LOS OLVIDADOS DE LA PROTECCIÓN DE DATOS

Personas refugiadas y tecnologías digitales

Olga Lucía Camacho Gutiérrez

Director: Javier Palummo

INTRODUCCIÓN

Las preocupaciones en torno a la protección de datos parecen nimias cuando se ve, de lejos, la experiencia de las personas que huyen de su lugar de origen y buscan en otro país el reconocimiento de medidas de protección que les permitan rehacer sus vidas. Con algo de razón se podría creer que, ante las amenazas a la vida o la libertad que sufren las personas refugiadas, los demás derechos pasan a una suerte de segundo plano hasta que otros más vitales no sean asegurados primero.

Sin embargo, los riesgos al derecho a la protección de datos pueden amplificar su condición de por sí vulnerable, más aún si se toma en cuenta que sus datos personales y sensibles pueden llegar a caer en manos de los Estados de los que huyen y les persiguen. No es, entonces, una preocupación menor indagar en los retos de este tipo, especialmente de cara al despliegue de tecnologías digitales que aumentan las capacidades de terceros para recolectar y procesar todo tipo de datos durante su jornada de huida: Estados, agencias y organizaciones de ayuda humanitaria, empresas del sector tecnológico, entre otros.

Al respecto vale la pena señalar que el uso y despliegue de este tipo de tecnologías por agencias y organizaciones humanitarias merece mayor escrutinio pues, con tal de llevar a cabo su objetivo humanitario, pueden llegar, por ejemplo, a ceder ante las presiones de los Estados en los que operan, compartiendo la información personal de las personas refugiadas a las que proveen asistencia y ayuda, tal y como sucedió recientemente con los datos biométricos de la comunidad Rohingya, administrados por ACNUR y cedidos luego a Myanmar (Human Rights Watch, 2021).

Las agencias y organizaciones humanitarias se desenvuelven, además, en terrenos donde el Estado de Derecho es débil o inexistente, y las protecciones a la privacidad de las personas se encuentran restringidas en múltiples sentidos: porque este puede no ser un derecho reconocido (en el mundo todavía hay países que no consagran leyes de este tipo); porque de haberlas pueden no aplicar a los actores que no se domicilian en dicho país en concreto –como los actores humanitarios– porque su ejercicio no es gratuito, o porque la persona es disuadida para ejercer su derecho debido a su condición irregular en un país que, además, le resulta ajeno cultural, legal y socialmente.

No obstante, el despliegue de tecnologías digitales en los espacios humanitarios en que actúan agencias y organizaciones internacionales, y por los que transitan las personas refugiadas de manera temporal hasta que su situación es resuelta del todo, ha significado también la presencia y participación de actores que no se orientan bajo los principios de humanidad, neutralidad, imparcialidad e independencia, sino por los valores del mercado: las empresas de *Silicon Valley* o las *Big Tech*.

Recientes casos de acuerdos suscritos por organismos de las Naciones Unidas especializados en la provisión global de alimentos y la atención y ayuda de personas refugiadas, con empresas tecnológicas que han sido cuestionadas también por las Naciones Unidas por sus pobres compromisos con los derechos humanos, pone de presente la urgencia de la pregunta en torno a quién y cómo se encarga de evaluar los riesgos que las tecnologías digitales representan para las personas refugiadas.

La literatura que se especializa en el análisis de la acción humanitaria para las personas refugiadas por un lado, y en el impacto de las tecnologías digitales en la privacidad y protección de datos por el otro, ha ido aumentando en la última década llamando la atención en torno a dicha pregunta.

Sin embargo, se trata de literatura dispersa cuya lectura reciente y conjunta es preciso llevar a cabo para determinar cuál es el estado real de la discusión, los contornos precisos del problema que se advierte, los actores que en dicho problema participan, los intereses y riesgos que les impactan a cada uno, incluyendo los que tienen que ver especialmente con la protección de datos de las personas refugiadas.

Ahora bien, en tanto que el destino y la suerte de las personas refugiadas no son una preocupación exclusiva de la geografía africana, y europea, donde se ha enfocado la literatura que indaga en este sentido, es relevante poder llevar a cabo la configuración del estado del arte que permita comprender problemas en derechos humanos que pueden llegar a aparecer en la región latinoamericana que también experimenta una grave crisis de refugiados.

Por ello, esta tesis se propone avanzar en la configuración del estado del arte del problema advertido para identificar los riesgos que representa para la protección de datos de la persona refugiada, la masificación de tecnologías digitales en la acción humanitaria a cargo de agencias y organizaciones internacionales especializadas en la atención de dicho grupo humano.

Para el logro de dicho propósito, esta investigación se divide en tres capítulos. El primero, provee un contexto breve sobre los principios que orientan y caracterizan el accionar de agencias y organizaciones internacionales de ayuda humanitaria, aborda así mismo un panorama amplio sobre cómo es la acción humanitaria que se provee a las personas refugiadas, y explica cómo es que aterrizan en dicho escenario las tecnologías digitales.

En el segundo capítulo se identifican y categorizan los riesgos que representan dichas tecnologías digitales para el ejercicio del derecho a la protección de datos de la persona refugiada. Se provee un marco sobre el "deber ser" basado en estándares en privacidad y protección de datos, y luego presentamos los hallazgos sobre "el ser" al que apunta la literatura revisada que señala sus beneficios y riesgos.

En el tercer capítulo se amplía el análisis de beneficios y riesgos más allá de la protección de datos y las personas refugiadas, para identificar qué está en juego para los otros actores que crean y despliegan tecnologías digitales para el contexto humanitario. Se apunta, por último, a la identificación de la promesa que, pese a los riesgos advertidos, sigue empujando su masificación.

Este escrito concluye con algunas reflexiones finales y la relación de la bibliografía consultada.

Metodología

El objetivo principal de este escrito es indagar en el estado del arte para identificar los riesgos que representa para la protección de datos de la persona refugiada la masificación de tecnologías digitales en la acción humanitaria.

Dicho proceso de identificación de beneficios y riesgos se orienta, en esencia, en un proceso de reconstrucción del estado del arte de la discusión. De manera que, atendiendo una lógica inductiva, se precisa del mapeo del desarrollo de las investigaciones que han explorado el mismo objeto de esta investigación, o que se han aproximado a este desde perspectivas similares o cercanas. Satisfecho este proceso, será posible arribar más claramente a la identificación de posturas críticas, entusiastas, que adviertan riesgos y beneficios en la materia.

Dicho esto, el proceso de reconstrucción del estado del arte –que es al tiempo un proceso y un producto– permite un acercamiento al objeto de esta investigación al facilitar la realización de múltiples propósitos. El primero, efectuar balances sobre el enfoque y acercamiento de la literatura seleccionada; el segundo, analizar sus alcances y vacíos para detectar oportunidades de profundización a futuro; el tercero, caracterizar y detectar tendencias y distancias epistémicas de la literatura escogida, para reflexionar sobre su significado en la problematización de las variables propuestas, entre otros.

Dicho esto, el estado del arte del presente escrito se enmarcó bajo técnicas que serán descritas a continuación con el fin de permitir una mayor comprensión, explicabilidad y transparencia sobre las decisiones metodológicas que atraviesan esta "investigación de investigaciones" (Guevara Patiño, 2016: 166).

Así las cosas, el proceso de reconstrucción del estado del arte de este escrito estuvo orientado por dos límites de base, uno temporal y otro lingüístico. El temporal, que comprendió la selección de literatura en un espectro de seis años, una cobertura de tiempo más o menos razonable para ser abarcado en el tiempo permitido para la realización de este escrito. Y el lingüístico, que comprendió la selección de literatura en español e inglés en tanto son los idiomas que domina la investigadora.

A partir de esos límites de base se estructuraron los criterios de selección y posterior caracterización de la literatura. La fase de selección se orientó en la búsqueda de literatura disponible en trece bases de datos[1] a partir de descriptores que pudieran abarcar la literatura más reciente en inglés y español.

1 Entre ellas: JSTOR, DOAJ, Scopus, SSRN, Elsevier, EBSCO, Scielo, ScienceOpen. Bases de datos editoriales como SpringerLink, Cambridge y Oxford. Y motores de búsqueda como Google Scholar y Microsoft Academic.

Un descriptor es un vocablo jurídico compartido de manera unívoca por la comunidad jurídica. Entre los descriptores de búsqueda[2] se eligieron los que hacían referencia a las tecnologías digitales en la acción humanitaria (en español: humanitarismo digital; tecnologías humanitarias; tecnologías digitales y ayuda humanitaria; tecnologías digitales y acción humanitaria; tecnologías digitales y sector humanitario. En inglés: *digital humanitarianism*; *digital humanitarians*; *humanitarian technology*; *technology in humanitarian action*; *technology in humanitarian sector*; *humanitarian aid technology*).

Y los que hacían referencia a la privacidad de las personas refugiadas en crisis humanitarias (en español: protección de datos y refugiados; privacidad de refugiados; protección de datos y refugiados en crisis humanitarias; privacidad de refugiados en crisis humanitarias; protección de datos en la acción humanitaria; privacidad en la acción humanitaria. En inglés: *refugees' data protection*; *refugees' privacy*; *refugees' data protection in humanitarian aid*; *refugees' privacy in humanitarian aid*).

Los resultados de búsqueda se limitaron a la conformación de un grupo de lecturas recientes, publicadas en los años 2021, 2020 y 2019. Una vez ubicada dicha literatura, se efectuó un proceso de ingeniería reversa, es decir, de revisión y búsqueda de las citaciones efectuadas por esos textos recientes, y que se extendió en dos niveles, esto es, de búsqueda de los textos citados en la literatura reciente, y de revisión y búsqueda de citas en esos otros textos citados.

Sobre dichos resultados se efectuó un proceso de barrido sobre su contenido para filtrar la literatura que pudiera intersectar, en mayor medida, las discusiones sobre uso y despliegue de tecnologías digitales en la acción humanitaria y su impacto en la privacidad de las personas refugiadas.

Luego de dicho barrido y filtrado, la muestra total de literatura seleccionada estuvo conformada por un total de 60 textos. Se trata de una muestra diversa que integra textos publicados por instituciones académicas, *think tanks*, organizaciones de la sociedad civil, organismos especializados de las Naciones Unidas, así como autores y autoras reconocidos. Los textos comprenden artículos académicos, informes de conferencias, reportes de investigación, libros especializados, publicaciones en blogs académicos y noticias.

Se procuró mantener una muestra diversa en ese sentido, al tiempo que se limitó la selección bibliográfica a máximo cinco textos provenientes de un mismo autor o autora. En los casos en que se ubicaron más de cinco textos por un mismo autor o autora en el espectro temporal de interés, se seleccionaron en su caso los textos más recientes. La exclusión no aplicó en los casos en que dicho autor o autora apareció en coautoría con otros.

Así las cosas, una vez se concluyó la fase de conformación de la muestra de la literatura objeto de revisión (cuyo listado hará parte de este texto a manera de anexo), se procedió a la fase caracterización de la misma con el fin de obtener una relación de datos identificadores (nombre del autor o autora, título del texto,

2 Otros descriptores que fueron empleados de manera menos intensiva fueron los de *responsible data* como una alternativa más reciente para referir a la privacidad y protección de datos junto a otros derechos, y el de *aid settings* o *crisis settings* como expresiones asociadas a la acción humanitaria.

medio de publicación y año), y de datos sobre el contenido de las lecturas (postura, enfoque, retos, riesgos). Datos dirigidos, en su conjunto, a informar el contenido de los capítulos segundo y tercero de este escrito.

El objetivo que persigue dicha caracterización a través de la extracción de un conjunto de datos concretos, apunta a facilitar la identificación de posturas compartidas y divergencias entre autores y autoras, así como permitir identificar enfoques comunes, vacíos y presencias que faciliten luego, en un proceso de abstracción, realizar agrupaciones y categorías que provean una mayor comprensión sobre el estado de la discusión en torno al objeto de investigación que desarrolla este escrito.

Por último, en el proceso de conformación de la muestra de la literatura de interés hay que hacer, al menos dos precisiones. La primera, que tiene que ver con la publicación de textos relevantes durante 2011 y 2013 que, al encontrarse fuera de la órbita temporal, no hicieron parte de los procesos de caracterización y análisis, los cuales debieran poder ser consultados en estudios posteriores más comprensivos que este.

La segunda, que el conjunto de textos seleccionados no es, por supuesto, exhaustivo y comprensivo sobre todas las voces ni las visiones en torno al objeto de investigación, considerando además las limitaciones (temporal y de idioma) que dejaron por fuera desarrollos y aportes relevantes. Se trata, entonces, de un grupo de textos que arroja luz sobre el debate, pero no por ello es la única ni es excluyente de otras que iluminan la comprensión del tema elegido.

Capítulo 1

DEL IDEAL DE LA ACCIÓN HUMANITARIA AL ATERRIZAJE DE LAS TECNOLOGÍAS DIGITALES EN LA CRISIS DE REFUGIADOS

La aproximación al estado del arte que propone esta investigación precisa de un contexto en tanto que las discusiones inmersas en este no se inscriben en el vacío.

Dicho contexto se encuentra enmarcado en este escrito, en primer lugar, en el abordaje del contenido de los principios de la acción humanitaria,[1] en segundo lugar, en los contornos de la acción humanitaria en beneficio de las personas refugiadas[2] y, en tercer lugar, en el aterrizaje de las tecnologías digitales[3] en la misma.

En la primera sección presentaremos los principios de la acción humanitaria a manera de propuesta de marco conceptual que permita orientar al lector en torno al ideal de la acción humanitaria. Dicho marco permitirá establecer puntos de referencia en la comparación entre lo que se supone que *debe ser* la acción humanitaria influida por el uso y despliegue de las tecnologías digitales, y los hallazgos sobre lo que *es* y que serán presentados en el capítulo siguiente.

La sección siguiente enmarcará los retos que atraviesa la acción humanitaria en beneficio de las personas refugiadas, con una breve referencia a las cuestiones que giran en torno al derecho internacional que los regula, y la alusión a algunas de las respuestas recientes de dicho marco a la crisis actual de refugiados. Allí mismo se hará referencia a los actores más representativos de la acción humanitaria en materia de refugiados y los problemas que, en su conjunto, han abierto paso

1 En adelante, toda alusión a este término estará asociada a las acciones de provisión de asistencia y ayuda que se procuran a las personas en contextos de emergencia y que se orientan por los principios humanitarios de humanidad, neutralidad, imparcialidad e independencia.

Si bien reconocemos que se trata actividades que pueden ser desempeñadas por los Estados, al hacer alusión a dicha expresión conservaremos especial énfasis en su desenvolvimiento por actores no estatales, es decir, aquellos que ni orgánica ni funcionalmente dependen de estos para llevar a cabo sus tareas aun cuando aquellos puedan llegar a contribuir a su financiamiento (Ginty & Peterson, 2015).

2 A efectos de este escrito, por personas refugiadas nos referimos a todas las personas que huyen de su Estado de origen por motivos asociados a la guerra, la persecución, la violencia, entre otros; y que se ven imposibilitadas o indispuestas para regresar a su propio país por miedo (es decir, personas refugiados en *stricto sensu)* y que, en ese sentido, buscan en otro Estado medidas de protección cuya resolución se encuentra pendiente (esto es, personas solicitantes de asilo) (Hathaway, 2005).

3 Para este escrito, por tecnologías digitales se entiende a las tecnologías y técnicas de datificación, es decir, capaces de capturar, almacenar y procesar datos y datos personales para, por ejemplo, automatizar la toma de decisiones, entre otros (Comité asesor del Consejo de Derechos Humanos, 2021).

de manera paulatina a la participación más abierta del sector privado como nuevo actor humanitario.

