido que trabajen de manera objetiva e imparcial. De acuerdo con Dencik y Sánchez Monedero, existen cuestiones estructurales que influyen en la elaboración y puesta en marcha de esta tecnología, ya sea por el fin que se persigue con su implementación, como por prejuicios, la presencia de sesgos en datos o la falta de participación de las comunidades afectadas en el proceso de diseño[62]. Es más, los autores defienden recuerdan que, según el *framework algorithmic ecology*, los algoritmos están diseñados para operativizar las ideologías de las instituciones de poder y, de esta manera, producir el impacto deseado sobre determinadas comunidades[63]. La noción de justicia con la que ambos trabajan ayuda a repensar las metodologías de las ciencias computacionales y de la ingeniería de software, de manera que se les imprima una dimensión más socio técnica[64].

Como señala Arce Jiménez, en el caso de las políticas fronterizas y de los refugiados es importante tener en cuenta los prejuicios, las percepciones y las opiniones personales de quienes elaboran el producto, pero también de quienes lo compran ya que pueden ser la causa de una aplicación parcializada. En otras palabras, en la puesta en marcha de los algoritmos, no debe sorprender que estos estén contaminados por cuestiones raciales, que en última instancia son aplicados a población vulnerable que sufren la exclusión social y racial en las fronteras[65].

[61] Ver capítulo 1, apartado 2: PRIMES.
[62] Dencik, Lina, and Javier Sanchez-Monedero. 2022. «Data justice». *Internet Policy Review* 11 no.1 (2022): 7.
[63] Dencik «Data Justice,» 7.
[64] Dencik «Data Justice,» 8.
[65] Carlos Arce Jiménez, *¿Una nueva ciudadanía para la era digital?* (Madrid: Dykinson, 2022), 75.

En su informe de 2021, la Relatora Especial sobre racismo y la discriminación racial de la ONU sostiene que no solo la tecnología no es neutral, sino que su diseño y uso refuerza tendencias sociales, políticas y económicas dominantes[66]. Es más, el propio informe recuerda que, en el caso de inmigrantes, refugiados y desplazados, la biometría tiende a incrementar la discriminación racial. Este también sería el caso para persona afrodescendientes, indígenas, minorías étnicas y cualquier población susceptible de ser racializada.

Las mismas inquietudes existen en lo que concierne al *big data*. McDonald describe el caso de la epidemia de ébola de 2014 como un ejemplo de mala práctica en el procesamiento datos personales a través del uso de *big data*—mediante el llamado *Call Detail Record*—para supuestamente mejorar la respuesta humanitaria, pero sin tener en cuenta los riesgos en materia legal[67]. Es más, en una de las peores emergencias sanitarias previas al estallido de la Covid-19, la respuesta internacional no solo fue inadecuada, sino que se evidenció la total carencia o indiferencia de las leyes que supuestamente debieron proteger a la población afectada del afán extractivista que se llevó a cabo sin ninguna consideración a los derechos fundamentales[68].

En el caso de las políticas migratorias, Ajana afirma que la aplicación de estrategias con *big data* en fronteras no se limita a una cuestión de tecnología de datos únicamente, sino que sugiere una transformación del concepto mismo de frontera en cuanto que los límites de los estados están externalizados y en donde los sistemas de control se puedan encontrar[69]. En este sentido, la explicación de la autora calzaría bien con la Unión Europea ya que el control migratorio se mueve fuera de la frontera y se ubica en un plano supraestatal. Es más, el *big data* y sus herramientas analíticas son una de las nuevas tecnologías que se están implementando cada vez más rápido para conseguir formas más sofisticadas de monitorear el movimiento y vigilar a individuos que son percibidos como peligrosos o no deseados[70]. De forma similar advierten Metcalfe y Dencik en cuanto a la aplicación de «fronteras datificadas» como un mecanismo para crear una lista negra de «migrantes ilegalizados» no deseados y

---

66 United Nations Human Rights Council, Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial and Xenophobic Discrimination and the Use of Digital Technologies in Border and Immigration Enforcement*, New York, NY: UN Headquarters, 2021: 4.

67 Sean Martin McDonald, «Ebola: A Big Data Disaster - Privacy, Property, and the Law of Disaster Experimentation,» *The Centre for Internet and Society*, no. 2016.01 (2016): 12.

68 McDonald, «Ebola: A Big Data Disaster» 48.

69 Btihaj Ajana, «Augmented Borders: Big Data and the Ethics of Immigration Control,» *Journal of Information, Communication and Ethics in Society* 13, no. 1 (2015): 5-6.

70 Ajana, «Augmented Borders,» 5-6.

como un sistema rígido de control de movimientos que también alienta un clima de deportación arbitraria.

En este sentido, como señalan las recomendaciones del Comité para la Eliminación de la Discriminación Racial, el uso cada vez más extendido de las nuevas herramientas tecnológicas, incluida la inteligencia artificial, en áreas como seguridad, control de fronteras y acceso a servicios sociales, tiene el potencial de profundizar el racismo, la discriminación racial, la xenofobia y otras formas de exclusión[71]. En el caso de la política fronteriza de la Unión Europea, la evidencia sugiere que el trinomio empresas, estados y agencias, explicado en el capítulo anterior, funciona como un excelente conductor en el que se perpetúan los prejuicios raciales de los refugiados.

Teniendo en cuenta este contexto, el derecho ha intentado ponerse al día en la carrera tecnológica, aunque cabe recalcar la dificultad que ello supone considerando la velocidad con la que se están desarrollando nuevas y mejores herramientas. La dificultad no solo se haya en el uso de la biometría como amplificador de ideas que incentivan la discriminación, sino también en el hecho de que existen muchos actores de por medio. La responsabilidad no se puede diluir en justificaciones basadas en las externalidades que pueden causar las tecnologías, sino que debe ser atribuida tanto a las empresas privadas que las fabrican, como a los estados que pagan por ellas, sin olvidar a las agencias que también retroalimentan este mercado. En este sentido, en los tratados, leyes y normas debe existir la posibilidad de una reparación justa para aquellas personas que han sufrido una vulneración de sus derechos[72].

Antes de enumerar los derechos específicos que debemos contemplar cuando hablamos de algoritmos en contextos de migraciones, es importante comprender que el marco jurídico normativo de los derechos digitales abarca otros temas relacionados de manera indirecta con este tema. Cuestiones relacionadas con la protección de datos personales como el derecho a la intimidad, el derecho al olvido, etc. se llevan trabajando desde hace décadas, sobre todo en lo que concierne a la protección de los usuarios de internet. Pero también existe un debate interesante en lo que respecta al derecho a la libre expresión en la nueva realidad digital, cuestión intrínsecamente unida con el delito de odio «online» que ha encontrado un espacio prominente en los estudios de comunicación.

[71] United Nations, *Racial and Xenophobic Discrimination and the Use of Digital Technologies*, 9.
[72] Arce Jiménez, *¿Una nueva ciudadanía para la era digital?,* 76.

2.1. Los derechos fundamentales en la era digital

Luego de dar un primer esbozo acerca de los derechos de los refugiados en el escenario europeo y de abordar las preocupaciones inherentes de la era digital, es necesario estudiar algunos derechos fundamentales que, por su valor intrínseco, protegen a los ciudadanos de las consecuencias que podría acarrear la difusión de información privada a través de los medios digitales. Más aún si hablamos de personas refugiadas que sufren las consecuencias de la extracción y procesamiento de datos personales.

El derecho a la intimidad, el derecho al olvido y el derecho al honor, los tres recogidos en la Declaración Internacional de los Derechos Humanos y en la mayoría de las constituciones de países democráticos, son las salvaguardas más importantes a la hora de proteger el ámbito privado de los individuos. Son de ineludible cumplimiento en la esfera internacional sin excluir a ninguna persona, sin importar el estatus migratorio.

En lo que atañe a la presente investigación, estos derechos son de obligada observación cuando analizamos la protección internacional que gozan los solicitantes de asilo en cuanto a la salvaguarda de su integridad en el proceso de extracción de datos, en particular aquellos que lo hacen en territorio europeo. Por los motivos que hasta ahora se han expuesto, los procesos de recepción de refugiados pueden carecer de las protecciones más fundamentales. En algunos casos, se producen detenciones temporales y la dilación de las respuestas pueden ser muy prolongadas, lo que produce el empeoramiento de una población que de por sí ya es vulnerable.

Por los límites de esta investigación, los dos apartados siguientes se desarrollarán de manera sucinta, pero respondiendo a tres ámbitos: el ordenamiento jurídico internacional, el europeo y el español. Los motivos de esta selección obedecen al muestreo poblacional que, a lo largo del trabajo, se ha ido exponiendo. Con esta explicación se desea entrever que los derechos fundamentales que arropan a la población refugiada ameritan una revisión para adaptarlos a la nueva realidad digital.

2.1.1. Derecho a la intimidad

El derecho a la intimidad es el derecho inherente de toda persona de tener una vida privada sin la intromisión no consentida de terceros. En uno de los artículos más famosos sobre este asunto, *The right of privacy* de S. Warren y L. D. Brandeis, publicado en 1890, se recogen los fundamentos por los que se debe proteger la intimidad de los individuos. En pocas palabras, los autores lo resumieron en una célebre frase: el derecho a la privacidad es el derecho a estar en paz (the right to be let alone).

El artículo sentó una base importante, en el contexto del creciente poder que estaba ganando la prensa amarillista de Pulitzer y Hearst. Más de un siglo después, el derecho a la intimidad se haya en un momento de profunda transformación debido al vertiginoso ascenso de las tecnologías de la información y comunicación. En la actualidad, el ámbito exclusivamente privado ha dejado de existir, ya que las nuevas tecnologías son capaces de extraer y compartir datos personales en cuestión de segundos.