En la sección final se presentará el contexto y narrativa que facilitó al sector de las tecnologías de la información y las comunicaciones llegar a la escena humanitaria como actor atípico, presentamos algunos desarrollos que confirman dicho aterrizaje y distinguimos dicho suceso desde el análisis al tecno-entusiasmo, sus riesgos y críticas para formular una visión crítica que orientará la revisión del estado del arte que será emprendida en el segundo capítulo de esta tesis.

1. El ideal de la acción humanitaria: la necesidad de los principios y sus dificultades prácticas

La acción humanitaria vista desde una perspectiva amplia como práctica cultural, social, filosófica y política refiere, en términos generales, al despliegue de actividades que buscan proveer asistencia, ayuda y socorro en el marco de las así denominadas "crisis humanitarias". Sin intención de ahondar en ninguna de estas perspectivas es posible, en todo caso, inscribir su nacimiento formal a nivel conceptual, institucional y operacional con la creación para 1863 del Comité Internacional de la Cruz Roja y la Media Luna Roja (CICR en adelante).

La acción humanitaria, así como los principios que la orientan, desde entonces se ha transformado en múltiples sentidos debido a los contextos sociales y políticos en que han tenido que desenvolverse durante más de un siglo y medio de reconocimiento formal. Dichos cambios comprenden, entre otros, la concurrencia de diversos intereses y actores que la ejecutan, su complejización a nivel operacional y financiero, variaciones en su alcance y objetivos.

Asimismo, estos han derivado en procesos de transformación a manera de idas y vueltas, y se han visto orientados bajo la centralidad de un conjunto específico de principios. Los principios de la acción humanitaria han sido desde su nacimiento formal –si se quiere– los ejes aspiracionales que han articulado su maduración progresiva. Poseen una suerte de resonancia más o menos amplia entre quienes ejercen la acción humanitaria, en tanto que revisten el carácter de orientadores, así como de declaraciones éticas frente a otros actores.

A partir del reconocimiento formal de la acción humanitaria surgió, entre los principios, una suerte de división: los Principios Fundamentales del CICR y los que serían conocidos como los principios de la acción humanitaria, que derivarían de estos.

Autores como Thompson en todo caso recuerdan que se trata de una distinción más bien formal, pues los principios de la acción humanitaria en general, y los del CICR en concreto, se nutren unos a otros y no conviven a manera de islas (2015), de ahí que sea común que en la reconstrucción de los principios de la acción humanitaria las referencias a la trayectoria del Comité sea una tarea común. Autores como Fiori, en cambio, sostienen que se trata de la reconstrucción de principios dominantes tan solo en la narrativa europea que no representa ni la jerarquía ni los contenidos de los principios vigentes en la acción humanitaria en regiones como el Sudeste Asiático o Latinoamérica (2013).

Como sea, el reconocimiento de los Principios Fundamentales que tuvo lugar a la conclusión de la Primera Guerra Mundial, se hizo a través de la reforma a los Estatutos del CICR que hicieron referencia expresa a los de imparcialidad, independencia política, religiosa y económica, la universidad del Comité y la igualdad de sus miembros.

La precisión sobre su contenido y alcance, pese a constituir una suerte de faro guía desde finales del siglo XIX, solo sucedió en 1965 gracias al trabajo de Jean Pictet, el cual conserva vigencia en la actualidad. En dicho año, la XX Conferencia Internacional de la Cruz Roja recogió en una declaración el trabajo de sistematización y análisis sobre el contenido de los Principios Fundamentales. Su contenido hasta entonces había sido dejado en manos de la costumbre y tenía, según dicho autor, que ser vertido en el derecho escrito pues "[c]ertain ideas of a moral order which it was not permitted to discuss or necessary to explain imposed themselves upon human conscience" (Pictet, 1979a: 133).

Pictet propuso una ampliación de los Principios Fundamentales (a siete en total)[4] y planteó su división entre aquellos fundamentales y extensibles al resto de actores que desplegaba la acción humanitaria, y los principios orgánicos aplicables propiamente al Comité y la Federación Internacional que aglutina al resto de sus filiales en varios países alrededor del mundo (Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja, 2016).

Los Principios Fundamentales que han sido más ampliamente aceptados como orientadores de la acción humanitaria son los de humanidad, imparcialidad, neutralidad e independencia. Son, a su vez, denominados como esenciales los dos primeros, y como principios derivados los dos siguientes. Entre ellos existe una jerarquía en donde el principio esencial es el de humanidad, sin embargo, todos en su conjunto deben permanecer en pie por encima de cualquier contingencia no importa su peculiaridad (Pictet, 1979a).

Según los comentarios de Pictet, estos son reglas de acción basadas en el juicio y la experiencia de actores como el CICR. Reconocen en su existencia la pluralidad de culturas y la riqueza de otros principios. No apuntan a ser valores absolutos ni imperativos más allá de discusión pero son, en todo caso, abstracciones de naturaleza moral que representan una guía de conducta en una sociedad ideal (1979a).

El principio de humanidad es esencial pues "human nature everywhere is the same and there is nothing more widespread than human suffering, to which all men are equally vulnerable and sensitive" (Pictet, 1979a: 134). Pese a las confusiones terminológicas entre humano, humanidad, humanitario y humanitarismo,[5] Pictet aclara que la humanidad como principio de la acción humanitaria tiene su punto de partida en el sufrimiento como una condición común a los seres humanos. Es acción dirigida a curar, pero también a la prevención del sufrimiento a través de dos acciones concretas: su prevención y alivio, y la protección de la vida y la salud de la persona (1979a).

4 Los Principios Fundamentales son los de humanidad, imparcialidad, neutralidad, independencia; y los de servicio voluntario, unidad y universalidad llamados también como principios orgánicos (Pictet, 1979a).

5 Para ahondar en esta diferencia sugerimos Pictet, (1979a) ver pp. 143 y ss.

El principio de humanidad implica acciones de contenido negativo y positivo. Las de contenido negativo se asocian al deber de respetar a los individuos, absteniéndose de hacerles daño y evitando ponerles en peligro. Las de contenido positivo implican el despliegue de acciones tendientes a su protección (Pictet, 1979b, 1979c). Según Pictet, el principio de humanidad es el más universal y menos controversial de los principios de la acción humanitaria (1979a).

El principio de imparcialidad reúne a su vez a los de no discriminación por nacionalidad, raza, creencias religiosas, clase y opinión política, y al de proporcionalidad según el cual la asistencia debe poder ser igual al sufrimiento de la persona considerando, además, que los recursos de la acción humanitaria son finitos y no pueden resolverlo todo al mismo tiempo. La no discriminación obra como regla de acción para descartar, en la entrega de ayuda y cuidado, toda distinción "objetiva" entre las personas beneficiadas de esta. La proporcionalidad a su turno, obra como regla de acción para descartar toda distinción "subjetiva" para beneficiar a las personas según la medida en que lo requieran (Pictet, 1979c, 1979d, 1979e).

La imparcialidad en la acción humanitaria también debe ser entendida como el deber de no tomar partido, ni siquiera por razones de interés o simpatía, al tiempo que prohíbe en su despliegue excluir a nadie que lo necesite de acceder o beneficiarse de la ayuda o alivio (Pictet, 1979e).

El principio de neutralidad, según Pictet, es el más confuso y difícil de diferenciar de otros, como el de imparcialidad. Su evaluación depende de circunstancias particulares. Presupone dos elementos: una actitud de abstención y la existencia de personas o grupos de personas que se oponen unas a otras. Su operacionalización en la práctica implica abstenerse de emitir juicios entre las partes enfrentadas "it is a form of discipline we impose upon ourselves, a brake applied to the impulsive urge of our feelings"(1979e: 311).

La neutralidad debe poder ser desplegada en dos vertientes. La neutralidad militar, donde la acción humanitaria debe abstenerse de tomar partido en las hostilidades. Y la neutralidad ideológica, donde no debe haber toma de postura ante controversias de contenido político, racial, religioso o de naturaleza ideológica –aprendizaje recogido especialmente por el acontecimiento de la Guerra Fría– (Pictet, 1980a).

Y finalmente, el principio de independencia que obra como garante del principio de neutralidad, que orienta a la acción humanitaria de manera que no dependa de otros actores estatales o no estatales política, religiosa o económicamente. Orienta el accionar humanitario como auxiliar de los actores estatales, por ejemplo, en la entrega de ayudas o servicios, pero no puede representar dicho vínculo una puesta en peligro del resto de los principios de la acción humanitaria. Habilita, en últimas, a la toma libre y autónoma de decisiones en el despliegue de esta (Pictet, 1980b).

Esta declaración de los Principios Fundamentales y la consistencia en torno a su contenido fue puesta a prueba en el acontecimiento de sucesivas guerras, conflictos civiles y crisis de hambruna que asolaron a varios países a finales del siglo XX. Las preguntas desde entonces y que hasta ahora han atravesado su

consolidación siguen teniendo que ver, en buena medida, con su alcance práctico y operacionalización en terreno.

Son múltiples y diversos los diagnósticos sobre las patologías de la acción humanitaria que, con mayor o menor optimismo, se han efectuado hasta ahora teniendo como punto en común los principios fundacionales de la acción humanitaria, su contenido y su transformación, según los contextos sociopolíticos de cada época.

Una evolución que se orienta en lo que Thomson señala como el estatus privilegiado de los principios que, operacionalizados correctamente, ofrecen la mejor forma conocida hasta ahora de desempeñar y acceder a los beneficios que promete la acción humanitaria, sin perjuicio de que otro paradigma mejor pueda emerger para ocupar ese lugar de brújula orientadora (2015).

La centralidad de los principios, con su componente conceptual adquiere sentido en adelante para comprender las crisis a las que responde el aterrizaje de las tecnologías digitales en la acción humanitaria y los problemas más o menos nuevos que su uso y despliegue genera.

2. La acción humanitaria que se dirige hacia las personas refugiadas: panorama breve de una crisis compleja

En la revisión sobre la evolución y alcance del derecho internacional de las personas refugiadas y sus diferentes tratados e instrumentos a nivel regional, Hossain Bhuiyan presenta que su nacimiento ha estado marcado por el deseo de los Estados de eximirse o minimizar su rol y responsabilidad en la protección de las personas refugiadas. En la marcada maleabilidad del concepto de persona refugiada, lo que ha permitido la discrecionalidad en la aplicación de los regímenes de protección de internacional; en el cariz politizado de las discusiones jurídicas en torno a dicho marco jurídico; y en la lenta aunque progresiva vinculación entre el derecho internacional de las personas refugiadas y el derecho internacional de los derechos humanos (Islam y Bhuiyan, 2013).

Sin ir más allá a los contornos de esta perspectiva global del autor, aquel apunta a la existencia de retos jurídicos y (geo)políticos que, en la práctica, y según cada época, tornan a dicho marco jurídico en uno más o menos protector de la persona que se ve obligada a huir de su país o lugar de origen por ser perseguida o por miedo a serlo, y que busca en otro Estado oportunidades y protección que le permitan rehacer su vida.

Algunos retos a los que refiere, y en los que coincide Papagianni, tienen que ver con la cuestión operativa y conceptual de dicho marco jurídico. Los retos operativos van desde la posibilidad de la aplicación del derecho internacional de las personas refugiadas a personas inicialmente no cubiertas por sus provisiones (desplazados internos); los debates en torno a las diferencia entre las personas refugiadas y las desplazadas a nivel interno y por qué el tránsito más allá de una frontera internacional debiera marcar una distinción entre los regímenes de protección que se procuran a cada una; la posibilidad de su aplicación extraterritorial en los espacios en que los Estados ejercen control sobre una población o los flujos

migratorios; hasta la responsabilidad de los Estados que deriva de la tercerización de la gestión migratoria en Estados costeros, entre otros (Islam y Bhuiyan, 2013; Papagianni, 2015).

Los cuestionamientos que se asocian a los contornos conceptuales de ese marco, que se refieren, por ejemplo, a si la expresión "miedo a ser perseguida" que motiva a la persona a huir de su lugar o país de origen, es un asunto subjetivo o que debe ser demostrable a través de factores objetivos y suficientemente fundados para ser aceptados por los oficiales de migración. O si la persecución que obra como requisito para reconocer la protección internacional a la persona refugiada puede o no ser ejercida por actores no estatales frente a los cuales, los Estados de origen fallan en proveer protección a la persona que se ve obligada a buscar asilo, por mencionar apenas un par de casos (Bohmer y Shuman, 2008; Islam y Bhuiyan, 2013; Papagianni, 2015).

Se trata de algunos retos que han tenido lugar en la transformación de los flujos migratorios y la acentuación de la migración mixta,[6] así como la securitización de la cuestión migratoria según la cual las personas refugiadas no solo huyen del conflicto sino que contribuyen a este (Betts, 2014; Hammerstadt, 2014) y que, junto a otras variables, ha impactado en la resolución reciente de algunos de estos en sentido desfavorable para las personas refugiadas con las consecuencias a nivel cultural, social, económico, familiar y en salud física y mental que esto genera para ellas.

Dicha resolución se ha traducido en la práctica, por ejemplo, en su criminalización o detención injusta y prolongada, en el olvido de su mera existencia en campos hacinados de refugiados en los que algunos Estados deciden no ejercer control como una forma de abstenerse a reconocer su condición, o en la imposición por estos de requisitos tan estrictos en el proceso de solicitud de asilo que lo tornan en una odisea para muchos, en el "mejor de los casos".

En ciertos eventos se enfrentan incluso a diversas formas de violencia ejercida por autoridades de los Estados, a la persecución, la repatriación o devolución forzadas incitada además por movimientos y discursos políticos anti inmigrantes (Amnistía Internacional, 2016; Council on Foreign Relations, s.f.; Feldman, 2015).

Se trata de "soluciones" que, recientemente, se han recrudecido por al cerramiento fronterizo o la limitación en la libertad de tránsito justificadas por la pandemia de Covid-19 que ha impactado negativamente a las personas migrantes en condición irregular y a las que buscan asilo, pues su condición de movilidad constante ha sido entendida como favorecedora de la propagación del contagio (OECD, 2020; UNHCR, 2020b).

Como sea, y sin intención de ahondar en el estado de cosas de la (des)protección internacional a las personas refugiadas en el presente –lo cual merece además una mirada cercana sobre la región que se trate– conviene considerar que en dicho ecosistema también se relacionan diversos actores que despliegan la acción humanitaria para atender la crisis de refugiados.

6 La migración mixta es el fenómeno en el que "se trasladan personas juntas con distintos objetivos que usan las mismas rutas y medios de transporte o los servicios de los mismos traficantes [que] pueden crear desafíos para los Estados, así como riesgos para los individuos que viajan como parte de tales movimientos […] identificar a los refugiados que van en los flujos mixtos irregulares puede ser un desafío, en especial cuando los mismos individuos tienen varios motivos para trasladarse" (ACNUR, 2010: 9).

La acción humanitaria en este contexto obra como el puente facilitador entre las personas que huyen de sus países o lugares de origen por razones diversas, y los Estados de origen, tránsito y destino (Ferris, 2011; Hathaway, 2005). Su desenvolvimiento puede llegar a marcar la diferencia en su integración local, su retorno voluntario, reasentamiento definitivo o reubicación. En ocasiones, es la única vía de socorro y ayuda en que las personas refugiadas pueden apoyarse ante la inacción o incapacidad de los Estados en proveer reconocimiento a su condición a través de la concesión de asilo (UNHCR, 2020b).

Su rol no solo es esencial en la provisión de ayuda y socorro a personas que se encuentran en extremas condiciones de vulnerabilidad, sino que se estima que tendrá cada vez una más alta demanda en los años que vienen.

A las razones que tradicionalmente han motivado a las personas a huir de sus países o lugares de origen como la persecución, el conflicto, la violencia, la violación de los derechos humanos, las crisis de hambruna, la pobreza, los eventos que perturban gravemente el orden público se suman el cambio climático, así como la pandemia por Covid-19 que ha elevado la condición de vulnerabilidad de quienes ya se encuentran huyendo y que ha motivado a nuevas personas a hacerlo "[e]merging evidence indicates that, in addition to precluding the possibility to flee, in some cases, COVID-19 may also have been a factor in triggering new movement of people in 2020" (UNHCR, 2020b: 56).

El primer reporte de tendencias globales en materia de refugiados publicado en 2012 por ACNUR,[7] señaló que entonces había 45 millones de personas forzosamente desplazadas a nivel global, una categoría que agrupa a las personas refugiadas, solicitantes de asilo, personas en desplazamiento interno y apátridas. Un número que en 2020 había ascendido a los 82 millones en total y que llegará a los 100 millones no en la década que sigue, sino en un par de años (UNHCR, 2020b).

En esa tendencia global, para 2020 había al menos 20.7 millones de personas refugiadas en el mundo –incluyendo a personas en situaciones potenciales de serlo–. De esas tan solo 765.200 personas recibieron protección internacional, ni siquiera el 5% del total de dicha población (UNHCR, 2020b).

Protección internacional que, en todo caso, prestan de manera mayoritaria los países en desarrollo mientras los países ricos han ido disminuyendo progresivamente la disposición hacia la apertura de sus fronteras, y la destinación de fondos capaces de sostener las acciones humanitarias que materializan la provisión de socorro y ayuda a este tipo de personas que se encuentra a cargo de actores como ACNUR y otras agencias humanitarias del sistema ONU, como OCHA (Amnistía Internacional, 2016).

Al respecto, Amnistía Internacional en su informe de 2016 que evaluó el desempeño de distintas regiones del mundo en la atención a la crisis de refugiados que estalló en 2015 sostuvo:

7 En adelante, entendemos que ACNUR, la Agencia de la ONU para los Refugiados y a la que haremos sucesivas alusiones en los próximos capítulos, es un actor no estatal en aplicación del criterio de desvinculación orgánica según el cual dicha agencia no pertenece ni hace parte de la estructura organizativa de los Estados. Reconocemos, según su Estatuto, que se trata de una Oficina que actúa bajo la autoridad de la Asamblea General de las Naciones Unidas, y que pese desempeñar, por acuerdos con los Estados, algunas funciones asociadas a la determinación del estatus o protección internacional de las personas refugiadas, aquella es una función que no convierte a ACNUR en un actor estatal.

> En 2015, la amplitud y el alcance de las crisis humanitarias en todo el mundo sometieron a una presión descomunal al sistema humanitario internacional. De todos los llamamientos a aportar fondos humanitarios (para refugiados y también para otras crisis, como catástrofes naturales) en 2016, la ONU informó de que solo se había cubierto el 40% de los 19.480 millones de dólares requeridos. La financiación de los llamamientos humanitarios para hacer frente a las crisis de refugiados es sistemáticamente, y a menudo gravemente, insuficiente. La complejidad de ciertas situaciones de emergencia relacionadas con personas refugiadas requiere la respuesta coordinada de varios organismos de la ONU, coordinados por ACNUR. Cuando casi se ha cumplido tres trimestres del año 2016, ni siquiera se ha cubierto el 50% de los fondos requeridos en todos estos llamamientos para financiar los planes de respuesta regional (2016: 39).

Para 2020 la situación para actores como ACNUR no había variado. En un reporte publicado a mediados de ese año sostuvo cómo la brecha entre el financiamiento requerido y las necesidades para sustentar la acción humanitaria había llegado a máximos históricos: un 51% de distancia que se hizo más honda en comparación con la década anterior que se había mantenido en mínimos del 36% y máximos del 49% (UNHCR, 2020d).

Para agosto de ese año ACNUR ya había gastado todo su presupuesto anual obligando al cierre, cancelación o desescalamiento de programas de protección a personas refugiadas (UNHCR, 2020a).

En su plan estratégico de 2018-2021 OCHA sostuvo, en relación con el financiamiento de la acción humanitaria que, en general:

> Funding for humanitarian action is higher than it has ever been, but growing humanitarian needs are outpacing available funding and current capacity for humanitarian response. Despite efforts to make the system more effective, the overall funding for humanitarian appeals as a percentage of total requirements has been declining over the past 20 years, significantly limiting the humanitarian system's ability to meet intensifying needs. In 2017, humanitarian appeals totalled over US$24.2 billion– the highest ever. But even with the generosity of donors, the funding gap remained wide. Not only are overall needs outpacing available funding, but the drivers of need and the average length of time that humanitarian assistance is needed are also changing (2018: 10).

Como si fuera poco, a este panorama de discutibles "soluciones" ante la crisis de refugiados que se encuentra aparejada a una crisis financiera de los actores más importantes en la materia, se suma el tradicional condicionamiento de buena parte del presupuesto del que estos actores disponen a través de la figura del *earmarking*, es decir, la manera en que los más importantes donantes estatales deciden hacia qué asuntos, en concreto, deben ser destinadas sus contribuciones.

Situación que condiciona la agenda de trabajo y deja un margen de maniobra limitado para la realización plena del mandato de ACNUR que, como vimos, es el actor humanitario más importante en materia de refugiados antecedido solo por los Estados. A propósito del *earmarking* Gil Loescher aclara:

> The practice of earmarking allows donors to exercise considerable influence over the work of UNHCR as programmes considered important by donors receive considerable support, while those deemed less important receive less support.
> The fact that donors largely contribute to UNHCR on the basis of their own perceived interests makes the concentration of donors all the more problematic. In 2012, the top ten donors were the major industrialized states, with all other countries accounting for less than a quarter of contributions to UNHCR. As a result, the interests of a relatively

> small number of Northern states have been highly influential in determining UNHCR's activities (2014: 5).

Esta situación de dependencia financiera en algunos Estados que cada vez financian en menor medida las crecientes necesidades producto de la crisis de refugiados ha dado lugar, además, a un escenario de alta competitividad por la búsqueda de nuevas fuentes de financiación que permitan una libre disposición de recursos para actores como ACNUR, y otra media docena de oficinas que pertenecen al sistema ONU y que se dedican a la acción humanitaria que impacta igualmente en la vida de las personas refugiadas.[8]

Este contexto de condicionamiento, que no es reciente, sugiere una suerte de disposición de los Estados más ricos en decidir pagar por mantener a los refugiados lejos, y que entraña según Amnistía Internacional y Loescher, relaciones Sur-Norte Global[9] que impactan negativamente en la eficacia de los mecanismos de protección internacional, pues genera tensión en las oportunidades de cooperación entre los países que financian el régimen de refugiados y aquellos otros que las reciben en sus territorios (Amnistía Internacional, 2016; Loescher, 2014).

Al respecto, Jacobsen y Sandvik mencionan cómo ACNUR, por ejemplo, ejerce una posición crítica de las políticas y prácticas hacia las personas refugiados por parte de los países del Norte Global al tiempo que, por la influencia que estos tienen en su financiamiento, actúa como *gatekeeper* o guardián en la gobernanza del régimen de refugiados en el Sur Global, es decir, de manera ambigua ejerce como crítico de un régimen defectuoso mientras toma partido en él como portero o guardián que decide también quién cruza o no la puerta de entrada hacia los países de Norte quienes, en diversas ocasiones, le delegan el poder de determinar el estatus de las personas refugiadas (2016).

La difícil relación entre el financiamiento del actor más importante que coordina y lidera el régimen de refugiados a nivel global, ACNUR, y los Estados del Norte Global, también se reporta en la manera en que este rinde cuentas y se hace responsable por sus actos frente a sus financiadores y frente a los Estados que hospedan sus actividades, pero también frente a las personas que beneficia. Jacobsen y Sandvik dan cuenta del historial negativo de ACNUR en lo que estas llaman como la responsabilidad pasiva y activa; ascendente y descendente de los actores humanitarios.

La responsabilidad pasiva pone en hombros de dicha agencia el deber, según su propio mandato, de monitorear el nivel de cumplimiento de la Convención de

---

8 Incluyendo la Oficina de las Naciones Unidas para Coordinación de Asuntos Humanitarios OCHA, el Programa Mundial de Alimentos, el Programa de las Naciones Unidas para el Desarrollo, la Organización de las Naciones Unidas para la Alimentación y la Agricultura FAO, el Fondo de las Naciones Unidas para la Infancia UNICEF, la Organización Mundial de la Salud OMS, y la Agencia de las Naciones Unidas para los Refugiados Palestinos UNRWA. Ver: https://www.un.org/en/our-work/deliver-humanitarian-aid

9 Si bien entendemos que esta es una categoría epistemológicamente debatida frente a la cual existen extensos trabajos que resignifican, más allá de lo territorial, el sentido de "Sur" y de "Norte", creemos que J. Obarrio aporta una idea de base para efectuar la lectura de esta expresión a lo largo de esta tesis.
El autor sostiene que "[e]l Sur presenta trayectorias interconectadas de imperialismos políticos y económicos, colonialismos externos o internos, conformación e interrupción del estado-nación y despliegue de proyectos de lo nacional-popular […] [e]n la actualidad, el Sur se halla articulado como el territorio de la subsunción real por el capital; el espacio geográfico y económico que es objeto de una nueva ronda de acumulación primitiva del capital, que se lleva a cabo bajo el signo de la absolutización del capital extractivo y el capital financiero" (Obarrio, 2013: 7, 8).

1951 a cargo de los Estados. Deber que en la práctica no se ha materializado pues, sostienen, no deja de ser políticamente complejo exigir responsabilidad de quien te financia y a quien se le pide que amplíe año a año la generosidad de su bolsillo (Jacobsen y Sandvik, 2016).

En esta responsabilidad pasiva también es cuestionable la manera en que ACNUR se relaciona con los Estados que hospedan sus operaciones. En ocasiones, ante regímenes poco democráticos o poco receptivos de los flujos de personas refugiadas y que solicitan el cierre de campamentos, la repatriación o la reubicación de estas en áreas donde su seguridad no puede ser garantizada, se deben efectuar acuerdos y concesiones (Jacobsen y Sandvik, 2016).

Existen acuerdos con el Estado hospedador que tienen lugar en un sistema que garantiza la inmunidad legal de ACNUR y sus agentes, práctica que constituye la norma en el sector humanitario y que los beneficia de la excepción de aplicar el régimen legal del terreno en el que operan.[10] Pese a que ahora existen mecanismos internos en la ONU para dar trámite a eventos en que la conducta de sus agentes humanitarios se encuentra inmersa en acusaciones de violación a los derechos humanos, no suele haber información actualizada sobre el destino o la suerte de los casos y el sentido en que se resuelven (Edwards, 2018).

Un análisis de 2015 que surgió a propósito de las denuncias de crímenes sexuales cometidos en Haití luego del terremoto de 2010 por agentes de Oxfam –una confederación internacional integrada por diecinueve organizaciones no gubernamentales–, se dio a la tarea de revisar ochenta y cinco documentos de quince organizaciones de ayuda humanitaria con presencia a nivel global.

El análisis resalta las reiteradas inconsistencias en torno a lo que estas entienden por responsabilidad o *accountability,* así como la ausencia de prácticas de *enforcement/enforceability* o de obligatoriedad y aplicación en torno a dicho concepto, aunado a la inexistencia de indicadores de medición de apego o cumplimiento a sus propias prácticas (Tan y Schreeb, 2015). Sophie Edwards resume el problema así "self-policing doesn't work" (2018).

En su libro *Doing bad by doing good: Why humanitarian action fails,* Christopher Coyne señala, en torno a esta realidad, algunas dificultades que se suman a los regímenes de inmunidad de los que gozan:

> There are often weak and inconsistent accountability mechanisms within the international humanitarian community regarding reporting, investigating, and adjudicating crimes. For example, investigations of alleged crimes are rarely made public and are often left up to the contributing country, resulting in a large variation in how allegations are handled and reported.*These difficulties are exacerbated by the fact that many humanitarian efforts take place in geographically isolated areas, making monitoring and investigation that much more difficult. Together, these factors lower the probability of a perpetrator being caught, either during or after committing a crime. Further, even if someone is accused, the associated punishment is often unclear or minimal* (Coyne, 2013:159). (Subrayado propio)

Volviendo a los conceptos de Jacobsen y Sandvick, la responsabilidad activa obliga a ACNUR a dictar estándares y lineamientos sobre su propia conducta, es

10 Inmunidad que, para las agencias del sistema de Naciones Unidas, encuentra respaldo en la Convención de Privilegios e Inmunidades de 1946.

decir, a autorregularse. Sin embargo, dichos estándares han tenido un enfoque predominante sobre la cuestión financiera y la pregunta sobre cómo y en qué gasta su presupuesto. Solo a partir de graves escándalos que involucraron a algunos de sus agentes en eventos de extorsión de personas refugiadas para conceder beneficios y acceso al régimen de protección internacional, y hechos de abuso sexual y explotación de menores de edad, se dio un viro aunque no del todo acabado hacia la responsabilidad descendente "accountability to persons of concern is an aspect of protection to which UNHCR still struggles to observe" (2016: 9).

Así, al deber de proteger a las personas refugiadas de amenazas de agentes externos, y ser capaz de responder por ello, se suma también el deber de protegerlas de las acciones desempeñadas por el propio actor humanitario, algo que en la práctica encuentra obstáculos asociados a los regímenes de inmunidad que ya referimos y que ponen a las personas refugiadas en un terreno de desventaja apenas obvia.

Marc Dubois señala cuán difícil puede ser para una persona cuestionar el ideal humanitario asociado a ciertos actores del tamaño de ACNUR, al menos no sin el riesgo de sonar como María Antonieta (2018). Pero no solo se trata del problema de cuán impopular pueda ser que un beneficiario cuestione a su benefactor, se trata también de si el beneficiario, es decir, la persona refugiada, cuenta con el *locus standi* para ejercer acciones judiciales y de qué tipo, contra ese otro frente al cual se encuentra en un plano de desigualdad, incluso en el evento en que no estuviera protegido por ningún régimen de inmunidad.

El *locus standi* o la capacidad legal de ser reconocido como accionante para comparecer ante el sistema judicial, es una discusión que supera los debates jurídicos sobre quién y cómo puede ejercer el derecho de acceso a la justicia en contra de un actor no-estatal, cuya capacidad de comparecer en juicio no deja de estar en entredicho. Es también una cuestión política en donde, la permanencia temporal en un determinado país en el que la persona no ha sido reconocida en su estatus como refugiada, o en un contexto donde "llamar negativamente la atención" puede motivar a las autoridades migratorias que actúan de manera discrecional a no conceder el pedido de asilo, obra a manera de *chilling effect* desincentivando a la persona para imaginar siquiera tales escenarios.

Si bien la Declaración Universal de los Derechos Humanos reconoce que todas las personas gozan del derecho a la igualdad ante la ley al tiempo que las faculta a buscar un remedio efectivo ante las autoridades judiciales, sin excepciones asociadas al estatus de la persona refugiada; y que así mismo la Convención de 1951 les reconoce el derecho de acceso libre al sistema judicial del país contratante en que estas se encuentran y afirma el derecho que tienen de ser tratadas en las mismas condiciones que los ciudadanos nacionales, el *locus standi* que jurídicamente se les reconoce a las personas refugiadas se limita, según Stevens y Eberechi (2019), a su comparecencia en calidad de testigos en procedimientos criminales o de infractores de la ley migratoria en procedimientos administrativos.

Es decir, la mayoría de las veces no cuentan con *locus standi* activo que las habilita para acudir en calidad de demandantes, por ejemplo, en casos criminales de denuncia de abuso o acoso sexual sufrido en los campos de refugio y que pueden

involucrar a actores estatales y no estatales, pues el *locu standi* en esos casos yace en cabeza del propio Estado.