Esto sugiere una drástica reconfiguración de conceptos. Como sugiere Martínez Pinzón, las nociones de vida privada e intimidad se deben adaptar a las nuevas necesidades de una sociedad inmersa en el desarrollo y cambio tecnológico. En este sentido, hay tres cuestiones que se deben tener en cuenta: primero, la existencia de espacio, en cuanto al dominio que un individuo tiene de su esfera íntima; segundo, la necesidad de protección, es decir, los límites que no permitan transgredir de manera arbitraria ese espacio; y, en tercer lugar, la capacidad para decidir. Esta última idea es importante porque radica en la idea de que ya no basta con una interpretación pasiva del derecho a la intimidad, sino a una acción proactiva, que sería el control en la gestión de la esfera privada y la información personal[73].

Sobre el derecho a la privacidad existe abundante materia a nivel internacional, pero también comunitario y estatal. Como rescata el documento de la Declaración Universal de los Derechos Humanos, «nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia»[74]. Así mismo, en el mismo artículo, la carta magna sostiene que cualquier persona tiene derecho a la protección de leyes que garanticen la no injerencia en su ámbito privado.

A nivel europeo, la Convención Europea de Derechos Humanos recoge en su artículo 8 el derecho a la intimidad personal y familiar. No obstante, también admite excepciones cuando se trata de cuestiones de seguridad, lo que abre la puerta a una interpretación que va desde restricciones internas, como es el caso de la ley mordaza en España, hasta políticas restrictivas en las fronteras exteriores e interiores de la Unión Europea.

En el ordenamiento español, existe una protección constitucional de la intimidad recogida en los artículos 18 y 20 de la carta magna, que, además garantiza el límite en el «uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus

[73] José Martínez de Pisón, «Vida privada sin intimidad. una aproximación a los efectos de las intromisiones tecnológicas en el ámbito íntimo,» *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos* no 37 (2017): 57.
[74] Asamblea General de las Naciones Unidas. *Declaración Universal de los Derechos Humanos* (1948). art. 18

derechos»[75]. Las leyes también son explícitas al respecto. En el código penal la intimidad goza de protección a través del artículo 197, que para fines de esta investigación es importante recordar que sanciona el apoderamiento de datos reservados de carácter personal de ficheros o soportes técnicos. Por ejemplo, habría que tener en cuenta el uso que se le da a los datos personales en las administraciones públicas y hasta qué punto esa información es conservada en el tiempo.

Así mismo, la ley civil, a través de la ley orgánica 1/1982, protege el derecho a la intimidad, honor y a la imagen propia. Sobre todo, en el Art. 1.2 se recogen los parámetros de la intimidad y hasta que punto esta puede ser compartida a través del consentimiento de un individuo, mientras que el Art. 2.1 recoge que la protección civil del honor deberá atender a la ley sobre protección de la intimidad y también los usos sociales.

Estas cuestiones del ordenamiento jurídico son claras en la dimensión analógica. Pero si las trasladamos a la esfera digital, existen dificultades a la hora de su aplicación En la nueva dimensión de la privacidad que se exponía antes, el derecho está llamado a encontrar los límites de la intervención de la tecnología y proteger no solo el ámbito físico, sino también el digital, que es donde fluye el tráfico de datos privados. No es tarea fácil ya que Internet ha supuesto la ruptura del control de la información personal y ha trastocado la gestión de los datos personales que se extraen en diversas plataformas. El ejemplo por excelencia son las redes sociales, como Facebook o Instagram, pero los datos de carácter personal son absorbidos y reutilizados constantemente por buscadores como Google, que rentabiliza la información de sus usuarios a través de las estrategias del marketing digital o en las aplicaciones de automatización de funciones empresariales.

El desdoble del «yo analógico» del «yo digital», que citábamos más arriba, sugiere que mientras en el mundo físico o analógico las demandas de privacidad se mantienen, en la esfera digital no existe una suficiente concientización de la importancia de salvaguardar los datos de carácter personal[76]. En la cotidianidad, buena parte de la población consiente que se extraigan sus datos y se guarden a través de determinados algoritmos que persiguen intereses comerciales. En esta nueva forma de entender la noción de intimidad, es necesario pensar en nuevas herramientas legales que garanticen la protección de esta.

[75] Constitución española (BOE núm.311, de 29 de diciembre de 1978). art. 18.
[76] Arce Jiménez, *¿Una nueva ciudadanía para la era digital?,* 92.

Si para la sociedad europea es difícil comprender este nuevo universo digital, las poblaciones vulnerables, como los refugiados, tienen escasa comprensión de lo que implica la extracción de sus datos personales en frontera. En los análisis de casos, buena parte de los encuestados no tienen un conocimiento claro del paradero de los datos privados que se les solicitaron a su llegada a la Unión Europea. Esos datos no solo quedan registrados por un periodo mínimo de diez años, sino que son susceptibles de ser sustraídos por las empresas tecnológicas que brindan la tecnología para la extracción de información biométrica.

2.1.2. El derecho al olvido

En el ordenamiento jurídico español, el derecho al olvido está garantizado, pero cuando se trata de la esfera digital, aún falta una mayor jurisprudencia. En el caso emblemático de Google Spain v. Agencia Española de Protección de Datos el fallo del Tribunal de Justicia de la Unión Europea a favor del segundo sentó un precedente importante[77], ya que se trató del primer reconocimiento del derecho al olvido online. Google Spain no solo estaba obligada a remover información a solicitud del denunciante (el señor Coteja González), sino que debía, conforme a lo establecido en la normativa europea, tomar todas las medidas necesarias para eliminar la información duplicada en otros medios. Pero lo más interesante es la reafirmación del principio de territorialidad de la norma: si Google Spain radicaba y operaba desde España, debía acogerse a las leyes del estado y de la comunidad europea.

La Unión Europea garantiza el derecho al olvido a través de la RGPD (Reglamento 2016/679). En su artículo 17, la ley comunitaria respalda la decisión de un individuo que desee eliminar información personal de cualquier tipo de «controlador», entendiendo por controlador a un motor de búsqueda como una base de datos. Incluso, la norma va mucho más lejos, exigiendo al controlador inicial que tome «medidas razonables» para eliminar la información personal que haya sido transferida o publicada por un tercer controlador, cuestión interesante si se complementa con lo explicado en el apartado acerca del trinomio empresas, agencias y estados[78].

A pesar de estos avances, varios investigadores han subrayado su escepticismo con la posibilidad de los solicitantes de asilo puedan realmente eliminar sus datos personales de los bancos de información. Aunque sí es verdad que en teoría existe una fecha de expiración de los datos, en la práctica es muy

[77] Hay que anotar que la Directiva 95/46 que se utilizó para dirimir el pleito quedó derogada al entrar en vigor el Reglamento 2016/679 del Parlamento Europeo.
[78] Ver capítulo 1, apartado 1.3: empresas, agencias y estados: el trinomio de la discriminación.

complejo eliminar información que probablemente ha pasado por diversas manos. Así, como afirma Madianou, la infinita replicabilidad de los datos a través de *blockchain* eleva una justificada preocupación acerca de quién es el dueño de la información extraída y, por lo tanto, la garantía de la persona a ser olvidada. Es más, no existe una real certeza de que los usuarios sepan cuales el destino final de su información.

Las entrevistas que se realizaron también abordaron esta cuestión al hilo del consentimiento informado. A la pregunta «¿Conoces o sabes que en la Unión Europea existe una normativa que protege los derechos de datos personales?», la mayoría de las respuestas eran positivas. Los encuestados sabían que la RGPD protege su información privada y aceptaron entregarla voluntariamente, incluidos algunos datos biométricos. Es importante hacer este contraste ya que el hecho de que en muchos casos no haya conocimiento específico sobre la complejidad tecnológica de los procesos y herramientas de extracción de datos, no implica que se ignore el marco normativo jurídico que los protege.

3. Los nuevos debates jurídico-normativos de la era digital

Lo que se ha explicado hasta el momento está relacionado con el esfuerzo por adaptar algunos derechos fundamentales que, para los propósitos de esta investigación, son de obligada observación y reconfiguración para mantener su vigencia y la obligatoriedad de su cumplimiento en un contexto de acelerados cambios. Cuando hablamos de población refugiada, como es el caso de los solicitantes de asilo, no podemos dejar de lado el escenario de vulnerabilidad al que se enfrentan.

Sin embargo, también es importante abordar algunos temas que son fundamentales en la era digital y que atañen de manera directa a los derechos de la población refugiada. A continuación, se proponen dos cuestiones: el debate en torno al discurso de odio online y el desarrollo de la legislación de protección de datos. Ambas discusiones responden a uno de nuestros argumentos centrales: el uso de las herramientas de extracción de información personal y datos biométricos puede acarrear graves riesgos para los derechos fundamentales de la población refugiada.

3.1. El discurso de odio online

La desinformación y las *fake news* no son fenómenos nuevos en la historia. A finales del XIX, el debate sobre la privacidad y el derecho a la intimidad, que desarrollábamos en el anterior apartado, surgió a partir del daño que ocasionaban los tabloides de la prensa amarillista que generó indignación por la

publicación incendiaria y falsa sobre determinados personajes de la época. Lo que resulta novedoso en la era contemporánea es que las noticias falsas han encontrado en las tecnologías de la información y comunicación las herramientas idóneas para viralizarse.

El uso de la biometría para generar contenido falso es también un problema en sí mismo. Este sería el caso de las *deep fakes,* contenido falso que se crea de manera automática a través de la inteligencia artificial[79]. De hecho, ya existen varios casos en los que a través de herramientas biométricas se utilizan los rostros y voces de terceras personas para crear contenido audiovisual falso que persiga un interés determinado. El problema de esta cuestión en concreto es que rastrear la fuente del contenido falso es extremadamente difícil.

Los actores extremistas detrás de las MDH (misinformation, disinformation and hate speech) tienen una especial apetencia por poblaciones vulnerables, las cuales son utilizadas de forma programática y perversa para alimentar discursos infundados y alterar los sistemas políticos, sobre todo, pero no únicamente, de los países democráticos[80]. En este contexto, el uso de las herramientas de extracción de datos, como la biometría, suponen un riesgo para la seguridad de la información personal de millones de refugiados. Como acierta en afirmar el Comité Internacional de la Cruz Roja, el uso indiscriminado de herramientas biométricas para la recolección de datos puede ser un problema en estos contextos porque la información recogida puede caer fácilmente en actores que sin ningún reparo las pueden utilizar fuera de contexto[81].