En el análisis de eventos de este tipo y la capacidad que tendrían de acceder a la justicia las mujeres refugiadas asentadas en los campos de Kyangwali, Adjumai, Kirandongo, Rwanmwanga, Arua, Kyaka II y Oruchinga en Uganda, tanto Stevens como Eberechi (2019), sostienen que la inexistencia de Cortes o juzgados en los campos de refugiados o sus proximidades impiden que eventos de esta naturaleza se reporten. En el mismo sentido, S. Edwards (2018) añade que, tratándose de los actores humanitarios, el desincentivo se agrava cuando la víctima no cuenta con vías judiciales accesibles y la única vía posible la obliga a agotar los procedimientos internos de la propia organización en una situación en que ya se ha roto la relación de confianza.

Dicho esto, la responsabilidad hacia las personas beneficiarias de la acción humanitaria de agentes como ACNUR, que Sandvick y Jacobsen (2016) denominan como responsabilidad descendente, comprenderá igualmente a partir del giro, producto de los escándalos que referimos más arriba, el deber de protección asociado a las posibles fallas en el desenvolvimiento de la acción humanitaria producto de la incapacidad o inhabilidad de desplegar los mecanismos de protección internacional para las personas refugiadas, o producto de las consecuencias imprevistas o involuntarias asociadas a las acciones humanitarias bien intencionadas.

La responsabilidad ascendente, complementaria a la responsabilidad activa, pone su énfasis en la importancia de transparentar y establecer límites de influencia en la relación Estados donantes-Estados hospedadores-intermediario humanitario, en donde la realización del mandato de este último no debe ocurrir sin considerar el impacto que tienen en su labor los contextos políticos y sociales tanto a nivel local como global.

Sin embargo, las autoras también reconocen la importancia de que los mecanismos de responsabilidad en el sector humanitario, en general, eleven preguntas sobre el rol de los Estados pues no importa cuán desarrolladas se encuentren las prácticas y la cultura de la responsabilidad pasiva, activa, ascendente o descendente al interior de los actores humanitarios:

> The state is not external to this culture but is, in fact, a key actor to ensure protection to the burgeoning number of refugees in the contemporary political landscape. In other words, no matter how committed NGOs and intergovernmental organizations are to accountability, failing to address the role of the state leaves an important dimension of the accountability issue unaddressed (Jacobsen y Sandvik, 2016: 16).

Capítulo 2

EL ATERRIZAJE DE LAS TECNOLOGÍAS DIGITALES EN LA ACCIÓN HUMANITARIA PARA LA ATENCIÓN DE LAS PERSONAS REFUGIADAS

Las tecnologías digitales aterrizan como una solución a la ecuación que plantea, por una parte, la precariedad de la acción humanitaria producto, entre otros, de la insuficiencia de recursos en que se sostiene y, por otra parte, las debilidades del sistema de responsabilidad de los principales actores humanitarios en la materia y en donde destacan los casos de ACNUR y los propios Estados.

Dicho aterrizaje como "solución" ha ocurrido de la mano de la narrativa de las Tecnologías de la Información y las Comunicaciones para el Desarrollo (o ICT4D por sus siglas en inglés) que se inscribe, como veremos, en la lógica del tecnosolucionismo.

El contexto que sirve a manera de pista de aterrizaje al uso instrumental de las tecnologías en la acción humanitaria para las personas refugiadas se enmarca, tanto en las causas que la han aquejado en la década reciente y que describimos más arriba, pero también en causas anteriores, que se remontan a inicios de siglo.

Entre esas causas anteriores se encuentran el aumento en el despliegue y uso de los servicios de telefonía móvil y de las redes sociales, el creciente rol y capacidad de *lobby* del sector privado en la gobernanza internacional del desarrollo aparejado a su crecimiento como industria a fines de la década de 1990, y la visión de la "buena gobernanza" que, en materia de tecnologías, promovió el modelo de múltiples partes interesadas o *multi stake-holder* para la discusión sobre su rol, futuro y regulación en foros internacionales en donde el sector privado sigue conservando una de las mejores sillas de la mesa.

Este marco general ha tenido lugar hasta ahora, bajo una visión dominante del desarrollo como "crecimiento económico" en el que la pobreza es el fenómeno más importante en materia de desigualdad, susceptible de ser reducido o erradicado. Esto puede ser medible bajo variables y métricas que, según Unwin (2017), sacrifican el contexto en el que habitan los individuos y desprecia el rol de la inequidad en el acceso a otros medios de subsistencia distintos a los puramente monetarios.

Pese a esto, la visión dominante del desarrollo asume la fórmula según la cual, si el sector de la tecnología es la industria capaz de contribuir sustancialmente al crecimiento económico de los países, ha de ser también el instrumento para llevar el desarrollo a aquellos menos aventajados (Unwin, 2017).

Su eco en el diseño de los Objetivos de Desarrollo del Milenio del año 2000 y en los Objetivos de Desarrollo Sostenible de 2015, abrió la puerta a la participación del sector privado y especialmente, el de las tecnologías de la información y la comunicación, para contribuir a la reducción de la pobreza global a través, por ejemplo, de la promoción de las alianzas público privadas en donde los Estados pudieran delegar en estos la provisión de bienes y servicios críticos para el desarrollo, como el acceso a internet y la telefonía celular (Marino, 2021; Unwin, 2017; Willits *et al.*, 2019). No obstante, dicha fórmula, según Unwin, padece de varios problemas.

El primero, la percepción buenista de la tecnología y su neutralidad según la cual su uso posee efectos intrínsecamente buenos o positivos en la vida de las personas "that can automatically do good, or be seen as a 'silver bullet' to 'fight poverty'" (Unwin, 2017: 23). Es una percepción que no considera, por un lado, el acceso inequitativo a las tecnologías de la información y la comunicación y el impacto que esto tiene en las brechas sociales preexistentes, y por el otro, que no advierte los efectos de los intereses de la industria en el diseño y los usos de dichas tecnologías (Unwin, 2017).

El segundo, supone una relación en que las personas beneficiarias del ICT4D tienen un rol pasivo como consumidoras o como emprendedoras de soluciones cuyo diseño y sostenimiento dependen, en todo caso, de la voluntad e interés de la industria tecnológica determinado por sus utilidades y ganancias. En ambos casos, las soluciones para el desarrollo son algo que viene de afuera "without sufficient consideration being given to the needs and contexts of those for whom they are intended" (Unwin, 2017: 27).

El tercero, según dicho autor, es la subversión reciente del ICT4D en una versión en que el desarrollo es una excusa para el uso y despliegue de tecnologías de la información y la comunicación que obran como el nuevo fin en sí mismo "many stakeholders are using the idea of 'development' as a means to promulgate and propagate their own specific technologies, or what might be called 'Development for ICT' (D4ICT)" (Unwin, 2017: 30).

Esta subversión tiene, entre otras, consecuencias como el despliegue y uso de tecnologías digitales aun cuando no se trate de la herramienta esperada o la prioridad más acuciante en un contexto determinado, y que en la práctica ha convertido en ocasiones al Sur Global en una suerte de basurero o sitio de experimentación de las tecnologías desarrolladas en el Norte Global (Burns, 2019; Unwin, 2017; Willits *et al.*, 2019).

Otra consecuencia se relaciona a su despliegue para estimular el desarrollo también conocido como *technological leapfrogging* es decir, situaciones en las que, por ejemplo, circulan tabletas y celulares de última generación sin que exista una infraestructura ampliada de conectividad móvil o incluso una infraestructura eléctrica de base, como una razón en sí misma para que dicha ampliación tenga lugar o dicha infraestructura sea al fin tendida.

Los problemas de esta última visión radican, entre otros, en la extensa capacidad de coordinación para que dicha expectativa resulte siendo operacionalizada de manera exitosa, en otras palabras, se trata de un salto de lógica que cree en la tecnología como motor del desarrollo en escenarios ideales que en la práctica no lo son tanto:

> The role of leapfrogging, within this developmental context, is not an easy one. Technology leapfrogging can exist, but leapfrogging alone does not guarantee, or even encourage, prosperity. This depends on the policy environment, how leapfrogging is operationalised (sic.), who is involved and who undertakes to support initiatives […]
> Furthermore, leapfrogging is a continuous event, and so resources need to be available in the long term. Consequently, it is critically important that all such leapfrogging ventures are carefully planned –amongst other things, this will help to prevent the development of cargo cults (Davison *et al*., 2000: 7).

Así las cosas, frente a las múltiples formas en que se ha precarizado la acción humanitaria que apunta a beneficiar a las personas refugiadas, el ICT4D –y su forma subvertida– se abre camino en el humanitarismo con la narrativa del *branding,* la eficiencia, y la equiparación de los resultados del sector humanitario con la lógica del sector privado.

No se trata de una racionalidad del todo nueva, sin embargo, su traslado al humanitarismo sí lo es e impacta no solo en las geografías del filantropismo, sino en la relación entre donantes, intermediarios y beneficiarios cuyas consecuencias siguen sin ser explorada del todo (Burns, 2019).

Según R. Burns, el *branding* es la práctica de traslado de la reputación marcaria de las grandes compañías del sector de las tecnologías de la información y la comunicación al humanitarismo tradicional con dos propósitos: el primero, elevar la reputación de este último, al tiempo que el sector privado se "vende a sí mismo" como uno valioso para la realización de los fines de la acción humanitaria.

El segundo, para facilitar la asociación entre la reputación marcaria con la entrega de ayuda humanitaria en forma de *software*, *hardware*, datos, entre otros, con lo que esto significa en materia de entrega adicional de una imagen, una cultura y un discurso organizacional inmersos en las relaciones de poder y sistema de valores propios del capitalismo. El *branding* a su vez transforma a los actores humanitarios y los beneficiarios en un solo grupo, el de consumidores, que sirven a los propósitos de desarrollo y crecimiento de la compañía y con ello, de una comunidad o población (Burns, 2019).

Al tiempo, la eficiencia como el discurso que tradicionalmente ha conducido a la privatización de bienes o servicios públicos es explotada por el sector privado de las tecnologías de la información y las comunicaciones en una doble vía que reporta ganancias para el humanitarismo, con la promesa de obtención de los resultados queridos con los mismos –o menores– recursos, y con la rapidez para conseguir dichos resultados en situaciones de crisis en que su despliegue oportuno es esencial. Entre las consecuencias directas de esta promesa, advierte Burns, se encuentra el favorecimiento al repliegue de los Estados, sus roles y responsabilidades como los más importantes actores humanitarios (Burns, 2019).

Y finalmente, la narrativa según la cual "salvar vidas" es también un objetivo del sector privado de las tecnologías de la información y las comunicaciones y no solo de la acción humanitaria. Según Burns no solo se trata de una narrativa reduccionista de los objetivos de la acción humanitaria en sus múltiples formas, sino que genera dudas metodológicas sobre la medición de lo que significa salvar vidas para un sector cuyo modelo de negocio mantiene como objetivo último la generación de utilidad y ganancias, frente a lo cual afirma:

> The history of humanitarianism is dotted with cases in which numbers of "lives saved" have been exaggerated to attract funders who want to increase their "impact" by reporting large numbers of beneficiaries. These two limitations notwithstanding, the logic of saving lives enables private business to leverage simplistic forms of accounting in order to sell products (Burns, 2019: 14).

Toda esta narrativa se enmarca en una tendencia discursiva mucho más amplia que ha distinguido al sector de las tecnologías de la información y las comunicaciones y sus prácticas más allá de su impacto en el sector humanitario, y que Evgeny Morozov (2015) denomina como solucionismo o determinismo tecnológico o tecnoentusiasmo.

El tecnoentusiasmo es presentado por este como el uso del martillo como solución única para el cual todos los problemas se convierten en clavos. Se trata también, según el autor, de una forma de definir los problemas que padecen de una "escasa comprensión, no solo de la naturaleza humana, sino además de las prácticas complejas que engendra esa naturaleza, y de las cuales se nutre" (Morozov, 2015: 26).

Es una forma de ser de la industria tecnológica que despliega herramientas "bienintencionadas" sin importar el contexto, y que son valiosas en tanto que permitan responder a problemas –que tampoco son nuevos–, el logro de una mayor eficacia y eficiencia en los procesos, la lucha por la transparencia, el exceso de información y la necesidad de más y mejores medios para analizarla, entre otros (Morozov, 2015).

La actitud buenista de las tecnologías de la información y la comunicación reafirma el entusiasmo en torno a su despliegue y uso, que se apoya en la creencia de que esta produce efectos que además son intrínsecamente buenos.

Morozov aclara que, no importa si en los supuestos efectos positivos que produce la tecnología no existe una relación causal o de correlación entre los factores que los determinan, el determinismo es también una manera de excluir otras variables que inciden en la realidad por lo que no es sino "an intellectually impoverished, lazy way to study the past, understand the present, and predict the future" (Morozov, 2012: 290).

Unwin también señala la manera en que el determinismo se empeña en reducir nuestra capacidad de ver el todo para hacernos conformar con una parte. La distinción entre una tecnología y la mínima porción de la realidad que nos provee fácilmente nos conduce a creer que lo que vemos es a la realidad por entero, al punto en que, por ejemplo, para una gran cantidad de personas en el mundo lo que sucede en una red social es lo que creen que es la internet "for a large numbers of people, Facebook literally is the Internet" (Unwin, 2017: 33)

La paradoja inadvertida por el tecnoentusiasmo, según dicho autor, es que la intención (¿o amenaza?) de "mejorar o morir" que motiva a los innovadores de *Silicon Valley*, de donde provienen los entusiastas de la tecnología, una vez "llevada a cabo ciegamente, termina por corroer otros valores importantes" (Mozorov, 2015:107) y que, en el campo de la acción humanitaria, puede significar poner en jaque a sus propios principios (Burns, 2019).

Morozov también pone de presente el impacto del tecnosolucionismo en las relaciones inmersas en un sector de la industria altamente cooptada por un grupo pequeño de grandes empresas globales, cuya geografía es igualmente reducida e inalcanzable para las personas que habitan en otros Estados.

Bajo esta mirada entusiasta, dice, se oscurecen las responsabilidades y roles de los seres humanos que intervienen en la toma de las decisiones, pues se empobrece la capacidad de interpelar el poder que tiene dicho sector sobre los Estados y la vida de las personas bajo la racionalidad según la cual la tecnología, como quiera que sea, es imparable y no hay nada que pueda interponerse en el medio –ni siquiera los derechos humanos– (Morozov, 2012).

Mirar de manera crítica al determinismo tecnológico obliga a reconocer el impacto de las tecnologías en las relaciones de poder, según Morozov, pues "[t]hroughout history, new technologies have almost always empowered and disempowered particular political and social groups, sometimes simultaneously–a fact that is too easy to forget under the sway of technological determinism" (2012: 291).

Hacerlo nos recuerda lo que resulta político en torno a la tecnología y el tipo de prácticas y resultados que tiende a favorecer por encima de otras. Sucumbir al solucionismo tecnológico distorsiona el interés de hallar lo político de la tecnología por explicar, en su reemplazo, la política a través de esta. Morozov señala como ejemplo lo que sucede al buscar información de la revolución de 2008 en Egipto y la atención de los titulares de prensa, que se centra en el uso de Facebook para la movilización, antes que en los pedidos sociales que motivaron la protesta. Afirma:

> What is, therefore, most dangerous about succumbing to technological determinism is that *it hinders our awareness of the social and the political, presenting it as the technological instead*. Technology as a Kantian category of understanding the world may simply be too expansionist and monopolistic, *subsuming anything that has not yet been properly understood and categorized, regardless of whether its roots and nature are technological* (Morozov, 2012: 293). (Subrayado propio)

El objetivo de identificar y reconocer los contornos del tecnoentusiasmo no apunta, según el autor, a promover una mirada desde el extremo contrario, la tecnofobia o una postura intermedia como la tecnoneutralidad, no invita a despojarse de la expectativa de que la tecnología pueda llegar a ser parte de un proyecto humano que aboga hacia el cambio. De lo que va es de "trascender la mentalidad racionalista que reformula cada falta de eficacia –por ejemplo, la ausencia de instrucciones perfectas y detalladas en la cocina– como un obstáculo que es necesario superar" (Morozov, 2015: 32).