Hay ejemplos concretos del uso inflamatorio y tergiversado de la información relacionada con población refugiada a través de las tecnologías y algoritmos de las redes sociales. En el año 2015, durante la mal llamada «crisis migratoria europea», las redes sociales se convirtieron rápidamente en difusores de contenido marcadamente xenófobo contra los más de un millón de refugiados sirios. En el caso concreto de Alemania, el país que recibió la mayor cantidad de solicitudes de asilo, las plataformas de Facebook y Twitter sirvieron como espacios para la libre circulación de mensajes discriminatorios en contra de los nuevos inmigrantes. Esta situación se agravó aún más luego de que

[79] Saman Rejali and Yannick Heiniger, «The Role of Digital Technologies in Humanitarian Law, Policy and Action: Charting a Path Forward,» *International Review of the Red Cross* 102, no. 913 (2020): 9.
[80] Rejali «The Role of Digital Technologies,» 9.
[81] Delphine van Solinge and Massimo Marelli, "Q&A: Humanitarian Operations, the Spread of Harmful Information and Data Protection," *International Review of the Red Cross* 102, no. 913 (2020): 30-31.

se produjeron casos de violencia contra mujeres en la ciudad de Colonia y el atentado de Berlín del año 2016.

La proliferación de mensajes xenófobos en redes sociales tuvo claras implicancias políticas en el país germano. En el año 2017, el partido de extrema derecha, Alternative für Deutschland (FDA), consiguió el 12,6% de los votos en las elecciones parlamentarias.[82] En consecuencia, en junio del mismo año, el Bundestag aprobó el Network Enforcement Act (NEA), cuyo propósito fue detener la propagación de *fake news*, sobre todo de aquellos mensajes cuyo contenido presentaba evidencia innegable de discurso de odio. A pesar de que sus detractores argumentaron el peligro de esta ley para el derecho fundamental de la libertad de expresión, la NEA alemana supone un caso paradigmático para comprender la construcción de un nuevo marco legal que defienda a los usuarios en medios online.

En materia jurídica, definir el discurso de odio online supone un reto importante, más aún cuando nos referimos a un contexto tan complejo como el escenario virtual, en donde la regulación vigente es muy insipiente. Sin embargo, el crecimiento exponencial de mensajes con contenido ilegal en plataformas como Facebook y Twitter obliga a insistir en la necesidad de construir un marco legal que sirva para evitar una mayor proliferación de contenido xenófobo o racista.

A pesar de que en la UE no existe una ley penal en contra del discurso de odio online, la decisión marco 2008/913/JAI del Consejo de la Unión Europea, relativa a la lucha contra determinadas formas y manifestaciones de racismo y xenofobia mediante el derecho penal (ahora en adelante, Framework Decision), sirve para obtener una definición relativamente adecuada del discurso de odio, el cual se describe como:

> «[A] public incitement to violence or hatred directed against a group of persons or a member of such a group defined on the basis of race, colour, descent, religion or belief, or national or ethnic origin»[83].

Así mismo, cabe destacar que el año 2016 la Comisión Europea adoptó un Código de Conducta para contrarrestar el discurso de odio ilegal online (en adelante, CoC), el cual tiene el propósito de frenar el crecimiento del discurso de odio en plataformas virtuales. Si bien no tiene carácter obligatorio, el

[82] Sylvia Jaki y Tom De Smedt, «Right-wing German Hate Speech on Twitter: Analysis and Automatic Detection» University of Antwerp, (2018), 1.
[83] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.

CoC se ha convertido en una herramienta que sirve como una "guía" para las principales empresas de servicios tecnológicos como Facebook, Twitter, YouTube y Microsoft.[84] Como señala la CoC:

> «The IT Companies underline that the present code of conduct is aimed at guiding their own activities as well as sharing best practices with other internet companies, platforms and social media operators»[85].

Este último se trata del esfuerzo más contundente de la Unión Europea hasta la fecha. No obstante, no deja de ser de carácter "voluntario", por lo que la CoC depende de la libre adopción por parte de las empresas IT (que se han adherido en buena medida) y por los países miembros de la UE. Por lo tanto, la CoC insiste en la necesidad de crear leyes nacionales que estén alineadas con el Framework Decision y cuyo contenido esté complementado con acciones orientadas a limitar el discurso de odio online en plataformas de redes sociales[86].

3.2. RGPD y la protección de datos a nivel europeo

El Reglamento General de Protección de Datos (RGPD) es una de las figuras legales más importantes en la protección de derechos digitales. Desde el 2018 lleva aplicándose como parte del reglamento europeo, tiempo durante el cual las empresas han ido adaptándose a las nuevas obligaciones y responsabilidades que tienen sobre el manejo de los datos personales de los ciudadanos comunitarios.

A pesar de que la Unión Europea ha sido pionera en el desarrollo de un marco jurídico-normativo que protege de manera integral la información personal, no deja de tener limitaciones. Como acierta en afirmar Paragi, el alcance geográfico de la RGPD es limitado, a pesar de que el Art. 4 sostiene que la aplicación del reglamento se extiende a todos los actores de la Unión Europea que mantengan actividades que incluyan extracción de datos sin importar el lugar. A simple vista esto debería bastar para que tanto empresas como estados respeten los datos personales de personas extracomunitarias. Pero la realidad es mucho más compleja, ya que el alcance territorial del reglamento es claramente limitado cuando hablamos del ámbito digital, además que la RGPD no es aplicable a organizaciones internacionales como la ONU o Cruz Roja[87].

---

[84] «Countering illegal hate speech online – Commission initiative shows continued improvement, further platforms join» European Commission, 19 January 2018, https://ec.europa.eu/commission/presscorner/detail/en/IP_18_261
[85] European Commission, *Code of conduct on countering illegal hate speech online,* 2016.
[86] European Commission, *Code of conduct on countering illegal hate speech online,* 2016.
[87] Beata Paragi, «Digital4development? European Data Protection in the Global South,» *Third World Quarterly* 42, no. 2 (2020): 4.

En este sentido, existe una preocupación justificada en la aplicación de herramientas biométricas para la extracción de datos personales de población vulnerable. En el caso de los refugiados, se entiende que la extracción de huellas dactilares, iris y rasgos faciales, así como también información de teléfonos móviles, información médica, historial familiar, entre otros datos, queda en un limbo legal. Lo que más llama la atención es que estas actividades se llevan a cabo en las propias fronteras de la Unión Europea, dentro del marco geográfico y personal en el que supuestamente sí debería aplicar la RGPD.

La RGPD, a pesar de ser pionera no es la única regulación que defiende datos personales. Según un estudio realizado por Open International y Cruz Roja, alrededor de 120 países tienen algún tipo de protección legal, mientras que 40 más están trabajando en conseguirlo. El problema, una vez más de carácter geográfico, es que los países en donde se realizan las operaciones de ayuda humanitaria o de donde provienen los refugiados no tienen ningún tipo de regulación que proteja a sus ciudadanos[88].

De igual forma, como se ha corroborado en el muestreo poblacional, no existen las condiciones necesarias para que se cumplan con los requisitos de consentimiento previo que exige la RGPD en su artículo 4[89]. Las personas refugiadas carecen de los medios para negar el consentimiento a la extracción de datos personales. Detrás de esta falsa impresión de consenso existe una asimetría de poder que permite a quienes ejercen el control de las fronteras, cumplir con sus objetivos.

3.3. Proposición No de Ley (PNL) sobre Derechos Humanos y Fronteras Inteligentes.

La aprobación de la Proposición no de Ley (PNL) sobre los usos de tecnología de reconocimiento facial y otros sistemas de reconocimiento biométrico en frontera marca un antecedente importante en la lucha por establecer límites concretos a las políticas fronterizas de la Unión Europea (y por tanto española) que autorizan el uso de herramientas biométricas con el objetivo de recoger datos de carácter personal de población migrantes y refugiada. Como bien explica esta propuesta, detrás del uso de estos mecanismos biométricos existe una lógica racial y discriminatoria.

[88] International Committee of the Red Cross (ICRC) and Privacy International, *The humanitarian metadata problem: "Doing no harm" in the digital era*, 2018, 38.

[89] «Aprobada una PNL para evitar sesgos y promover la transparencia en el uso de sistemas biométricos en la frontera sur,» Algorace, 5 de abril de 2022, https://algorace.org/2022/04/05/aprobada-una-pnl-para-evitar-sesgos-y-promover-la-transparencia-en-el-uso-de-sistemas-biometricos-en-la-frontera-sur/

Como reconoce un artículo publicado por AlgoRace, la PNL propuesta por Unidas Podemos exige al gobierno de coalición que establezca garantías técnicas que fiscalicen las herramientas de Inteligencia artificial que se utilizan en fronteras, sobre todo aquellas que, a través de la biometría, funcionan mediante el reconocimiento facial. En concreto la iniciativa busca limitar la discriminación en la que pueda incurrir el uso de esta tecnología, como en cuestiones de raza, género, edad, religión o nacionalidad[90].

El debate, que se produjo en la Comisión de Interior del Congreso, y tuvo como voceros a los diputados de UP, Ismael Cortes y Joan Mena, no deja de tener algunas limitaciones. Como acierta en señalar el equipo de AlgoRace, los sesgos de los algoritmos no se pueden eliminar al 100% ya que en la base de la construcción de estos existe una «fragante discriminación y criminalización que tiene como consecuencia un rechazo generalizado hacia la población migrante y racializada»[91]. En este sentido, la utilización de este tipo de tecnología en las fronteras no hace más que reforzar un estigma sobre la población refugiada.