La mirada crítica de la tecnología propone no entretenerse con la novedad, el discurso de la eficacia, la información y la transparencia, para detenerse en

cambio en preguntas normativas sobre la tecnología y las sociedades y contextos en que se despliegan y a las que impactan, cuestionar lo que de verdad importa: su interacción con el poder, el origen y razón de su legitimidad y su moralidad sin perder de vista, en todo caso, a las personas (tomadoras de decisiones de política pública, desarrolladoras de las tecnologías, personas usuarias, etc.).

Morozov ejemplifica esto último al mencionar cómo, frente a los regímenes autoritarios que monitorean, cooptan y vigilan internet, la pregunta sobre el poder, la legitimidad y la moralidad recae casi siempre en la figura del dictador, evadiendo la importancia de que las mismas preguntas sean elevadas respecto a la Red. La mirada crítica que propone invita a cuestionar "both the logic of technology *and* the logic of society that adopts it; under no circumstances should we be giving technologies –whether it's the Internet or mobile phones– a free pass on ethics" (Morozov, 2012: 298).

Emprender dicha mirada crítica parte por reconocer como punto de partida que las tecnologías no son neutrales. La neutralidad de la tecnología, dice Morozov, se encuentra asociada a la creencia según la cual un cuchillo no es bueno ni malo, sino que su función depende de la persona y la intención con que esta lo usa, según los tecnoentusiastas las tecnologías "no toman partido [y] en buenas manos puede hacer maravillas" (2015: 195).

La afección por el ideal de la neutralidad viene dada por la expectativa de los tecnoentusiastas de eliminar los sesgos producto de la intervención humana, sesgos que aprecian como negativos no por sus resultados e impacto a nivel social, sino por su asimilación a la subjetividad como contaminante del componente científico de la tecnología. Lauren Klein y Catherine D'Ignazio, en su libro "Data Feminism" explican la pretendida neutralidad de los datos y ofrecen una fórmula condensada de dicha racionalidad que aplica también a las tecnologías digitales: "the more plain, the more neutral; the more neutral, the more objective; and the more objective, the more true" (2020: 76).

Una posición llamada por el autor como tecnoestructuralista, presta atención a la intención que subyace en el diseño de las tecnologías de la información y la comunicación o las tecnologías digitales. Las que son ocultas y no tan ocultas, reconociendo el rol y presencia de los sesgos humanos, viendo no a través de los lentes binarios entre lo bueno y lo malo de la tecnología, sino reconociendo que estas son partícipes de estructuras del poder existente o en surgimiento y que, por lo mismo, estas "conceal the ideologies and political agendas of their creators" (2012: 298) lo que invita a preguntar ¿cómo las tecnologías digitales reestructuran las relaciones sociales y políticas?, ¿a qué nuevos actores introducen en determinados escenarios?, entre otros (Morozov, 2015).

Que una tecnología pueda a un mismo tiempo "centralizar y descentralizar, homogeneizar y pluralizar, empoderar y desempoderar" (Morozov, 2015: 196) eleva la importancia sobre las relaciones de poder que influyen en su uso y despliegue así como sus funcionalidades y su variación según la temporalidad que se trate. Examinar las relaciones de poder de la tecnología implica, entre otros, describir y reconocer la estructura del sistema de privilegios y opresión, cómo se configuran y experimentan por las personas en posiciones menos aventajadas, entre otros.

Klein y D'Ignazio (2020) retoman, a propósito de las discusiones sobre las relaciones de poder que se expresan en los datos como insumo de las tecnologías digitales, la importancia de reconocer la "mátrix de dominación" o los cuatro terrenos en que las relaciones de poder se expresan: el terreno estructural de las políticas y las leyes que codifican y organizan la opresión; el terreno disciplinante, que maneja y administra la opresión a través de las burocracias y jerarquías; el terreno de lo hegemónico en que se inscriben las ideas opresivas como la cultura y los medios de comunicación; y el terreno de las relaciones interpersonales, en que el individuo experimenta la opresión.

Este ejercicio laborioso del tecnoestructuralismo que, según hemos descrito al acudir a Morozov, apunta por identificar las relaciones de poder en que se inscriben las tecnologías digitales y sus promesas para compararlas con las necesidades que dice resolver y las personas a las que impacta. A su vez, examina la legitimidad y moralidad de su uso y despliegue así como el papel que desempeñan sus promotores; entre otros, requiere también de un ejercicio anterior al que apunta este descrito: identificar cuales son las voces, enfoques y retos que advierten quienes refieren a las tecnologías digitales que se despliegan y usan en la acción humanitaria en beneficio de las personas refugiadas.

Ahora bien, uno de los retos de adoptar esta postura tecnocrítica de la tecnología en la cuestión de los refugiados y la acción humanitaria es entender a qué sociedad y líderes debemos cuestionar ¿a la del Estado hospedador en que transitan o habitan temporalmente hasta llegar a su destino final?, ¿a la del Estado en cuyas manos se encuentra reconocer la calidad de asilo a la persona?, ¿a la del Estado del que estas huyen? Esta última es una pregunta también urgente si la mirada crítica interpela las cuestiones en torno al poder, la legitimidad y la moralidad que obligan a ponerle un nombre a ese sujeto que lo detenta o ejerce.

También, implica reconocer que, pese a la impopularidad de la tarea, los sujetos de escrutinio no pueden ni deben ser en exclusivo los Estados sino también a los actores humanitarios más importantes en materia de refugiados como ACNUR, y otros que pertenecen al sistema de las Naciones Unidas, o que pertenecen al ámbito no estatal y por supuesto, de los innovadores de *Silicon Valley* que se han puesto la camiseta edulcorada de la acción humanitaria sin apropiarse necesariamente de sus principios. Burns advierte la resistencia a la crítica de estos dos últimos actores "because of humanitarianism's appeal to notions of altruism, global citizenry, and saving lives" (2019: 4).

Mirar de manera crítica las promesas de las tecnologías digitales en esa materia implica reconocer, al mismo tiempo, las fallas de la gestión de la crisis de refugiados a través de la acción humanitaria. Comprender que las geografías del poder en que transitan y habitan las personas refugiadas se manifiestan a través de sistemas dispares y diferenciados de gobernanza como sucede en los campos de refugiados, los centros de detención, los corredores de movilidad por tierra y mar, entre otros.

Después de responder a las preguntas sobre cómo las tecnologías digitales impactan en el poder existente o emergente, cómo se legitima y a quién para la consecución de qué objetivos, y cuál es la moralidad con la que las tecnologías

digitales homogenizan la acción humanitaria que beneficia a las personas refugiadas, la pregunta habrá de ser ¿qué estaremos dispuestos a hacer si la respuesta nos advierte del tránsito sobre un camino peligroso e incorrecto? Morozov no lo dice así, pero la respuesta lógica debería ser el cambio ¿hacia qué?, dependerá del diagnóstico sobre el estado de cosas, la voluntad de los actores involucrados por aceptar el problema, entre múltiples factores.

Sin intención de llegar con este escrito hasta ese estadio de previsión de alternativas para el cambio, lo que se espera con el capítulo siguiente, atendiendo esta visión crítica de la tecnología que hemos descrito hasta ahora, es identificar el estado de la discusión sobre el despliegue de tecnologías digitales en la acción humanitaria dirigida a personas refugiadas. Discusión en la que se espera entender cómo se manifiestan las posturas más o menos cercanas al tecnoentusiasmo, qué escenarios advierten a manera de retos y riesgos quienes participan en ella, qué visión ofrece sobre el (o los) problema(s) que creen que resuelve(n) las tecnologías digitales, entre otros.

***

En resumen. En la sección subtitulada "la acción humanitaria y sus principios" se proveyó un marco conceptual amplio sobre el contenido de los principios de humanidad, neutralidad, imparcialidad e independencia que tienen más o menos una vocación universal entre quienes desenvuelven la acción humanitaria.

Se reconoció, palabras más, palabras menos, que no ha habido hasta ahora una suerte de "época dorada" de la acción humanitaria ni sus principios (Ferris, 2011). Las fallas sobre la operacionalización de estos últimos siguen alimentando debates en la actualidad sobre su conveniencia o relevancia. Sin embargo, los más importantes actores del sistema de ayuda humanitaria de las Naciones Unidas, como ACNUR y OCHA mantienen apego al contenido teleológico que estos proponen.

La historia de la acción humanitaria demuestra que, pese a la idea sobre la importancia de los principios orientadores, su contenido ha sido en repetidas ocasiones puesta en duda o ha sido contradicha directamente. Por ejemplo, en los procesos de entrega de ayuda y socorro en los que la determinación de la calidad del beneficiario como tal, ha dependido no de la condición humana del otro sino de otros factores asociados a una suerte de política del merecimiento dictada por los donantes o los intermediarios de la acción humanitaria.

La discriminación o la distinción entre a quiénes se entrega ayuda y socorro y quiénes no, hace parte del ADN de la acción humanitaria desde su inicio formal que tuvo lugar con el CICR. También lo es la intensa politización de su alcance y cobertura, en donde los Estados actúan como el jugador de mayor peso y poder frente a los actores humanitarios no estatales que, para realizar su mandato, han tenido que ceder a su presión en más de una ocasión; y la producción de efectos indeseados pese a sus propósitos bienintencionados.

La nueva acción humanitaria, que se distingue de ese otro período clásico de consolidación sobre el contenido de los principios y de repetidas experiencias que

hablaban de sus virtudes y defectos; tiene lugar en un escenario de securitización y repliegue de los Estados como actores y financiadores de la misma, situación que ha dado paso al ingreso de otros no tradicionales, como el sector privado.

En la sección sobre cómo es la acción humanitaria que se dirige hacia las personas refugiadas señalamos algunos de los retos operativos y sustantivos que enfrenta el derecho internacional de las personas refugiadas, como la aplicación del marco internacional de protección a las personas en desplazamiento interno forzado o si la interpretación de la expresión "persecución" podría comprender a actores no estatales, entre otros.

Dijimos que la aplicación de este marco jurídico internacional se ha dado en un sentido que, en las últimas décadas, ha tenido lugar en un contexto socio político global desfavorable para las personas refugiadas. La securitización de la migración, la migración mixta, y más recientemente el Covid-19 ha derivado en el cierre antes que en la apertura de las fronteras de los países.

En dicho escenario, rescatamos el valor que tiene la acción humanitaria. Aquella es el puente que media entre las personas refugiadas y los Estados hospedadores y de destino. En ocasiones, es en actores como ACNUR, el más importante actor no estatal en la materia, en quien algunos Estados delegan algunos de sus deberes, como los de determinación del estatus de refugiado, entre otros.

La acción humanitaria es esencial, no solo por su rol de intermediación sino, además, porque los flujos de personas refugiadas aumentarán con los años progresivamente. A la par, el aumento en la demanda no se ha correspondido en las últimas décadas, ni recientemente, con el aumento de la financiación de las necesidades que enfrenta la acción humanitaria que se procura a las personas refugiadas.

La desfinanciación, producto de la distribución inequitativa de recursos así como de la restricción en el bolsillo de los países más ricos acentúa la carga de los países en desarrollo, que tradicionalmente, han sido los receptores de la mayor cantidad de personas refugiadas en el mundo (A. Binder y Koddenbrock, 2013; Binder, 2017; Churruca-Muguruza, 2018). Dicho panorama, aunado a la manera en que los financiadores condicionan a actores como ACNUR y OCHA hacia qué asuntos priorizar su gasto, ha dado paso a un escenario de mercantilización de la acción humanitaria gracias a la mayor participación del sector privado producto de las estrategias de diversificación de recursos a que han tenido que acudir los intermediarios tradicionales del sistema de Naciones Unidas.[1]

Por el rol protagónico que tienen actores como ACNUR en materia de refugiados, prestamos atención a la manera en que su financiación impacta en la realización de su mandato, pero, sobre todo, en cómo este responde ante sus donantes, los Estados hospedadores y más importante aún, las personas refugiadas.

Retomamos los conceptos de responsabilidad pasiva, activa, vertical y horizontal de Jacobsen y Sandvick. El balance sobre cómo ACNUR se dicta normas para regularse a sí y sus agentes (activa), cómo vigila el cumplimiento de la Convención de 1951 por los Estados parte (pasiva), cómo responde ante los

1 En su más reciente informe sobre requerimientos financieros para 2020-2021, ACNUR identificó al sector privado como un sector estratégico al cual acudir para resolver su brecha de financiación y que incluye fortalecer y ampliar lazos con corporaciones, fundaciones y filántropos privados (UNHCR, 2020a, 2020b).

Estados hospedadores (horizontal), y cómo lo hace frente a las personas refugiadas (vertical), deja dudas sobre la ambigüedad con que actúa y por cómo las personas afectadas por el resultado de sus operaciones se ven imposibilitadas de ejercer alguna acción judicial para la defensa de sus derechos.

Las personas refugiadas en ese escenario, se ven en un grado de vulnerabilidad notable. No solo dependen de un actor, un intermediario, amparado en regímenes de inmunidad, sino que suponer accionar en su contra demanda un escenario de ejercicio de derechos ideal, ajeno a las personas refugiadas alejadas geográficamente de los sistemas de justicia o desincentivadas por la idea de provocar decisiones discrecionales de las autoridades migratorias que obren en su contra.

En la última sección, sobre cómo aterriza el uso de las tecnologías digitales en la acción humanitaria para la atención de las personas refugiadas, hicimos hincapié en la continua puerta abierta que representó para el sector privado de las tecnologías de la información y la comunicación, el repliegue de los Estados en la financiación de la acción humanitaria, así como la narrativa global del ICT4D sobre el uso de las tecnologías para el desarrollo y que fue afirmada en los Objetivos de Desarrollo del Milenio del 2000 y de Desarrollo Sostenible de 2015.

La narrativa del ICT4D se apoya en una visión optimista de las tecnologías digitales como vehículos del progreso económico y de erradicación de la pobreza, pese a las desigualdades de base que condicionan aspectos como su acceso, uso y apropiación y que no son las mismas para los países del mundo.

El aterrizaje concreto del ICT4D a la acción humanitaria ha tenido lugar a través de tres estrategias: el *branding,* es decir, como el sector privado de las tecnologías ha apropiado la acción humanitaria como un nuevo producto con las lógicas de mercado que vienen detrás. La segunda es la narrativa de la eficacia, que recuerda su experticia para hacer más y mejor aquello que precisan los actores que despliegan la acción humanitaria en escenarios donde los recursos son escasos y deben ser optimizados. Por último, la apropiación del objetivo de "salvar vidas" como un nuevo *slogan* del sector de las tecnologías, donde cada producto vendido cuenta como una vida salvada.

Hicimos un recuento de los principales despliegues tecnológicos que han tenido lugar en el ámbito humanitario que impacta en las personas refugiadas, y dijimos cómo dichos despliegues se han enmarcado en una visión tecno-entusiasta de la tecnología.

Acudimos a Evgeny Morozov, creador de dicho concepto, quien explica los riesgos y defectos de la mirada puramente entusiasta de las tecnologías digitales. Suponer su buenismo y dar por sentada su neutralidad no solo reduce la complejidad de la realidad a una visión según la cual la tecnología es una suerte de panacea, sino que olvida la importancia sobre la pregunta en torno al problema que se quiere resolver a través de su uso y despliegue y pone en peligro otros valores importantes cuando se lleva a cabo ciegamente esa visión y que, para la acción humanitaria, puede suponer el sacrificio de sus propios principios.