Por lo expuesto en las investigaciones de otros autores, es posible argumentar que los factores discriminatorios de las herramientas algorítmicas se encuentran en sus propias programaciones. Sobre todo, si volvemos al hecho de que detrás de la construcción de los algoritmos y su aplicación se encuentran intereses particulares[92]. Como se explicará en el siguiente capítulo, la gobernanza algorítmica de los datos de refugiados obedece al mismo tiempo a las estructuras coloniales que aún existen en la forma de interacción entre los países de acogida y los países del denominado sur global. Ambas realidades separadas por la división abismal que define el pensamiento occidental moderno[93]**.** La combinación de las nuevas tecnologías y las bases coloniales preexistentes dan como resultado el concepto que Mirca Madianou ha acuñado como «tecnocolonialismo». Estudiar este concepto es fundamental para seguir construyendo el marco jurídico normativo que requiere la era digital.

[90] Algorace, «Aprobada una PNL,»
[91] Algorace, «Aprobada una PNL,»
[92] Ver capítulo 1, apartado 1.3: empresas, agencias y estados: el trinomio de la discriminación.
[93] Boaventura de Sousa Santos, *Una epistemología del sur: la reinvención del conocimiento y la emancipación social,* (México: siglo XXI Clacso, 2009), 168.

CAPÍTULO III

TECNOCOLONIZADOS: LA DATIFICACIÓN DE LOS REFUGIADOS

En las páginas anteriores se han expuesto los aspectos técnicos y legales de esta investigación. Con ello se ha intentado ofrecer al lector una radiografía lo más completa posible de la complejidad que afronta este tema. Por un lado, se han mencionado algunas herramientas biométricas que se vienen desarrollando para el tratamiento de datos de población refugiada. Por otro lado, se han estudiado las fuentes del derecho que limitan o deberían limitar su uso en determinados casos. Ambas cuestiones deben entenderse como parte integral de esta investigación, pero por sí solos no son suficientes para fundamentar sus objetivos.

En este sentido, para comprender de forma coherente la tesis de la gobernanza algorítmica, es necesario abordar el marco teórico que yace detrás de este fenómeno. Nuestra hipótesis defiende que detrás del procesamiento de datos de la población refugiada se encuentran mecanismos coloniales que, de manera directa o indirecta, provocan la discriminación y la criminalización de población vulnerable. En este contexto, es indiscutible que las garantías que defienden los derechos fundamentales de los refugiados, recogidos en el ordenamiento jurídico normativo internacional, como es el caso del derecho a la privacidad o al olvido, son violados de forma frecuente y sin las debidas repercusiones legales.

Así mismo, el objetivo de este capítulo es explorar algunos conceptos que se han mencionado a lo largo de esta investigación, como «extractivismo» o «datificación» con el propósito de examinarlos a través del «tecnocolonialismo», idea que a nuestro juicio permite explicar las prácticas de determinadas tecnologías. Estas nociones ya han sido trabajadas ampliamente por los autores de distintas disciplinas, por lo que se reitera el aspecto multidisciplinar de este trabajo. Así, cabe recalcar que la tesis del tecnocolonialismo parte de determinadas posturas de los estudios poscoloniales, cuestión sobre la que se hará énfasis de aquí en adelante.

1. El poscolonialismo y la permanencia de los imperios

En *Imperial Debris*, Ann Stoler defiende que, en los remanentes del periodo colonial –lo que ella denomina «las ruinas de los imperios»–, las estructuras de la discriminación y el racismo permanecen y se transforman de manera invisible. Para la autora, «existen remanentes que se escapan de la visión

inmediata, detritos que son difíciles de percibir, heridas íntimas que aparentan ser superficiales o transformaciones profundas de la geografía social que son denominadas de forma distinta»[94].

España tiene una larga tradición colonial, al igual que sus pares europeos. Si bien la relación con América Latina parece ser la más observada al respecto, no podemos obviar las «heridas íntimas» que dejó el imperio y que aún perviven en otras regiones como Filipinas o en países de África Occidental como Guinea Ecuatorial o el Sahara Occidental. Este último, es particularmente interesante por el reciente revuelo que ha creado el giro diplomático entre el gobierno español y marroquí. Uno de los entrevistados, ya citado anteriormente, afirmó en su entrevista que su estatus de refugiado tiene un carácter «especial» al tratarse de alguien que vive en un antiguo protectorado de España. Si bien esta idea podría observarse en tanto a su validez en materia legal, las subjetividades son también importantes de considerar cuando abordamos las motivaciones de los movimientos migratorios.

Esta idea es importante como punto de partida para entender la presencia de la colonización en el uso de las herramientas para la extracción de datos. La discusión acerca de la permanencia del periodo colonial debe incorporar los aspectos intangibles o involuntarios, como las reapropiaciones de las individualidades, los lugares o las relaciones. En palabras de Stoler, adentrarnos en los escombros de los imperios es pensar también en los reposicionamientos dentro del juego político internacional, en las jerarquías de poder que dominan las relaciones internacionales[95]. En este sentido, la realidad digital no escapa de la poscolonialidad, sino que se reconfigura y se desarrolla a partir de sus patrones particulares.

La continuidad de las estructuras de dominación puede tomar diversas formas, pero conserva los mismos errores del pasado: las relaciones basadas en la fuerza, la exclusión, la desigualdad, la falta de dignidad y la privación de derechos fundamentales[96]. En la actualidad, la mutación de la colonización ha encontrado en el sistema capitalista un nuevo canal a través del cual poder implantar sus infraestructuras de control y explotación. Sin embargo, la novedad es que los recursos ya no son solamente físicos, sino inmateriales, como es el caso de los datos personales, una nueva fuente de riqueza para empresas tecnológicas cuya materia prima es precisamente la información privada de los individuos.

[94] Ann Laura Stoler, «Imperial Debris : Reflections on Ruins and Ruination» *Cultural Anthropology* 23, no. 2 (2016): 200.
[95] Stoler, «Imperial Debris» 196.
[96] Stoler, «Imperial Debris» 211.

La supervivencia de las antiguas estructuras a lo largo de más de 500 años se entiende a través del concepto de «colonialidad del poder», acuñado por el sociólogo peruano Aníbal Quijano. Según el autor, las ideas de raza y clasificación social suponen el punto de partida de la creación de una infraestructura de poder eurocéntrica. La colonialidad del poder se basa en la estratificación racial, la cual explica la concentración del poder de productividad y del capital, así como la perpetuidad de los privilegios de quienes dominan la estructura de este poder, es decir, la población blanca euro descendiente[97]. Esta teoría, que parte de una perspectiva latinoamericana y que podría discutirse en otros contextos poscoloniales, permite entender los patrones históricos que se siguen repitiendo hasta la actualidad.

Una cuestión que también es importante de tener en cuenta es la transformación de los actores coloniales, en el sentido de que ya no nos encontramos ante el antiguo modelo de dominación imperial decimonónica. En el trinomio que existe entre las empresas privadas, las agencias internacionales y los estados nacionales[98], existe una dinámica de explotación reforzada por el sistema capitalista contemporáneo. En esta lógica, para las gigantes tecnológicas como IBM, Microsoft, Facebook o Amazon, entre otras, la relación con proyectos humanitarios resulta muy atractiva ya que les permite acceder a nuevos mercados y oportunidades de innovación técnica[99]. No solo los campos de refugiados son un nuevo mercado del cual se puede conseguir un beneficio, también lo son para los estados que, en alianza con algunas organizaciones de ayuda humanitaria, consiguen recabar datos personales para llevar a cabo políticas fronterizas que no respetan las garantías en materia de derechos humanos, como el ya mencionado caso de los Rohingya en Myanmar y Bangladesh.

La «colonialidad del poder» no solo nace y pervive en el tiempo gracias a la jerarquización racial, sino que encuentra nuevas formas de expresión. En su dimensión más amplia, el extractivismo[100] guarda una estrecha conexión con la globalización, el sistema capitalista y la colonización. Como señala Madianou, la convergencia de estos tres fenómenos explicaría las formas inmateriales de extractivismo, como, por ejemplo, las técnicas de «minería de datos» biométricos que se lleva a cabo sobre la población refugiada en el contexto europeo. Como bien señala Ponzanesi, las nuevas prácticas de realidad digital, como el caso del extractivismo de datos, utilizan la información biométrica extraída

[97] Aníbal Quijano, «Coloniality of Power and Eurocentrism in Latin America,» *International Sociology* 15, no. 2 (2000): 218.
[98] Ver capítulo 1, apartado 3: empresas, agencias y empresas: el trinomio de la discriminación.
[99] Mirca Madianou, «Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises,» *Social Media and Society* 5, no. 3 (2019): 5.
[100] Ver capítulo 1, apartado 1.1: La infraestructura de la hipervigilancia.

para llevar a cabo políticas de vigilancia y control sobre los solicitantes de asilo[101]. Este sería el caso de las bases de datos de Frontex o Eurodac a nivel de la Unión Europea, cuyos posible malos usos hemos comentado en el primer capítulo.

En este juego de poder, sostenido por el sistema neocolonial y capitalista hegemónico, quienes dominan el *big data* son los agentes que ejercen el control. En palabras de Taylor y Broeders, la relación entre empresas privadas y los gobiernos domina una estructura asimétrica y desigual en donde la visibilidad y la invisibilidad corresponde a una lucha entre quienes tienen el poder de ver y quienes carecen de la capacidad de demandar ser vistos o, más importante aún, no ser visibles[102]. Es decir, una lucha entre quienes extraen los datos para propósitos gubernamentales o económicos y quienes han sido despojados de estos y no tienen poder de reclamar sus derechos. En este «autoritarismo de datos», dominado por quienes tienen el control sobre estos, el mundo de la ayuda humanitaria se ha convertido en un escenario de abuso en donde las empresas que poseen el poder de la información tienen también una alta capacidad de influencia. Por este motivo, cuando se hace referencia al trinomio empresas-oenegés-estados nos referimos a una infraestructura de la discriminación. Si los tres actores extraen, retienen e intercambian los datos personas de personas refugiadas, el poder que tienen para explotar y beneficiarse de estos nuevos recursos intangibles es muy alto.

1.1. El colonialismo de datos: la «acumulación mediante la desposesión»

Los mecanismos biométricos de extracción y procesamiento de datos de población refugiada responden a las estructuras asimétricas del poder que, como explica Quijano y Stoler, son consecuencia de las ruinas del colonialismo. Como bien indican Thatcher, O'Sullivan y Mahmoudi esta asimetría que reproduce el extractivismo de datos es una forma propia del capitalismo que se denomina «acumulación por desposesión», concepto recogido a partir de la teoría marxista y que, aplicado al *big data,* se podría describir como el uso de herramientas algorítmicas para mercantilizar millones de datos personales[103].