Este propone una mirada crítica que denomina como tecno-estructuralismo. Según esta mirada es preciso desprenderse y dudar de las promesas en torno a la efectividad, la transparencia, mayor información y capacidad de analizarla, así

como la novedad de las tecnologías digitales; para girar la mirada hacia las relaciones de poder que reproduce o amplifica, sobre la legitimidad y moralidad con la que homogeniza o reviste ciertas prácticas o discursos.

Se trata de una mirada que debe poder cuestionar a la tecnología, pero especialmente a las personas que la despliegan y la sociedad a la que impacta y la adopta sin que deba dársele a ninguna un pase libre en materia de ética.

En el próximo capítulo, esa visión crítica será útil para distinguir más fácilmente las visiones y posturas que se acercan o se alejan de la visión tecno-entusiasta. Así, el objetivo del capítulo siguiente es poder proveer un mapa –aunque incompleto– sobre una realidad que no sucede exclusivamente en los escritorios, sino que está ocurriendo al tiempo que se escribe esta tesis con efectos tangibles sobre la vida de personas que se encuentran en situaciones extremas de vulnerabilidad y que huyen de sus Estados o lugares de origen.

Se espera que dicho mapa contribuya a la delimitación de la geografía de una discusión mucho más amplia sobre el uso y despliegue de tecnologías digitales en espacios desregulados y de gobernanza difusa que impactan en la vida de poblaciones en continuo tránsito.

1. Tecnologías digitales, acción humanitaria y personas refugiadas: aproximación a los riesgos para la protección de datos

En el capítulo anterior proveímos un marco de contexto sobre el ideal de la acción humanitaria y sus principios. A su vez, vimos cómo algunos aspectos que dan cuenta de la acción humanitaria que se procura a las personas refugiadas y cómo, en dicho contexto, habían aterrizado las tecnologías digitales para responder a necesidades que advertimos en torno a la eficacia, la transparencia y la optimización de recursos en un escenario de financiación decreciente y de retirada de los Estados como principal actor humanitario.

Con este panorama, la revisión de la literatura que sigue a continuación busca proveer al lector de una geografía de la discusión sobre el despliegue y uso de las tecnologías digitales en la acción humanitaria para las personas refugiadas. Dicha geografía se limita por dos aspectos específicos: idioma, pues se revisa literatura disponible en español e inglés; y tiempo, que comprende un espectro de seis años que se extienden desde el año 2015 hasta el actual.

En la literatura revisada, se seleccionaron[2] artículos publicados en revistas académicas, en *blogs*, reportes o informes de conferencias, capítulos de libros, informes de investigación, entre otros. Se conformó un grupo total de 60 lecturas en cuya autoría participan organizaciones de la sociedad civil, academia, *think tanks*, organismos de las Naciones Unidas, entre otros.

El análisis que sigue busca responder a preguntas como ¿cuáles son los riesgos advertidos por la literatura en torno a la protección de datos de las personas refugiadas expuestas al despliegue de tecnologías digitales por parte de agentes humanitarios?, ¿qué actores destacan como más relevantes en ese escenario y

2 Sugiero consultar la sección de metodología en la que se describe en detalle cómo fue llevado a cabo el proceso de selección de la literatura que se revisa en este capítulo.

qué tecnologías digitales son más comunes en dicho contexto?, ¿qué casos de éxito o fracaso mencionan para demostrar su postura o preocupación en torno a dichos riesgos?

Para facilitar el análisis sobre las preguntas propuestas, presentamos dos niveles de aproximación que son a su vez las secciones de este capítulo: el primero, enfocado en la revisión de los estándares en materia de protección de datos que permitan un punto de referencia sobre las buenas prácticas en dicha materia. En la segunda sección, se presenta la recopilación de los riesgos advertidos por la literatura. Al cierre de este capítulo se recogen algunas ideas de cierre para transitar al capítulo siguiente.

2. Privacidad y protección de datos: el "deber ser"

El derecho a la privacidad es un derecho humano de recepción universal según las Naciones Unidas (UN High Commissioner for Human Rights, 2014). Se basa en "la presunción de que el individuo debe tener una esfera de desarrollo autónomo, interacción y libertad, una 'esfera privada' con o sin relación con otras y libre de la intervención del Estado y de la intervención excesiva no solicitada de otros individuos no invitados" (UN High Commissioner for Human Rights, 2015, prr. 5).

Es un derecho esencial para el libre desarrollo de la personalidad y la identidad de la persona. Es una precondición esencial para la protección de valores fundamentales, incluyendo la libertad, la dignidad, la equidad y la libertad de la intrusión del gobierno lo cual constituye un ingrediente para habilitar la existencia de las sociedades democráticas (UN Human Rights Council Special & Rapporteur on the Right to Privacy, 2019).

La privacidad también está íntimamente asociada a la realización de otros derechos como el derecho a la salud, derechos de raigambre democrático como la protesta, la libertad de expresión y la libre asociación a través de las garantías del anonimato, entre otros. Por tanto, su afectación puede limitar el ejercicio de otros derechos humanos (UN Committee on Economic, Social and Cultural Rights, 2000; UN Human Rights Council Special & Rapporteur on the Right to Privacy, 2019).

Este derecho a la privacidad se encuentra consagrado, con algunas variaciones en su contenido, en instrumentos de alcance global[3] y regional.[4] Su núcleo esencial apunta a la protección de la integridad y confidencialidad de las comunicaciones, el domicilio, la vida familiar y vida personal de la injerencia o ataques arbitrarios o ilegales por parte de terceros.

3 Declaración Universal de Derechos Humanos (art. 12), Pacto Internacional de Derechos Civiles y Políticos (art. 17), Convención de los Derechos del Niño (art. 16), Convención Internacional para la Protección de todos los Migrantes Trabajadores y los Miembros de su Familia (art. 14)

4 En la región americana: la Convención Americana de Derechos Humanos (art.11), en la Declaración Americana sobre Derechos Humanos (art. 5). En la región europea: en la Convención Europea de Derechos Humanos (art. 8), la Carta de Derechos Fundamentales de la Unión Europea (art. 7 y 8). En oriente: la Carta Árabe de Derechos Humanos (art. 16 y 21), Declaración del Cairo de Derechos Humanos (art. 18). En el continente africano: la Carta Africana de Derechos y bienestar del Niño (art. 19). Y en el sudeste asiático: la Declaración de Derechos Humanos de la Asociación de las Naciones del Sudeste Asiático (art.21)

Su ámbito de aplicación se extiende a la información contenida en –y producida por medio de– las tecnologías digitales. Información que puede referirse a la persona, sus comunicaciones, su vida familiar y esfera íntima. La privacidad cobija tanto el contenido de las comunicaciones como los metadatos asociados a ellas pues, de su procesamiento, se puede obtener información detallada sobre los hábitos, comportamientos, preferencias privadas e identidad de una persona. Protege a la persona de interferencias ilegales o arbitrarias cuando emanan del Estado o de personas naturales o jurídicas (UN High Commissioner for Human Rights, 2014, 2015; UN Human Rights Committee, 1988).

El Alto Comisionado en Derechos Humanos de las Naciones Unidas expresó que la aplicación de este derecho no puede discriminar por razones de nacionalidad ni puede ser restringida su aplicabilidad por consideraciones basadas en la extranjería o irregularidad de la persona (2014). Es más, el Comentario General n. 31 del Comité de Derechos Humanos reafirmó que los Estados obligados por el contenido del Pacto Internacional de derechos Civiles y Políticos, deben respetar los derechos fuera de su territorio de la misma forma en que lo harían dentro de sus fronteras (UN Human Rights Committee, 2000).

El Alto Comisionado reiteró que la consagración del derecho a la privacidad en el art. 17 del Pacto de Derechos Civiles y Políticos (2014) no hace excepciones y debe leerse en consonancia con el texto del artículo 26 según el cual todas las personas son iguales ante la ley. Cualquier previsión orientada a limitar la efectividad del derecho a la privacidad según la nacionalidad de la persona debe satisfacer los requisitos de proporcionalidad, necesidad y legalidad para que tenga un carácter legítimo.

La privacidad como derecho humano contiene una facultad que habilita a la persona a ejercer control sobre su información personal cuando quiera que esta esté siendo procesada por terceros (UN Human Rights Council & Special Rapporteur on the Promotion and Protection of the Right to Freedom of opinion and expression, 2011, 2013; UN General Assembly, 2019).

El ejercicio de tal capacidad, reconocida bajo el derecho de protección de datos, se encuentra orientado bajo una serie de principios de adopción internacional y amplio reconocimiento. Aquellos se encuentran contenidos en el Convenio 108 del Consejo de Europa de 1981 y su versión actualizada de 2018,[5] los Lineamientos[6] de la Organización para el Desarrollo Económico y la Cooperación OCDE de 1980, los principios rectores sobre la reglamentación de ficheros computarizados de datos personales de la ONU de 1995, los principios para la Cooperación Económica de

5 Se trata del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, suscrito el 28 de enero de 1981, adoptado en Estrasburgo. Su protocolo adicional al Convenio para la protección de las personas con respecto al tratamiento de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos, suscrito el 8 de noviembre de 2001 en Estrasburgo. Su texto ha sido adoptado por países fuera del ámbito comunitario europeo, comprendiendo por ejemplo a algunos de América Latina como Uruguay, Argentina, y México. Más recientemente, el 18 de mayo de 2018 se modernizó su texto. A efectos de este texto, la referencia al Convenio 108 también comprende su versión actualizada según el texto del Protocolo CETS n. 223.

6 Se trata de las Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales, suscritas el 23 de septiembre de 1980 con el ánimo de ayudar a "armonizar la legislación nacional relativa a la intimidad y que, a la vez que defiendan tales derechos [la intimidad en relación a los datos personales] impidan interrupciones en la circulación internacional de datos" (OECD, 1980).

Asia-Pacífico,[7] los principios del ámbito interamericano adoptados en 2012 y actualizados en el año 2021, y del ámbito africano[8] del año 2020, entre otros.[9]

Todos ellos[10] constituyen el canon o estándares del debido tratamiento de la información personal en las legislaciones de este tipo que han sido sancionadas a la fecha (Wacks, 2015). En lo que sigue, y previo a la identificación de riesgos advertidos por la literatura revisada, haremos una revisión breve de dichos principios sin entrar a discutir el diseño específico de alguna legislación.[11]

En una lectura conjunta de aquellos instrumentos internacionales y regionales, se incluyen *el principio de legalidad y el de lealtad,* según los cuales el tratamiento debe atender a un propósito legítimo consagrado en la ley (como el cumplimiento de un deber legal o contractual, el tratamiento para permitir la provisión de un servicio o bien, etc.) o atender al consentimiento de la persona. La recopilación

7 Adoptados por primera vez en 2005 y actualizados en 2015. Orientados, en esencia, en los lineamientos de la OCDE de 1980 (Charles Raul y Porath, 2020).

8 Que se encuentran contenidos en la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos.

9 Entre otros textos que refieren a la protección de datos de las personas refugiadas añadimos lo previsto por el Pacto Global para las Migraciones, un Informe del Alto Comisionado para las Naciones Unidas, y un informe reciente de la Comisión Interamericana de Derechos Humanos sobre debido proceso para la determinación de la condición de persona refugiada, apátrida y el otorgamiento de protección complementaria, de 2020. Pese a que refieren a la protección de datos y deber de confidencialidad de la información de las personas refugiadas, no proveen un marco ampliado sobre el conjunto de obligaciones, acciones o medidas que deben asumir todos los actores involucrados en el tratamiento de sus datos. No obviamos dichas referencias en todo caso pues afirman el conjunto de estándares aplicables en la materia y al que referimos en los principios de este segundo capítulo.

En 2016 los gobiernos de 193 Estados miembro de Naciones Unidas firmaron el Pacto Mundial para la Migración a través de la Declaración de Nueva York para los refugiados y los migrantes. El Pacto Mundial reconoce la necesidad de proveer un abordaje integral a la crisis de refugiados. Dicho pacto comprende a su vez un Pacto Mundial para la Migración Segura, Ordenada y Regular, así como un Pacto Mundial sobre los Refugiados, ambos del 2018. El Pacto Mundial no es legalmente vinculante. Fija una serie de principios, compromisos y entendimientos entre los Estados negociadores para aproximarse a todas las dimensiones de la migración. En materia de protección de datos la Declaración propone un enfoque de doble vía. Uno en el que se precisa la necesidad de recolectar datos sobre la migración para que los Estados puedan diseñar mejores políticas públicas de abordaje de la migración. Otro, de captura de los datos personales de las personas refugiadas en condiciones que protejan su privacidad sin importar su estatus, debiendo proteger sus derechos humanos en todo momento. En la jornada de huida de las personas refugiadas, el Pacto Mundial para los Refugiados reafirma la necesidad de capturar sus datos personales con el fin de identificarlas para asistirlas y proveerles condiciones de protección. El registro individual de datos podrá ser asistido por el uso de tecnologías biométricas que será coordinado por la Oficina del Alto Comisionado para las Naciones Unidas en colaboración con otros actores (ACNUR, 2018).

También, la Oficina del Alto Comisionado para las Naciones Unidas en 2014 en el informe "The economic, social and cultural rights of migrants in an irregular situation" previó con relación a la captura de datos personales de las personas migrantes y refugiadas el deber de protegerlos a través de "firewalls" para que no fueran accedidos por las autoridades migratorias del territorio en que estas se encontraran (United Nations, 2014). Y por último, el informe de la Comisión Interamericana de Derechos Humanos refiere que la confidencialidad constituye una garantía de protección contra terceros, y que se reconoce a la persona el derecho de acceso a sus archivos. Se debe respetar en el tratamiento de los datos de la persona refugiada el principio de finalidad y se impone el deber de no compartir su información a terceros países salvo que así lo autorice el titular del dato de manera expresa, libre e informada (Comisión Interamericana de Derechos Humanos, 2020).

10 Entendemos que los instrumentos revisados pueden tener una nomenclatura distinta a la de "principios" (como sucede con los lineamientos de la OCDE), sin embargo, usaremos la expresión "principios" pese a que puede existir una variación en el significante de cada instrumento concreto.

11 Presentamos algunos principios de manera integrada debido a la interrelación que sostienen entre sí, con el fin de compactar en algunos casos la revisión que sigue, lo cual no desdice ni de su validez ni de su importancia.

de los datos, además, debe ser llevada a cabo a través de medios leales y legítimos (African Union, 2020; OEA, 2021; OECD, 1980; UN General Assembly, 1995, Council of Europe, 2018).

El principio de finalidad y el de conservación limitada. La finalidad indefinida, incierta, imprecisa o ilimitada se considera ilegal. La legitimidad sobre quién puede llevar a cabo la recolección de los datos depende de las finalidades advertidas que justifican el tratamiento. Finalidades adicionales a la advertida inicialmente precisan por su cuenta una justificación legal (consagrada en la ley o autorizada expresamente por la persona) que debe asociarse a la finalidad inicial, de manera que el tratamiento orientado a nuevos fines no sea inesperado o sorpresivo para el titular de los datos (African Union, 2020; Council of Europe, 2018; OEA, 2021; OECD, 1980; UN General Assembly, 1995).

También prevé que el uso y divulgación de dicha información debe ajustarse a la finalidad específica consagrada en dicho marco legal o la finalidad consentida por la persona quien, previamente, debió haber sido informada de manera suficiente, transparente y accesible sobre quién estará a cargo del tratamiento de sus datos, cómo los protegerá, para qué los recolecta y por cuánto tiempo será tratada su información.

La conservación de los datos debe poder extenderse por un tiempo específico y necesario que permita la realización de las finalidades advertidas. Si los datos se conservan con fines históricos, estadísticos o científicos deberá ajustarse a los tiempos consagrados en una ley específica.