Esta idea, ya utilizada por Madianou para explicar la relación entre capitalismo y humanitarismo, debe ser tomada con cautela por la escasa evidencia que aún se tiene acerca del uso indebido de datos de población refugiada por empresas tecnológicas. No obstante, sí es cierto que existe una creciente

[101] Laura Candidatu, Koen Leurs, and Sandra Ponzanesi, «Digital Diasporas: Beyond the Buzzword: Toward a Relational Understanding of Mobility and Connectivity,» *The Handbook of Diasporas, Media, and Culture*, (2019): 982.
[102] Linnet Taylor and Dennis Broeders, «In the Name of Development: Power, Profit and the Datafication of the Global South,» *Geoforum* 64 (2015): 231.
[103] Jim Thatcher, David O'Sullivan, and Dillon Mahmoudi, «Data Colonialism through Accumulation by Dispossession: New Metaphors for Daily Data,» *Environment and Planning D: Society and Space* 34, no. 6 (2016): 5.

preocupación académica sobre los usos de la información personal y las consecuencias negativas que podría traer. Es más, esta hipótesis nace de antecedentes ampliamente documentados, como son la mercantilización de los datos personales de los usuarios de internet. En ambos casos, el principio es casi el mismo. En la transformación de los datos individuales en un valor comercial, el *big data* maquilla las relaciones asimétricas de poder entre quienes usan la tecnología (estos pueden ser usuarios de redes sociales o los refugiados a quienes se les extrae la información) y las entidades corporativas que, a través de algoritmos, recolectan enlazan y analizan los datos de los usuarios[104].

Como aciertan en señalar Thatcher, O'Sullivan y Mahmoudi, en el proceso de transformación de dato individual a un conjunto de información con valor mercantilizable, los algoritmos son un requisito fundamental para organizar, discriminar e interpretar la inmensa cantidad de información extraída. En este sentido, los parámetros que se eligen para seleccionar los datos están claramente gobernados por algoritmos, los cuales, a su vez, obedecen a la programación desarrollada por las compañías tecnológicas en su búsqueda de un beneficio[105]. Es más, como ya hemos señalado, detrás de la fachada purista de la programación algorítmica y biométrica se esconden predisposiciones socioculturales que pueden reforzar estereotipos raciales.

De esto último debemos subrayar dos ideas importantes sobre la gobernanza algorítmica[106] para entender los mecanismos de control que ejercen sobre poblaciones vulnerables. En primer lugar, el diseño de la programación puede, y a menudo lo hace, perseguir un interés mercantilista para las empresas tecnológicas que se encargan de su creación. En segundo lugar, el diseño y proceso de ingeniería, los datos, infraestructuras, etc. que constituyen los elementos de la gobernanza algorítmica, entendidos como sistemas sociotécnicos, pueden reproducir e incluso amplificar prejuicios y lógicas raciales. Estas dos premisas apuntan hacia el siguiente argumento: los algoritmos que se emplean para procesar los datos personales no deben ser considerados como neutrales o imparciales. Por el contrario, al ser el producto de una infraestructura comercial, se buscará la forma de capitalizar la materia prima con la que trabajan.

En su informe de 2021, la Relatora Especial sobre racismo y la discriminación racial de la ONU, Tendayi Achiume, concluye que estas nuevas tecnologías tienen precedentes históricos en el pasado colonial y sobre todo en la gobernanza racial, como explicaba Quijano. Es más, el informe insiste que

[104] Thatcher, O'Sullivan, and Mahmoudi, «Data Colonialism through Accumulation by Dispossession» 6.
[105] Thatcher, O'Sullivan, and Mahmoudi, «Data Colonialism through Accumulation by Dispossession» 6.
[106] Ver capítulo 1, apartado 1.4: La gobernanza algorítmica de datos.

el diseño y puesta en marcha de la tecnología tiende a reforzar tendencias sociales, políticas y económicas[107]. En este sentido, la gobernanza algorítmica y la gobernanza racial no son dos cuestiones que se deban considerar por separado ya que la recolección de datos despierta una preocupación acerca de las formas directas e indirectas de discriminación en base a raza, etnicidad, nacionalidad, descendencia y religión[108].

2. Los refugiados como sujetos de datificación

La datificación se entiende como la cuantificación automatizada de los procesos que antes se realizaban de manera cualitativa[109]. Este concepto sirve a la hora de explicar el funcionamiento de las herramientas algorítmicas para extraer datos privados biométricos ya que, como se ha señalado en el apartado anterior, la tecnología permite acelerar la recopilación de información, organizarla e interpretarla para fines determinados, muchos de los cuales responden a una agenda capitalista basada en el extractivismo.

Como sostiene Madianou, el sector del humanitarismo está fuertemente intervenido por estas metodologías. Como defiende la autora, la ayuda humanitaria reproduce estructuras coloniales, en tanto refuerza la visión civilizadora de occidente. Esta vez, mediante la intervención de oenegés para la gestión de la ayuda destinada a la población refugiada y de empresas privadas que aporta la tecnología necesaria para tales fines. Pero cuando la innovación digital se combina con la datificación se generan graves asimetrías de poder en el humanitarismo. Por ejemplo, a través de la repetición de patrones neocolonialistas, una forma contemporánea de mantener el control y el dominio de las potencias occidentales sobre sus antiguas colonial del sur global.

Leese, Noori y Scheel aciertan en sostener que las tecnologías de la innovación digital tienden a ser probadas en poblaciones de países en vías de desarrollo, generalmente bajo pretextos de ayuda humanitaria[110]. No obstante, es importante anotar que detrás de este testeo de tecnología en población vulnerable, el fenómeno de datificación está presente también en las políticas fronterizas y de

[107] United Nations Human Rights Council, Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial and Xenophobic Discrimination and the Use of Digital Technologies in Border and Immigration Enforcement*, New York, NY: UN Headquarters, 2021: 3.
[108] UN Human Rights Council, «Racial and Xenophobic Discrimination,» 9.
[109] Mirca Madianou, «Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises,» *Social Media and Society* 5, no. 3 (2019): 2.
[110] Matthias Leese, Simon Noori, and Stephan Scheel, "Data Matters: The Politics and Practices of Digital Border and Migration Management," *Geopolitics*, (2021): 6.

migración de los estados. En esta dinámica, la infraestructura asimétrica de poder se impregna en las relaciones de los gobiernos del norte y las poblaciones del sur global[111].

El eslogan *tech for good* es un ejemplo de cómo las empresas tecnológicas justifican el uso de los algoritmos para mejorar la eficacia de las organizaciones de ayuda humanitaria[112]. Pero en realidad esta frase no podría distar más de la realidad. Para varios académicos, como Magalhães y Couldry, una visión crítica de la datificación es que esta práctica socava los derechos fundamentales de quienes necesitan ayuda humanitaria o acceso al asilo, como el caso de la población refugiada, a quienes la automatización de datos ayuda a producir políticas de hipervigilancia y criminalización[113]. Por ejemplo, el registro biométrico invasivo de refugiados, aunque mejora la rendición de cuentas de las organizaciones humanitarias, ignora los derechos a la privacidad de personas vulnerables, lo cual las expone a una posterior persecución y acoso[114], sin mencionar el potencial riesgo de que los bancos de datos caigan en manos de terceros.

El trabajo de campo realizado para esta investigación refuerza la idea de estos autores. A la pregunta «¿Qué información te pidieron en ese momento (de llegada)?» los entrevistados respondieron que se les solicitó información sobre sus familias, sobre su historial laboral, pero no mencionaron los datos biométricos. Solo cuando surgió la pregunta sobre si se les había pedido huellas dactilares, lectura de iris o escáner facial, la respuesta fue unánime: sí se les había pedido las huellas dactilares. En una tercera pregunta, «¿Te comunicaron o informaron qué propósito tenía la recolección de estos datos?» la mitad respondieron que sí, mientras que la otra mitad respondieron que no. La calidad de las respuestas sobre la extracción de datos biométricos y sus propósitos no permiten hacer una conclusión fehaciente, pero apuntan a un desentendimiento sobre esta cuestión. No obstante, se podría adelantar que en el proceso de extracción de datos existen algunos indicios de que hay entendimiento implícito entre las personas refugiadas, que en su esfuerzo por conseguir el asilo no tienen una mayor objeción a dar su información personal (incluidos los datos biométricos) sin conocer realmente los riesgos de la externalización que podría sufrir los bancos de datos y las autoridades migratorias que cumplen con las políticas de extranjería de los gobiernos

[111] Leese, Noori and Scheel, «Data Matters»: 6.
[112] João Carlos Magalhães and Nick Couldry, "Giving by Taking Away: Big Tech, Data Colonialism, and the Reconfiguration of Social Good," *International Journal of Communication* 15 (2021): 344.
[113] Magalhães and Couldry, «Giving by Taking Away,» 344.
[114] Magalhães and Couldry, «Giving by Taking Away,» 344.

3. Tecno-colonialismo y gobernanza algorítmica

La elección del «tecno-colonialismo» como marco conceptual de la presente investigación no responde a una decisión fortuita. Por el contrario, ha sido el producto de una reflexión acerca de las consecuencias que determinadas herramientas tecnológicas pueden tener cuando se emplean en contextos en los que las estructuras colonialistas aún persisten. En este sentido, se ha intentado buscar un concepto que ayude a entender los efectos dañinos que puede tener el uso de los algoritmos cuando se emplean como herramientas para procesar millones de datos de las personas refugiadas.