El principio de transparencia. Trata de la necesidad de informar a la persona sobre cómo están siendo recolectados sus datos, qué datos serán recolectados y para qué fines serán empleados, cómo serán asegurados, qué riesgos existen asociados al tratamiento, con qué terceros y para qué fines serán compartidos sus datos, qué derechos tiene la persona titular de los datos y cómo podrá ejercerlos. Información que debe ser entregada de manera clara y accesible antes de que ocurra el tratamiento, pero también, cuando esta eleve pedidos de acceso a su propia información al responsable del tratamiento de sus datos. Cuando el consentimiento no sea la base legal del tratamiento, esta en todo caso debe poder ser informada de manera transparente sobre el tratamiento de su información (African Union, 2020; APEC, 2015; Council of Europe, 2018; OEA, 2021).

El principio de consentimiento. La persona, frente a dicha información, está en la facultad de autorizar o no el tratamiento de sus datos. Su consentimiento, cuando sea prestado, deberá ser previo al tratamiento, expresado de manera inequívoca, libre e informada. Su consentimiento debe poder ser manifestado durante el ciclo de vida del dato si las condiciones del tratamiento varían o son modificadas por su responsable (African Union, 2020; APEC, 2015; Council of Europe, 2018; OEA, 2021; OECD, 1980; UN General Assembly, 1995).

El principio minimización, implica que el tratamiento de la información debe limitarse solo a los datos que sean necesarios, relevantes y adecuados para la satisfacción del objeto o propósito previsto. El propósito del tratamiento debe poder ser realizado con información lo menos invasiva posible (Council of Europe, 2018; OEA, 2021).

El principio de exactitud refiere a la necesidad de que los datos se encuentren actualizados y completos. Su veracidad no debe ser alterada. En caso de encontrarse desactualizados, deben ser borrados o rectificados por el responsable o encargado del tratamiento (African Union, 2020; APEC, 2015; Council of Europe, 2018; OEA, 2021; OECD, 1980; UN General Assembly, 1995).

El principio de seguridad y el de confidencialidad implican el despliegue de medidas técnicas, administrativas y organizacionales razonables que permitan asegurar la protección de la información en contra de accesos, tratamientos o su transmisión a terceros no autorizados o ilegítimos. Dichas medidas deben poder ser revisadas regularmente y auditadas (African Union, 2020; APEC, 2015; Council of Europe, 2018; OEA, 2021; OECD, 1980; UN General Assembly, 1995).

En caso de tratarse de datos que no deben ser divulgados, accedidos por terceros o emplearse para finalidades distintas de las originales, debería poder emplearse medidas para garantizar la confidencialidad y seguridad de los mismos. De manera particular, el Convenio 108 prevé al respecto, que las brechas de seguridad en que los datos del titular se han perdido, han sido divulgados o alterados, el responsable del tratamiento debe notificar a las autoridades de lo sucedido y si esta tiene la potencialidad de perjudicar a la persona en el ejercicio de otros derechos, debe también notificar sin demora (Council of Europe, 2018).

El de responsabilidad y rendición de cuentas dicta que los responsables y encargados del tratamiento de datos adopten activa y continuamente las medidas técnicas y organizacionales adecuadas para garantizar que el tratamiento se adecúa a los principios referidos más arriba. Su cumplimiento debiera ser auditado o supervisado de manera periódica (African Union, 2020; APEC, 2015; Council of Europe, 2018; OEA, 2021).

Además, los principios revisados reconocen un conjunto de derechos al titular de los datos, los de *acceso, rectificación, cancelación y oposición* o reconocimiento del ejercicio de derechos ARCO. El ejercicio de dichas facultades debe poder ser facilitado mediante un mecanismo razonable, ágil, sencillo, eficaz y gratuito (African Union, 2020; APEC, 2015; Council of Europe, 2018; OEA, 2021; OECD, 1980; UN General Assembly, 1995).

Ahora bien, estos principios y el conjunto de derechos ARCO aplican especialmente frente al tratamiento de los datos personales. Sin embargo, existe en el grupo de datos personales un subconjunto de datos frente a los que estos principios y derechos son aplicables y que reciben, a su vez, un grado de protección mayor: los datos sensibles. Los datos sensibles son una categoría especial de datos personales reconocidos así tanto en los principios interamericanos (principio 9), africanos (artículo 14) según el Convenio 108 en su versión modernizada (artículo 6), y los principios de Asia-Pacífico (principio 7).

Son sensibles pues su tratamiento puede derivar en afectaciones graves a otros derechos, en tanto que suelen referirse, por ejemplo, al origen racial o étnico de las personas, sus creencias religiosas, afiliación sindical o a organizaciones de derechos humanos, sobre su salud (sexual y reproductiva), datos genéticos que pueden informar sobre la relación de la persona en procesos o sentencias penales, y los datos biométricos que identifican de manera única a su titular. Información

que puede ser empleada de manera indebida, derivando en eventos de discriminación en contra de su titular.

Los datos biométricos, como una subcategoría entre los datos sensibles, son producto de la medición de los rasgos biológicos o comportamentales de una persona. Estos se dividen, a su vez, en rasgos biológicos tales como su ADN, huellas digitales, su rostro, voz e iris, el patrón de sus venas o densidad ósea, la geometría de las manos u oídos, su olor. Y rasgos comportamentales, como las emociones, el patrón al caminar o al firmar, entre otros. Los datos biométricos son particularmente apetecidos en los procesos de asociación entre un individuo y su identidad personal con dos fines: identificación o verificación (Jain, 2011).

Los procesos de identificación o verificación de la identidad se distinguen no solo por la pregunta a la que cada uno busca responder –¿quién es esta persona?– y aquella, si la persona es quien dice ser, sino especialmente por cómo sucede a nivel técnico. Los procesos de identificación implican la comparación de un dato biométrico transformado en una plantilla (o *template) y* su comparación con cientos de otras plantillas que reposan en una base de datos. La verificación consiste, por su parte, en la comprobación de la coincidencia entre dicha plantilla y otra previamente almacenada de una persona particular. En ambos casos se espera un grado de compatibilidad entre la plantilla provista por la persona y aquella otra contra la cual se la compara (Fairhust, 2018).

Tradicionalmente, los procesos de asociación entre un individuo y su identidad –o verificación– han dependido de (i) lo que sabe la persona (una contraseña o clave), y (ii) lo que tiene una persona (un token, una tarjeta) o una combinación de ambos. Los datos biométricos introducen una nueva modalidad de establecimiento de la identidad a partir de lo que la *persona es*, lo cual, en teoría, adquiere valor pues se trata de información que la persona no puede en principio modificar y, por ello, reduce las posibilidades de fraude y suplantación (Fairhust, 2018; Jain *et al.*, 2011).

Esta característica resulta especialmente atractiva en el manejo de la identidad de una población para la prestación de bienes y servicios o la investigación y prevención del crimen (Jain *et al.*, 2011), entre otros. También sirve para proveer seguridad en actividades cotidianas que son facilitadas a través del uso de las tecnologías digitales en las que la memorización de lo que sabe una persona, como principal mecanismo de seguridad y establecimiento de su identidad, no solo resulta inconveniente sino poco práctica ante la necesidad continua de probar quiénes somos y que somos quienes afirmamos ser (para desbloquear un teléfono inteligente, realizar una operación bancaria, recibir un beneficio social, etc.)

Las ventajas de los datos biométricos para facilitar los procesos de establecimiento de la identidad de una persona, según Fairhust (2018), son al menos cuatro. La primera, se trata de información personal *universal*, es decir, todas las personas la poseen y procesan de manera manual o (cada vez más) automática, permiten identificar a una persona en cualquier parte del mundo. La segunda, se trata de información personal *única*, no hay dos personas con la misma información biométrica. La tercera, se trata de información personal que *permanece* en el tiempo. Y la cuarta, se trata de información que no es ambigua en los procesos de

determinación de la identidad de alguien. Por supuesto, los datos biométricos que permiten concretar mejor esas ventajas son, por lo general, los rasgos físicos o biológicos de la persona puesto que los comportamientos pueden ser menos confiables.

El tratamiento de los datos biométricos, en tanto que jurídicamente datos sensibles, y según la lectura de los principios del Convenio 108, de la región Asia-Pacífico, de la región americana y los de África se ajusta a uno de dos modelos generales de tratamiento.

El primero prevé una cláusula de prohibición con un marco de excepciones limitado. Excepciones que suelen ser de dos tipos: las que se amparan en criterios ajenos al consentimiento de la persona, en donde la necesidad de provisión de un servicio o la realización de una actividad esencial sirve como mecanismo de autorización;[12] y la base que se apoya específicamente en el consentimiento de la persona. Y el segundo, en donde se autoriza al tratamiento solo cuando medidas adecuadas de seguridad hayan sido adoptadas, una vez adoptadas, el consentimiento será también –entre otras previsiones contenidas en la ley correspondiente– la base para proceder al tratamiento.

En el primer modelo se pueden leer previsiones de este tipo:

> El tratamiento de: datos genéticos; datos personales relacionados con delitos, procesos penales y sentencias penales de condena, y medidas de seguridad relacionadas; datos biométricos que identifican únicamente a una persona; datos personales por la información que revelan en relación con los orígenes raciales o étnicos, opiniones políticas, afiliaciones sindicales, creencias religiosas u otras, salud o vida sexual, *estará permitido únicamente cuando se consagren garantías apropiadas conforme a la ley, complementando aquellas del presente Convenio.* (Council of Europe, 2018, art. 6). (Subrayado propio)

Sobre el segundo modelo que advertimos (African Union, 2020, art. 14):

> State parties shall undertake to prohibit any data collection and processing revealing racial, ethnic and regional origin, parental filiation, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or, more generally, data on the state of health of the data subject.
> *The prohibitions set forth in Article 14.1 shall not apply to the following categories where* (Subrayado propio):
> ►Processing relates to data which are manifestly made public by the data subject;
> ►The data subject has given his/her written consent, by any means, to the processing and in conformity with extant texts;
> ►Processing is necessary to protect vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his/her consent;
> ►Processing, particularly of genetic data, is required for the establishment, exercise or defence (sic.) of legal claims;
> ►A judicial procedure or criminal investigation has been instituted;
> ►Processing is necessary in the public interest, especially for historical, statistical or scientific purposes;
> ►Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request for the data subject prior to entering into a contract;
> ►Processing is necessary for compliance with a legal or regulatory obligation to which the controller is subject;
> ►Processing is necessary for the performance of a task carried out in the public interest

12 Ejemplos de estos eventos son citados más abajo en el artículo 14 del Convenio de la Unión Africana.

> or in the exercise of official authority or assigned by a public authority vested in the controller or in a third party to whom data are disclosed.

El tratamiento de datos sensibles –y biométricos–, con apego más o menos riguroso a alguno de estos dos modelos advertidos, se encuentra, en todo caso, sujeto a los más altos estándares de seguridad. Por ejemplo, así se advierte en el ámbito interamericano y en la región Asia-Pacífico:

> Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de causar daños considerables a las personas si se hace mal uso de ellos. Las categorías de estos datos y el alcance de su protección deberían indicarse claramente en la legislación y normativas nacionales. *Los responsables de los datos deberían adoptar medidas de privacidad y de seguridad reforzadas que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los titulares de los datos* (OEA, 2021, ppio 9). (Subrayado propio)
>
> Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. *Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment*. (APEC, 2015, ppio. 8). (Subrayado propio)

En un barrido a nivel global efectuado por la Conferencia en Comercio y Desarrollo de las Naciones Unidas UNCTAD (por sus siglas en inglés), se estimó que para abril de 2020 había al menos 128 países en el mundo de 194[13] [14] oficialmente reconocidos que habían adoptado una ley de protección de datos (UNCTAD, 2020).

En los países que han adoptado una legislación sobre datos personales, se han introducido requerimientos adicionales para permitir a los responsables y encargados, el tratamiento de datos sensibles. Se pueden mencionar los siguientes:

► El deber de elaborar, previo al tratamiento, estudios de impacto en privacidad.[15]

► El deber de solicitar autorización previa a la autoridad de protección de datos para proceder al tratamiento de datos biométricos.[16]

13 El 66% de países contaban con una legislación; 10% tiene un proyecto de ley en curso,19% no tiene legislación al respecto y sobre un 5% no se tienen datos.

14 En América Latina y el Caribe solo Guatemala, Cuba, Belice, Haití, Venezuela y Guyana no contaban con un régimen en la materia. En África, no lo tenían Guinea-Bissau, Sierra Leona, Liberia, Camerún, Burundi, República Centroafricana, Etiopía, Eritrea, Sudán, Egipto y Libia. En Oriente Medio, solo Siria. En el Sudeste Asiático ni Sri Lanka, Afganistán ni Bangladesh. Y en Asia solo Camboya, Timor Oriental y Brunei. Y, por último, en Oceanía no cuentan con legislación de este tipo Papúa Nueva Guinea, las Islas Salomón y Vanuatu. (UNCTAD, 2020)

15 Tal y como sucede en Brasil, donde el responsable y encargado del tratamiento debe describir, entre otros, la metodología usada para la recolección, las medidas de seguridad empleadas, los mecanismos de mitigación del riesgo, entre otros; así mismo en China, por recomendación del *Personal Information Security Specification*; y Suiza (DLA PIPER, 2021).

16 Tal y como sucede en Cabo Verde y Egipto (DLA PIPER, 2021).

►El deber de designar internamente un encargado u oficial de tratamiento de datos si entre los datos recolectados se encuentran los biométricos.[17]

►Exigencia de contar con un consentimiento separado para autorizar específicamente el tratamiento de datos biométricos.[18]

►La prohibición de transferencia de datos sensibles a otros países sin regulación o a terceros sin el mismo nivel de protección.[19]

►Registro de la base de datos, de los procesadores o controladores de datos o el deber de notificación previa al Ombudsman.[20]

Algunos países amplían el listado de datos sensibles para considerar, entre ellos, otros cuyo riesgo de divulgación pueden impactar negativamente en los derechos de la persona.[21]

Entre las regulaciones de alcance regional o comunitario que imponen un estándar igualmente elevado para el tratamiento de datos sensibles destacan, por supuesto, el Reglamento General de Datos de la Unión Europea (o RPGD en adelante) vigente desde 2018.

Este instrumento adopta en su artículo 9 un modelo de prohibición general de su tratamiento advirtiendo un listado exhaustivo de excepciones (diez en total) que tienen como base el consentimiento expreso de la persona, la necesidad por razones de interés público, la necesidad para proteger intereses vitales de la persona, entre otras.[22] Al respecto uno de los considerandos del Reglamento General señala:

---

17 Sucede en China (si se trata del tratamiento de datos sensibles de más de 100.000 individuos), Croacia, Chipre, República Checa, Dinamarca, Estonia, Finlandia, Francia, Alemania, Gibraltar, Grecia, Hungría, Islandia, India, Irlanda, Italia, Laos, Letonia, Lituania, Luxemburgo, Malta, Holanda, Noruega, Polonia, Portugal, Rumania, Eslovaquia, España, Suecia, Reino Unido y Uruguay (DLA PIPER, 2021).

18 Como sucede en China y Corea del Sur (DLA PIPER, 2021).

19 Como sucede en China e India. Sin embargo, otras legislaciones aplican en este sentido las previsiones sobre flujos transfronterizos de datos que impiden la transferencia de datos personales, en general, a terceros países respecto de los cuales no se haya declarado un nivel adecuado de protección (DLA PIPER, 2021).

20 Israel, Kenia, Macao, Filipinas (al menos cuando se trata del registro de datos sensibles de 1.000 personas), Catar, Suiza, Turquía, Emiratos Árabes Unidos y Ucrania (DLA PIPER, 2021).