La gobernanza algorítmica como estrategia de control de la población refugiada no sucede por sí sola, si no que tiene el componente colonial como base. En la infraestructura del control que ha sobrevivido a las ruinas del imperialismo, el «extractivismo» y la «datificación» son fenómenos que se explican a través de la discriminación, la explotación y la racialización de determinadas poblaciones. Los refugiados, aquellos individuos que necesitan la ayuda humanitaria de los países del norte global, son considerados de forma directa o indirecta como una materia prima, ya no en su condición física, sino abstracta. Sus datos personales son recogidos y automatizados a través de algoritmos que dictaminan sus futuros y, al mismo tiempo, son utilizados como una fuente de lucro para las empresas o como mecanismo de control de las fronteras y los flujos migratorios para los estados.

En este contexto, la evidencia sugiere que existe un riesgo alto de que los derechos fundamentales de los solicitantes de asilo estén siendo violados o por lo menos ignorados. La extracción de datos biométricos no solo repercute con el derecho al olvido o el derecho a la privacidad, sino que también deja de lado marcos normativos muy explícitos sobre protección de datos, como es el caso de la RGPD europea[115].

La hipótesis formulada del trinomio de la discriminación está intrínsecamente relacionada con el tecno-colonialismo[116]. Autoras como Mirca Madianou sostienen que este concepto es fundamental para entender las relaciones que existen entre el sector del humanitarismo con las empresas tecnológicas, en tanto la innovación digital y las herramientas de procesamiento de datos ayudan a amplificar las desigualdades entre la población refugiada y quienes se benefician de las prácticas extractivistas[117].

[115] Ver capítulo 2: El derecho en los predios de la era digital.
[116] Este trinomio de la discriminación se explica en el capítulo 1, apartado 3.
[117] Madianou, «Technocolonialism,» 10.

No obstante, este concepto puede profundizarse aún más, ya que la existencia de un tercer actor, el estado, es fundamental para entender estas desigualdades históricas. Solo mediante las jerarquías raciales es posible entender las diferencias que existen en las relaciones norte-sur y este-oeste. Las nociones de ciudadanía y sub-ciudadanía[118] son claves para entender las desigualdades imperantes en las antiguas potencias coloniales (y, por extensión en los países colonizados), nos permite comprender la forma en la que la tecnología es un beneficio al alcance de quienes gozan de un espacio de dominio.

El trabajo de Durán y Camarena ofrece una perspectiva interesante al respecto. En el caso de México, la tecnología aplicada a los procesos electorales discrimina a los candidatos que tengan acceso y conocimientos de determinadas herramientas digitales. En 2018, María de Jesús Patricio Martínez, conocida como Marichuy, fue excluida de los comicios presidenciales por no tener una cuenta en Google o Facebook para acceder a la recolección de firmas digitales que le permitiesen justificar su candidatura. Marichuy es una mujer indígena perteneciente a una comunidad originaria de México, por lo que no sería precipitado asumir que su exclusión del proceso electoral estuvo relacionada con el hecho de ser una mujer perteneciente a un grupo racial históricamente segregado[119]. En este caso, la tecnología es un agravante de la discriminación.

En el contexto europeo, Nedelcu y Soysüren recuerdan la interacción entre la precarización de la migración y la tecnología que se despliega en las fronteras comunitarias. En concreto, en materia de seguridad y vigilancia, las herramientas biométricas y bancos de datos como Eurodac juegan un rol preponderante[120]. Ambos autores defienden la idea de que estas tecnologías de la migración han cambiado de manera radical los procesos de control fronterizos en el sentido que son herramientas muy efectivas para limitar drásticamente a la población proveniente de otros países o limitar los intentos de los refugiados que, de acuerdo con el marco normativo jurídico internacional, tienen el derecho de solicitar asilo[121].

Ambos autores recuerdan el consenso académico en cuanto a la transformación del concepto de soberanía del estado mediante las tecnologías fronterizas. La biometría juega un rol preponderante en

[118] Durán y Camarena, que se citan a continuación, explican este concepto como la falta de acceso a medios digitales, lo cual limita el libre ejercicio de los derechos ciudadanos. Esta situación crea otra brecha entre los que tienen los recursos para acceder a herramientas tecnológicas y quienes no.
[119] Inés Durán Matute and Rodrigo Camarena González, «The Machinery of #techno-Colonialism Crafting 'Democracy.' A Glimpse into Digital Sub-Netizenship in Mexico,» *Democratization* 28, no. 8 (2021): 1545–63.
[120] Mihaela Nedelcu and Ibrahim Soysüren, «Precarious Migrants, Migration Regimes and Digital Technologies: The Empowerment-Control Nexus,» *Journal of Ethnic and Migration Studies*, (2020): 2.
[121] Nedelcu and Soysüren, «Precarious Migrants,» 2.

el control de movimiento, en la proliferación y permanencia de los sujetos que circulan en los límites del estado[122]. La nueva configuración de soberanía y frontera de los estados a través de las llamadas «fronteras inteligentes» arroja nuevos conceptos como *smart borders, i borders* o *big borders* para describir el impacto que están teniendo las nuevas tecnologías en la creación de una infraestructura de la vigilancia y el control[123].

En esta nueva forma de interpretar la soberanía y el control sobre las fronteras y migrantes, los estados juegan un rol particular en la relación que hemos descrito entre el sector privado y las agencias de ayuda humanitaria. Al respecto de la relación de estos tres actores, la Relatora Especial sobre racismo y la discriminación racial opina que:

> «Más allá del dominio del mercado, las empresas sirven de intermediarios fundamentales entre los gobiernos y sus naciones, y además tienen la capacidad para transformar significativamente la situación de los derechos humanos. La tecnología creada por poderosas empresas del Norte global se inscribe en un contexto político, económico, social y de gobernanza muy concreto. Puede tener efectos muy perjudiciales en otros contextos, como los del Sur global»[124].

Para los objetivos de esta investigación, es necesario insistir, sobre todo en la cuestión biométrica. Los refugiados son la base de una experimentación cuyos principales beneficiarios son las empresas privadas que han aprendido a lucrar o innovar a partir de la materia prima que son los datos personales[125]. Es más, la noción de «identidad digital» no es más que un proyecto neoliberal que, aunque promete desarrollo económico y más libertades para todos los ciudadanos, en el fondo solo favorece a los sistemas de control migratorio y acumulación de capital que benefician a unos cuantos y marginan a muchos otros[126]. Esta lógica capitalista ha acelerado la implementación del «ensamblaje biométrico», oculto detrás de los argumentos que positivizan la datificación en los entornos de ayuda humanitaria, como, por ejemplo, a través del uso indiscriminado de bases de datos como PRIMES por agencias como ACNUR o el WFP [127].

---

[122] Nedelcu and Soysüren, «Precarious Migrants,» 2.
[123] Nedelcu and Soysüren, «Precarious Migrants,» 2.
[124] United Nations Human Rights Council, Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis.* New York, NY: UN Headquarters, 2020: 6.
[125] Mirca Madianou, «The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies» *Television & New Media* 20, no 6, pp. 581-599 (2019): 24.
[126] Madianou, «The Biometric Assemblage,» 24.
[127] Madianou, «The Biometric Assemblage,» 24.

Latzer y Festic describen la gobernanza algorítmica[128] como el gobierno institucional de la movilidad por medios tecnológicos[129]. A través de esta definición, Kasapoglu explica que, a través de bancos de datos, la recolección de datos biométricos o incluso redes sociales los refugiados son sometidos a regímenes de fronteras cada vez más digitalizados. Esto implica que, por razones de seguridad, progreso tecnológico o desarrollo humanitario, la movilidad de los solicitantes de asilo está hipervigilada a través de algoritmos cuya programación puede generar casos potenciales de discriminación, violaciones de derechos humanos, como el caso del derecho a la privacidad u otras cuestiones como la protección de datos[130].

Aunque relativamente separada de la tesis del tecno-colonialismo, la biopolítica es un concepto que amerita ser repasado, aunque sea de forma breve. La idea, desarrollada inicialmente por Agamben, es puesta en valor en el trabajo de Btihaj Ajana, en lo que ella describe como las técnicas de identificación en donde las medidas biológicas (el concepto más purista de biometría) son parte importante de las estrategias e intervenciones de las políticas migratorias a través de las tecnologías de control fronterizo[131].

La autora analiza herramientas como Eurodac desde una perspectiva no tanto tecnológica, sino más bien desde una mirada sociopolítica, en donde la identificación y verificación biométrica de los individuos no obedece a una cuestión tecnológica, sino una forma de concebir la política de asilo comunitaria de la Unión Europea (definida en la Convención de Dublín). En este caso, las herramientas biométricas sirven un objetivo que más mucho más allá de lo establecido en el tratado, incluso rompe con este de varias maneras. Se trata del acto de hacer pasar los cuerpos de individuos indeseables través de filtros de control biopolítico, como lo son las herramientas biométricas, con el objetivo de crear un límite para aquellos que el estado en cuestión considera ilegítimo, criminal e ilegal[132].

---

[128] Ver capítulo 1, apartado 4: La gobernanza algorítmica.

[129] Latzer, M., & Festic, N. «A guideline for understanding and measuring algorithmic governance in everyday life». *Internet Policy Review* 8 no. 2 (2019), citado en Tayfun Kasapoglu, Anu Masso, and Stefano Calzati, "Unpacking Algorithms as Technologies of Power: Syrian Refugees and Data Experts on Algorithmic Governance," *Digital Geography and Society* 2 (2021): 2.

[130] Tayfun «Unpacking Algorithms as Technologies of Power,» 2.

[131] Btihaj Ajana, «Asylum, Identity Management and Biometric Control,» *Journal of Refugee Studies* 26, no. 4 (2013): 584.

[132] Ajana, «Asylum, Identity Management and Biometric Control,» 584.

CONCLUSIÓN

El objetivo de la presente investigación era demostrar que el uso de determinadas herramientas de extracción de datos, como la biometría, responde a una intención: el control de las personas refugiadas a través de sistemas de información y algoritmos que permitan extraer, procesar y analizar sus datos personales de manera automática. Esta gobernanza algorítmica tiene como propósito, directo o indirecto, reforzar una política fronteriza externa e interna lo suficientemente rígida como para que limite el libre movimiento de los solicitantes de asilo.

Nuestro marco conceptual, basado en el trabajo de otros autores, ha permitido comprender que la población refugiada es sujeto de las infraestructuras poscolonialistas que aún permanecen y se transforman en la actualidad. En este sentido, a través de nociones como «tecno-colonialismo» «datificación» o «extractivismo biométrico» se ha intentado demostrar que la tecnología para el procesamiento de datos no puede ser entendida de manera imparcial. La discriminación, la criminalización y el racismo que estas tecnologías pueden generar obedecen a los parámetros que sus diseñadores deciden imprimirles.

Así mismo, a lo largo de estas páginas se ha insistido en la importancia de los actores que se encuentran implicados en esta gobernanza biométrica. Las grandes agencias de ayuda humanitaria, las *big tech* y los estados nacionales conforman lo que hemos denominado «el trinomio de la discriminación». La evidencia apunta a que los datos obtenidos a través de herramientas de extracción son susceptibles de ser externalizados, ya sea para propósitos monetarios o para el interés de ciertas políticas migratorias.

El aspecto normativo-jurídico ha sido una de las columnas de nuestra investigación. Se ha tenido cuidado de ofrecer, de la manera más comprensiva posible, un repaso por los tratados, leyes y normas que, en el ámbito internacional, comunitario y nacional, son la garantía de los derechos fundamentales de los solicitantes de asilo. También, se han abordado los nuevos debates que en la actualidad se están dando en cuanto a los desafíos que supone la no tan nueva era digital y que, a todas luces, es el contexto en el que se desarrollan todas las tecnologías de procesamiento de datos.

Finalmente, las entrevistas que se han realizado como parte de nuestro marco metodológico han servido para reforzar nuestra hipótesis e ilustrar de la mejor manera posible las diferentes historias de quienes, por múltiples motivos, se han encontrado en una situación de alta vulnerabilidad.

BIBLIOGRAFÍA

Algorace. «EURODAC: un sistema biométrico para categorizar y criminalizar a esos migrantes y refugiados que no queremos,» 20 de abril de 2022. https://algorace.org/2022/04/20/eurodac-un-sistema-biometrico-para-categorizar-y-criminalizar-a-esos-migrantes-y-refugiados-que-no-queremos/

Algorace. «Aprobada una PNL para evitar sesgos y promover la transparencia en el uso de sistemas biométricos en la frontera sur,» 5 de abril de 2022. https://algorace.org/2022/04/05/aprobada-una-pnl-para-evitar-sesgos-y-promover-la-transparencia-en-el-uso-de-sistemas-biometricos-en-la-frontera-sur/

Arce Jiménez, Carlos. *¿Una nueva ciudadanía para la era digital?* Madrid: Dykinson, 2022.

Ajana, Btihaj. "Asylum, Identity Management and Biometric Control." *Journal of Refugee Studies* 26, no. 4 (2013): 576–95. https://doi.org/10.1093/jrs/fet030.

Ajana, Btihaj. "Augmented Borders: Big Data and the Ethics of Immigration Control." *Journal of Information, Communication and Ethics in Society* 13, no. 1 (2015): 58–78. https://doi.org/10.1108/JICES-01-2014-0005.

Boaventura de Sousa Santos, *Una epistemología del sur: la reinvención del conocimiento y la emancipación social,* (México: siglo XXI Clacso, 2009)

Candidatu, Laura, Koen Leurs, and Sandra Ponzanesi. "Digital Diasporas: Beyond the Buzzword: Toward a Relational Understanding of Mobility and Connectivity." *The Handbook of Diasporas, Media, and Culture*, 2019, 31–47. https://doi.org/10.1002/9781119236771.ch3.

Couldry, Nick, and Ulises A. Mejias. "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject." *Television and New Media* 20, no. 4 (2019): 336–49. https://doi.org/10.1177/1527476418796632.

Crawford, Kate, and Megan Finn. "The Limits of Crisis Data: Analytical and Ethical Challenges of Using Social and Mobile Data to Understand Disasters." *GeoJournal* 80, no. 4 (2015): 491–502. https://doi.org/10.1007/s10708-014-9597-z.

Carly Nyst, Zara Rahman, Paola Verhaert y Anna Kondakhchyan, eds., *Biometrics in the Humanitarian*

Sector (Oxford: Oxfam, 2018).

Dencik, Lina, and Javier Sanchez-Monedero. 2022. «Data justice». *Internet Policy Review* 11 no.1 (2022). DOI: 10.14763/2022.1.1615.

Durán Matute, Inés, and Rodrigo Camarena González. "The Machinery of #techno-Colonialism Crafting 'Democracy.' A Glimpse into Digital Sub-Netizenship in Mexico." *Democratization* 28, no. 8 (2021): 1545–63. https://doi.org/10.1080/13510347.2021.1947248.

Elise Thomas «Tagged, tracked and in danger: How the Rohingya got caught in the UN's risky biometric database». Wired, March 12, 2018, http://www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh.

Hueso, Vicente. "Johan Galtung. La Transformación de Los Conflictos Por Medios Pacíficos." *Cuadernos de Estrategia* 111 (2000): 125–59. https://dialnet.unirioja.es/descarga/articulo/595158.pdf.

International Committee of the Red Cross (ICRC) and Privacy International, *The humanitarian metadata problem: "Doing no harm" in the digital era*, 2018.

Kasapoglu, Tayfun, Anu Masso, and Stefano Calzati. "Unpacking Algorithms as Technologies of Power: Syrian Refugees and Data Experts on Algorithmic Governance." *Digital Geography and Society* 2 (2021): 100016. https://doi.org/10.1016/j.diggeo.2021.100016.

Latonero, Mark, and Paula Kift. "On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control." *Social Media and Society* 4, no. 1 (2018). https://doi.org/10.1177/2056305118764432.

Leese, Matthias, Simon Noori, and Stephan Scheel. "Data Matters: The Politics and Practices of Digital Border and Migration Management." *Geopolitics*, 2021. https://doi.org/10.1080/14650045.2021.1940538.

Madianou, Mirca. "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises." *Social Media and Society* 5, no. 3 (2019). https://doi.org/10.1177/2056305119863146.

Madianou, Mirca. *The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies*. *Television and New Media*. Vol. 20, 2019. https://doi.org/10.1177/1527476419857682.

Madianou, Mirca, Jonathan Corpus Ong, Liezel Longboan, and Jayeel S. Cornelio. "The Appearance of Accountability: Communication Technologies and Power Asymmetries in Humanitarian Aid and Disaster Recovery." *Journal of Communication* 66, no. 6 (2016): 960–81. https://doi.org/10.1111/jcom.12258.

Magalhães, João Carlos, and Nick Couldry. "Giving by Taking Away: Big Tech, Data Colonialism, and the Reconfiguration of Social Good." *International Journal of Communication* 15 (2021): 343–62.

McDonald, Sean Martin. "Ebola: A Big Data Disaster - Privacy, Property, and the Law of Disaster Experimentation." *The Centre for Internet and Society*, no. 2016.01 (2016). http://cis-india.org/papers/ebola-a-big-data-disaster.

Nedden, C. zur and Ariana Dongus. «Tested on millions Non-volunteers / Getestet an Millionen Unfreiwilligen,» *ACNUR*. 2017, December 17. https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/01/article_1.pdf.

Nedelcu, Mihaela, and Ibrahim Soysüren. "Precarious Migrants, Migration Regimes and Digital Technologies: The Empowerment-Control Nexus." *Journal of Ethnic and Migration Studies*, 2020. https://doi.org/10.1080/1369183X.2020.1796263.

Pisón, José Martínez de. «Vida privada sin intimidad. una aproximación a los efectos de las intromisiones tecnológicas en el ámbito íntimo,» *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos* no 37 (2017).

Paragi, Beata. "Digital4development? European Data Protection in the Global South." *Third World Quarterly* 42, no. 2 (2020): 254–73. https://doi.org/10.1080/01436597.2020.1811961.

Ponzanesi, Sandra. "Digital Diasporas: Postcoloniality, Media and Affect." *Interventions* 22, no. 8 (2020): 977–93. https://doi.org/10.1080/1369801X.2020.1718537.

Quijano, Aníbal. "Coloniality of Power and Eurocentrism in Latin America." *International Sociology* 15, no. 2 (2000): 215–32. https://doi.org/10.1177/0268580900015002005.

Rejali, Saman, and Yannick Heiniger. "The Role of Digital Technologies in Humanitarian Law, Policy and Action: Charting a Path Forward." *International Review of the Red Cross* 102, no. 913 (2020): 1–22. https://doi.org/10.1017/S1816383121000114.

Rodríguez-Villasante y Prieto, José Luis. «La protección de los refugiados y desplazados internos por

el derecho internacional», en *Migraciones en el siglo XXI: riesgos y oportunidades: XXIV Curso Internacional de Defensa*, Academia General Militar (Zaragoza) (dir.), Universidad de Zaragoza (dir.) (Jaca, 2016), 1.

Rodríguez y Gonzalo Fanjul, Virginia. *La industria del control migratorio ¿Quién gana en España con las políticas fronterizas de la Unión Europea?* Madrid: Porcausa, 2017: 11.

Sánchez-Monedero, Javier. "The Datafication of Borders and Management of Refugees in the Context of Europe," 2018. http://www.unhcr.org/uk/primes.html.

Solinge, Delphine van, and Massimo Marelli. "Q&A: Humanitarian Operations, the Spread of Harmful Information and Data Protection." *International Review of the Red Cross* 102, no. 913 (2020): 27–41. https://doi.org/10.1017/S1816383120000429.

Stoler, Ann Laura. "Imperial Debris : Reflections on Ruins and Ruination Published by : Wiley on Behalf of the American Anthropological Association Stable URL : Http://Www.Jstor.Org/Stable/20484502 RInation „: B S ~ : R1efeton NRun N." *Cultural Anthropology* 23, no. 2 (2016): 191–219.

Taylor, Linnet, and Dennis Broeders. "In the Name of Development: Power, Profit and the Datafication of the Global South." *Geoforum* 64 (2015): 229–37. https://doi.org/10.1016/j.geoforum.2015.07.002.

Thatcher, Jim, David O'Sullivan, and Dillon Mahmoudi. "Data Colonialism through Accumulation by Dispossession: New Metaphors for Daily Data." *Environment and Planning D: Society and Space* 34, no. 6 (2016): 990–1006. https://doi.org/10.1177/0263775816633195.

United Nations Human Rights Council, Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis.* New York, NY: UN Headquarters, 2020

United Nations Human Rights Council, Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial and Xenophobic Discrimination and the Use of Digital Technologies in Border and Immigration Enforcement*, New York, NY: UN Headquarters, 2021

ANEXO I

CONCLUSIONES DEL TRABAJO DE CAMPO

El presente TFM contó con entrevistas a ciudadanos extracomunitarios que son o han sido personas refugiadas. Las entrevistas realizadas han aportado un valioso testimonio con el cual se han podido reforzar algunos de los argumentos que sostienen nuestra hipótesis. Algunas ideas que se expondrán a continuación ya han sido recogidas en los tres capítulos, mientras que otras forman parte del proceso de recolección y análisis de la información obtenida.

Conclusiones generales (aspectos técnicos):

La muestra demográfica contó con diez personas de diferentes nacionalidades. Se realizaron entrevistas a individuos provenientes del Sahara Occidental, Mali, Senegal, El Salvador y Venezuela. La mayoría llegó a España por medios regulares, como aeropuertos, mientras que dos casos fueron de personas que entraron al país por medios irregulares como embarcaciones clandestinas. Esto sugiere que, si bien la demografía no es numerosa, el ámbito geográfico es lo suficientemente amplio para conocer experiencias distintas y obtener conclusiones más variadas.

El estudio cualitativo de la muestra demográfica permite conocer con un mayor detalle las historias de vida de las personas que se ofrecieron a ser consultadas. Si bien no todas las experiencias recogidas se han incluido en la investigación, la mayoría ofrecen perspectivas únicas de la realidad ya que cada testimonio ha aportado ideas originales para este TFM. Debido a los límites impuestos por el tema trabajado y por la dificultad que supone el traslado a fronteras o a campos de refugiados en el contexto de postpandemia, no se han podido obtener testimonios *in situ*. Por este motivo, se ha contado con el apoyo de la Cruz Roja Española para gestionar las entrevistas, las cuales se llevaron a cabo en la oficina provincial de Córdoba y a través de videollamadas.

Las preguntas se formularon con el objetivo de incentivar un ejercicio de reflexión, teniendo en cuenta que el tema de tratamiento de datos, en especial la biometría, es un campo desconocido y con muchas incógnitas. Respetando en todo el momento el contexto de las personas refugiadas, también hubo un esfuerzo de obtener información relacionada con los métodos de llegada a España y también los tratos recibidos por las autoridades migratorias.

Las preguntas se formularon en español, en inglés y en francés. Así mismo, se tuvo el apoyo de una traductora para los ciudadanos provenientes de países francófonos de África Occidental, como los

casos de Mali y Senegal. En el caso de estos últimos, hubo cierta dificultad de entablar un diálogo fluido, ya que en varias ocasiones las respuestas eran muy cortas o monosílabas. Por este motivo, cuidando de no forzar ninguna respuesta determinada, sí se intentó insistir sobre ciertas preguntas para intentar obtener alguna información que no se haya mencionado por omisión.

Al comienzo de cada entrevista, se hizo una breve explicación sobre el tema de investigación, con la finalidad de centrar la conversación en la experiencia relacionada con el tratamiento de datos, intentando en la medida de lo posible que los individuos pudieran explayarse en sus historias y en las posibles preocupaciones que tuvieran en cuanto a este tema en concreto. También, se les comunicó a las personas que sus datos serían tratados para fines académicos de este TFM y el consentimiento informado se gestionó a través de Cruz Roja.

Conclusiones del trabajo de campo

La interpretación de los datos obtenidos permite reforzar la hipótesis de la investigación. La evidencia recogida a partir de las entrevistas revela la existencia de métodos de extracción y procesamiento de datos en políticas migratorias de la Unión Europea. Todos los individuos afirmaron que al momento de solicitar el refugio se les solicitó el registro de datos, a menudo personales o privados, cuyo contenido es altamente sensible, como la historia familiar, antecedentes médicos, experiencia profesional y la evidencia que justifica la solicitud de asilo. Así mismo, todos aseguraron que se les extrajo datos biométricos, en especial la toma de huellas dactilares.

Este resultado permite comprender los mecanismos de extracción de información y la forma en la que los grandes sistemas informáticos como Eurodac son capaces de recolectar y retener millones de datos de población refugiada. A partir de lo que hemos explicado, podemos concluir que esos datos forman parte de la infraestructura implementada por la Unión Europea que contribuye a fortalecer una política de seguimiento y control de la población refugiada. La datificación, que en este trabajo se ha explicado como automatización de los procesos de gobernanza a través de datos, a la que son sometidos los refugiados, responde precisamente a estas cuestiones.

En relación con nuestro marco conceptual, podemos comprobar que los países originarios de los encuestados pertenecen al llamado «sur global» y son en efecto territorios en los que aún predomina una herencia colonial que cuya expresión contemporánea es el «tecno-colonialismo». Aunque sería premeditado asumir que estos individuos son percibidos como potenciales criminales, la evidencia de

otras investigaciones más robustas sugiere que sí existen motivos para sospechar que el lugar de origen de los refugiados constituye una fuente de desconfianza en el entorno europeo.

Todos los entrevistados afirmaron que las autoridades migratorias les informaron sobre los motivos por lo que sus datos se recogían. No obstante, como se ha explicado a lo largo de este estudio, la cuestión relacionada con el consentimiento previo requiere de una reflexión. La evidencia recogida, que ha sido contrastada con otras investigaciones del tema, permite suponer que existe una ambigüedad en el proceso de recogida de información por los agentes de migración. En la mayoría de los casos, los refugiados no tienen la opción real de negarse a la extracción de sus datos privados por el riesgo que supone el posible rechazo de sus solicitudes. Las «asimetrías de poder» son las que Madianou asume como las causas de que no exista un consentimiento real o significativo. Este desequilibrio que se ha conceptualizado a través de la noción de la «infraestructura del poder» permite entender los mecanismos del extractivismo de datos.

Otro problema que también revelaron las entrevistas es la relación ambigua que hay con las autoridades, con quienes existe una relación de gratitud y correspondencia. En su mayoría, los sujetos reconocieron que el trato en las oficinas de extranjería fue positivo, pero al mismo tiempo aseguraron que la precariedad de su situación les impedía negarse a dar los datos que se les solicitaba. En este sentido, si bien todos los participantes tuvieron experiencias positivas con las autoridades, ninguno de ellos se negó a cumplir con todos los requerimientos de información que se les solicitó. Es más, algunos individuos dieron a entender que su situación no permitía mucho margen de acción y mucho menos de decisión.

Así mismo, las entrevistas ayudaron a reforzar la idea de que existe un desconocimiento general acerca de las cuestiones por las que se les preguntaba. Todos, excepto un individuo, no conocían las consecuencias de que sus datos fueran compartidos o externalizados. Tampoco expresaron una preocupación por estos riesgos, sino que, por el contrario, manifestaron no conocer realmente el posible paradero de los datos compartidos. En otras palabras, se trata de una falta de información relacionada con el uso de algoritmos en el procesamiento de datos y los peligros que conlleva la automatización de estos procesos. El único entrevistado que expresó preocupación sobre esta cuestión resultó ser informático de profesión, por lo que tenía formación al respecto.

Esto no debe interpretarse como una ignorancia en material legal. En realidad, se puede concluir que los entrevistados eran plenamente conscientes de los derechos que los protegen. Casi todos afirmaron

conocer acerca de las leyes que los amparaban como refugiados. Uno de los entrevistados, de origen saharaui, afirmó que su condición como habitante de un antiguo protectorado español le daba determinados beneficios. Otros, de Senegal o de Mali, afirmaron haber recibido asesoría legal sobre sus derechos.

Finalmente, en el trabajo de campo con personas refugiadas no se debe omitir en ningún momento el contexto de sufrimiento desde el cual se está recabando la información. En todas las entrevistas, los individuos aseguraron que habían llegado a España en los últimos dos años, la mayoría en el año 2021, por lo que los recuerdos son muy recientes. Por este motivo, no se puede obviar que las respuestas puedan estar limitadas o influenciadas por las experiencias negativas que atravesaron, ya sea en sus países de origen, al momento de llegar a España o cuando solicitaron el refugio a las autoridades correspondientes. En general, a través de algunas respuestas se pudo comprender que la prioridad de los solicitantes es obtener la salvaguarda y la seguridad que ofrece el estatus de refugio, mientras que otras cuestiones, como la entrega de datos personales, se convierten en un bien inmaterial que, de ser necesario, están dispuestos a ceder.

ANEXO II

CUESTIONARIO DE LAS ENTREVISTAS

1. ¿Cuándo llegaste a España?

2. ¿Cómo fue tu experiencia al momento de pedir refugio? ¿Cómo te trataron?

3. ¿Te pidieron información personal al momento de ingresar a España?

- Pregunta puede variar si la persona entró por otro país de la UE.

4. ¿Qué información te pidieron en ese momento?

- Historia familiar, estudios, trabajos, etc.
- El proceso de llegada a España

5. ¿Tienes un pasaporte? ¿De qué país es?

6. ¿Te comunicaron o informaron qué propósito tenía la recolección de estos datos?

7. ¿Pudiste decidir qué datos personales entregabas y cuáles no?

- ¿Qué sensaciones te produjo el momento de recolección de datos?

8. ¿Cómo te hubiera gustado que hubiera sido el proceso de recolección datos personales?"

- ¿Cuál sería tu preferencia en relación a dar o no dar datos personales?

9. ¿Qué sabías sobre estos temas previamente antes de llegar a España? ¿Sabías algo acerca de la información que tenías que dar? ¿Alguien te aconsejó acerca de cuándo era mejor o pertinente solicitar esa información?

10. ¿Conoces o sabes que en la UE existe una normativa que protege los derechos de datos personales?

11. Finalmente ¿Recuerdas qué agencia te pidió esta información?