21 Entre esos países se incluyen a China (que adiciona el número de identificación personal, el número de teléfono personal, el rastreo de ubicación de la persona, y su información de hospedaje); Australia (incluye expresamente las plantillas biométricas), Camboya (los datos personales de los niños y niñas), Egipto (incluye los datos de los niños y niñas), Estados Unidos (datos de los niños y niñas menores de 13 años y recogidos en línea), Honduras (características físicas, morales o emocionales, número de teléfono, correo electrónico), India (contraseñas), Indonesia (incluye datos de los niños y niñas), Kenia (incluye además la información marital, nombres de los hijos, parientes, esposas/sos, detalles de las propiedades), Lesoto (incluye datos de los niños y niñas), México (fotos y vídeos, huellas digitales, geolocalización, firma de la persona), Suiza (perfiles de personalidad), Turquía (información sobre la vestimenta de la persona). Casos paradigmáticos como el de Turquía contemplan incluso como sanción las penas de prisión frente al indebido tratamiento de los datos sensibles (DLA PIPER, 2021).

22 Los diez eventos se expresan así en el Reglamento: "a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;
c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una

> Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales (Reglamento General de Protección de Datos, 2016, consid. 51).

Además, exige a los responsables del tratamiento (tanto responsables[23] como encargados),[24] dada la propensión al riesgo de este tipo de datos:

► Llevar a cabo estudios de impacto en privacidad (art. 35, secc. 3, lit. b).

► La designación de un oficial de protección de datos si el tratamiento de datos. sensibles constituye la actividad principal del responsable o el encargado procesador (art. 37, secc. 1, lit.c).

► Adoptar medidas técnicas y organizaciones basadas en el alto riesgo asociado al tratamiento de esta categoría especial de datos.

► Las previsiones sobre protección de los datos sensibles deben ser parte de las reglas corporativas internas o políticas de protección de datos vinculantes al responsable del tratamiento cuando este realiza transferencias de datos a un tercer país, una tercera empresa o grupo de empresas unidas por la misma actividad económica (art. 47, secc. 2, lit. d).

En definitiva, podemos decir que, el tratamiento de datos sensibles, exige al responsable tanto en el ámbito público como privado (i) la aplicación general de los principios de la protección de datos, (ii) la implementación de medidas técnicas y organizacionales que permitan asegurar dichos datos de los elevados riesgos a que son expuestos por su tratamiento, (iii) la realización de estudios de impacto en privacidad, la designación de un oficial de datos personales, entre otras.

---

fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional" (Reglamento General de Protección de Datos, 2016: 34).

23 Art 4, num 7 "«responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento" (Reglamento General de Protección de Datos, 2016).

24 Art. 4, num 8 "'encargado del tratamiento' o 'encargado': la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento" (Reglamento General de Protección de Datos, 2016).

Las exigencias vistas dan cuenta, en su conjunto, del interés mayoritario de los reguladores en la materia que pueden resumirse como de exigencia al responsable del tratamiento de la debida diligencia frente a información personal cuya divulgación, pérdida, modificación o acceso no autorizado tiene el potencial de impactar negativamente en el ejercicio de los derechos de su titular.

Riesgos para la protección de datos: del *deber ser* a lo que *es*

Con este trasfondo, la pregunta que busca resolver esta subsección es ¿qué riesgos advierte la literatura sobre el impacto en el derecho a la protección de datos de las personas refugiadas en escenarios en que actores humanitarios capturan y dan tratamiento a su información personal?

El valor de la privacidad para las personas refugiadas

Pese a las condiciones de vulnerabilidad que enfrentan dada la situación de huida de sus países o lugares de origen y el arribo a lugares en los que se encuentran ante contextos culturales, sociales, políticos y legales ajenos; las personas refugiadas conceden a la privacidad y la protección de sus datos un papel importante por el impacto que tiene en su jornada de arribo hacia el lugar en el que poder hallar protección, acogida y solicitar asilo.

Según Latonero, las personas refugiadas reconocen que los datos recogidos sobre ellos pueden llegar a ser usados en su contra, por eso no solo cuidan sus dispositivos móviles sino que, en ocasiones, pueden mantener reservas o incluso pueden llegar a negarse frente a la recogida de sus datos más sensibles, incluyendo los biométricos (2019). Kaurin, por su parte, manifiesta que los procesos de recolección de sus datos pueden generar una sensación de castigo o proceso punitivo sobre las personas refugiadas que son expuestas a procesos de captura intensiva de su información, en ocasiones siendo obligadas a ello, situación que en su conjunto termina contribuyendo a reafirmar estereotipos en contra de la población refugiada (2019).

La protección de datos no es un derecho de interés menor para personas que buscan, como prioridad, la preservación de su propia vida e integridad. Pero su ejercicio, por las condiciones de las que provienen y motivan su huida, aunado a la urgencia de hallar protección y gozar de medidas de asilo, sitúan a estas personas en condiciones en las que ocupan el extremo más débil en relaciones de poder que se extienden también en el ámbito humanitario.

De hecho las preocupaciones de algunas personas refugiadas en torno a la protección de su privacidad es igualmente intensa a la de protección de su vida cuando la motivación por la que huyen de sus lugares de origen tienen ver que ver, por ejemplo, con persecución política, amenazas de muerte violencia por prejuicio en su contra (Latonero y Kift, 2018).

Así, los riesgos que se advierten a continuación, no se presentan frente a un titular del dato "ideal" al que suelen referirse las regulaciones de protección de datos, sin perjuicio de que, como lo advertimos páginas más atrás, todas las personas sin excepción son titulares del derecho a la privacidad y sus garantías que cubren, por supuesto, el derecho a controlar quién, cómo, por qué y para qué recolecta sus datos personales y sensibles.

En su lugar, las personas refugiadas, como titulares de los datos, se pueden encontrar en una posición de especial vulnerabilidad que se refleja, al menos, en: i) una menor capacidad de oposición ante los tratamientos por el temor a la alternativa –la no protección–; ii) el reconocimiento de que el procesamiento y custodia de sus datos no solo afecta a su privacidad sino, potencialmente, su vida e integridad. Una tensión en la que, por un lado, la no entrega de los datos puede suponer la denegación de protección internacional mientras que la entrega de los mismos puede derivar en una renovación del riesgo del que escapan. Esta situación supone afectaciones, jurídicamente, a la institución del consentimiento como base de la regulación de protección de datos y a los derechos afectados directamente más allá de la privacidad o intimidad.

La captura de datos: ¿una actividad necesaria?

La recolección de datos de las personas refugiadas pese a que no es una actividad principal de agencias del sistema ONU, organizaciones de la sociedad civil, organizaciones no gubernamentales, entre otros, dedicados a desplegar acciones humanitarias en beneficio de las personas refugiadas, parece ser –sin que sea del todo evidente por qué– indispensable para la realización de su cometido.

Así, actores como ACNUR o el Programa Mundial de Alimentos, dicen requerir datos personales de las personas refugiadas para determinar, por ejemplo, a quiénes, qué tipo de ayuda y cuánta asignar o proveer a las personas beneficiarias.

En el caso de ACNUR se precisa la recolección de datos personales para llevar a cabo los procesos de asistencia en la solicitud de asilo, así como para la búsqueda de alternativas de protección internacional (como la repatriación voluntaria, su reasentamiento, etc.), incluso para la búsqueda de las familias de menores de edad refugiados perdidos (Kuner *et al.*, 2017). No es, en definitiva, una actividad baladí. Autores incluso la califican como de vida o muerte al constituir una puerta que facilita, para la persona refugiada, el acceso a bienes o servicios valiosos (Kuner *et al.*, 2017).

La pregunta que generan estas apreciaciones límite, como la de Kuner, es ¿qué sucedería en el caso en que no se recogieran datos personales en absoluto o se recogieran en una mínima cantidad? ¿No podrían ser llevadas a cabo las actividades de asistencia? ¿Obstaculizaría ello el fin esencial de las organizaciones de ayuda? ¿Es esta una actividad de la que dependen las operaciones de los actores humanitarios? En definitiva ¿en qué razones se funda el tratamiento de datos en dicho contexto? Pese a la relevancia de preguntas de este tipo, la literatura examinada no indagó sobre el particular.

Basta señalar, por ahora, que la 37 Conferencia Internacional de Comisionados de Privacidad y Protección de Datos (2015) afirman que "data processing is an integral part of the performance of the mission of humanitarian actors and that the increasing use of technological solutions *to respond to demands of more efficiency* leads to a diversification in the nature of the data collected and to an increase in its number and in data flows". (Subrayado propio). Sobre la relación entre eficiencia del gasto y despliegue de tecnologías intensivas en datos, ahondaremos un poco más en el capítulo tercero para proveer algunas ideas que pueden orientar el análisis en torno a la necesidad de esta actividad en la acción humanitaria.

Qué datos se recogen en la acción humanitaria

Los tipos de datos recolectados en estos procesos son diversos y son requeridos en vastas cantidades a través de formularios, o de manera repetitiva dependiendo el actor humanitario que la solicite. Puede comprender información sobre eventos de violencia sexual, tortura, crímenes de guerra o crímenes de lesa humanidad experimentados por la persona durante su jornada de huida de su país o lugar de origen; datos de su procedencia y su jornada de huida; así como datos biométricos como el iris, las huellas digitales y fotografías del rostro, todas procesadas a través de sistemas de reconocimiento biométrico (Kaurin, 2019).

Latonero (2019) también señala que, cuando la recogida de información sucede al tiempo por actores humanitarios y actores estatales en escenarios de frontera, puede implicar la solicitud de datos personales comunes como el nombre, la fecha de nacimiento, la revisión o decomiso del dispositivo móvil de la persona, lo que va aparejado a la solicitud sobre su número celular, la revisión de su historial de búsqueda, la descarga de metadatos de su teléfono móvil, entre otros.

En el caso de ACNUR, el proceso de recepción y registro de la persona refugiada, y que se lleva a cabo para identificarla, comprende, durante la entrevista, la captura de datos sobre la religión de la persona; sexo; origen étnico; estatus marital, nombre y apellido de su pareja (UNHCR, 2020c). Como datos sensibles, también recolecta datos biométricos de la persona (iris, huellas y fotografía) tanto de adultos como niños desde los 5 años o antes. Y datos de naturaleza no sensible como el nombre de la persona, lugar y fecha de nacimiento, educación, ocupación, fecha de salida del país, medios de viaje, países de tránsito, entre otros (UNHCR, 2018c).

3. Estado del arte de riesgos en materia de protección de datos: lo que sugiere la literatura

En lo que sigue, abordaremos los riesgos identificados para la protección de datos de las personas refugiadas según la literatura revisada. Para ello, mostraremos en la tabla que sigue una relación de riesgos que agrupamos por cada uno de los principios vistos. Empezamos con el principio de consentimiento pues es un eje articulador no solo de los otros principios sino del tratamiento de datos como un todo.

Veremos que los riesgos identificados para el principio de consentimiento informado, así como frente al resto de los principios se origina en la fragilidad de la condición base del ejercicio del derecho a la protección de datos: el respeto a la libertad y el reconocimiento de la autonomía de su titular.

Riesgos asociados al principio de consentimiento

Según los riesgos señalados por la literatura en relación con los principios de la protección de datos, el consentimiento es uno de los de mayor preocupación o interés. Los riesgos denotan problemas que revelan el desconocimiento a la libertad y autonomía del titular de los datos. También, exponen la debilidad con que sus condiciones (que sea expreso, previo, libre e informado) se operativizan en la práctica. Condiciones inaplicadas que, un escenario en el que decir *no* a la entrega de datos biométricos para recibir asistencia humanitaria, significa de plano no acceder a la misma.

Problemas del consentimiento en tanto que informado. En cuanto a la información como garantía y requisito del consentimiento, los problemas que fueron identificados tienen que ver con la ambigüedad o falta de claridad en su provisión por los agentes de organizaciones humanitarias o la falta de habilidad en su traducción en términos sencillos por los mediadores culturales que conocen los contextos, idioma e indagan en las preocupaciones de la persona y están dispuestas a facilitar su llegada a los campos de refugiados (Jacobsen, 2016; Kaurin, 2019; Latonero *et al.*, 2019).

Así mismo, en materia de información, las barreras culturales y el idioma en el que se entrega son asuntos igualmente relevantes que fueron advertidos por Latonero y Kaurin.

En materia cultural, la visión de la privacidad de la agencia u organización humanitaria que recolecta la información y la visión de la privacidad de la persona pueden distar profundamente, pudiendo constituir para esta última, en principio, un derecho de interés colectivo cuya faceta más intensa no es la protección de los datos sino la de ser dejados solos o no ser molestados en grupo (Latonero *et al.*, 2019).

En materia de idioma, los formatos o políticas de protección de datos en los que se encuentra la información sobre los propósitos de la recolección no se encuentra traducida a su idioma de origen y, cuando es presentada por agentes humanitarios, su texto no es traducido punto por punto o de manera literal, por lo que se abre una brecha entre lo que dice el formulario y lo que se dice que este contiene que pone en cuestionamiento el carácter informado del consentimiento.

Dragana Kaurin añade que las brechas culturales y de idioma se amplifican ante la vulnerabilidad de las personas refugiadas que pueden haber experimentado en su jornada de huida eventos traumáticos, haber desarrollado desorden de estrés postraumático, persecución estatal y violencia. Condiciones que conducen a la persona a aceptar los términos de lo que sea que les sea ofrecido por actores humanitarios, incluso si ello significa sacrificar en el medio su privacidad:

> *Once we arrived in Moria [refugee camp] they took us to registration. They said "Give us [your] fingerprints, this is to show you're legal for 6 months." I didn't ask who this is for, I just wanted to follow orders. I still have fear from my own police and military, and I didn't even think once to ask* (2019: 11). (Énfasis original).

Otra experiencia que cita Kaurin pone en evidencia cómo no todas las personas refugiadas experimentan la vulnerabilidad de la misma manera y hallan en las tecnologías digitales que tienen a la mano, como su teléfono celular, una vía para sobreponerse a las barreras de acceso a la información que pueden tener lugar en los procesos de tratamiento de sus datos. Sin embargo, el idioma persiste como un problema:

> *Everything I know about the process, and what is going to happen to us, I learned through Google. No one tells you anything.*
> *I got moved back from Germany to Italy because of [the] Dublin [Regulation], I didn't know about it back then. So, I started finding more information online, like the 1951 Refugee Convention online, and the UNHCR* [Handbook for Registration]*. It's good to have this online, but it's only in English.* (2019:11). (Énfasis original).

Tabla 1. Hallazgos de riesgos en materia de protección de datos

Criterio	Riesgos de personas refugiadas
Principios protección de datos	Principio de consentimiento
	No ser informados plenamente o no estar en capacidad plena de entender los propósitos de recolección de su información personal (por escepticismo o barreras culturales, de idioma, etc.)
	Ausencia consentimiento significativo, incluso ser obligados a la entrega de sus datos personales como mecanismo de presión para la entrega efectiva de la ayuda humanitaria
	Principio de finalidad y conservación limitada
	Compartición, acceso y usos no autorizados de datos personales a individuos y Estados de los que huyen
	Compartición, acceso y usos no autorizados de datos personales a autoridades migratorias o de policía del Estado hospedador, así como por compañías privadas incluyendo a las del sector tecnológico
	Que la información recogida para un fin concreto, como la entrega de ayuda, termine siendo empleada por terceros para efectuar
	Ausencia de transparencia en las razones por las que la información que se recolecta es capturada
	Cruzamiento e interoperabilidad de las bases de datos sensibles de personas refugiadas con otras bases de datos sin haber recibido previamente información al respecto
	Ausencia de información sobre con quiénes es compartida la información recolectada
	Repatriaciones involuntarias, persecución o reasentamientos forzosos, rastreo de su ubicación con fines de seguridad, entre otros.
	Principio de exactitud
	Inconsistencias y errores en los procesos de recogidas de datos que impactan negativamente en su utilidad, impidiendo a la persona refugiada acceder a bienes o servicios en el ámbito humanitario
	Principio de seguridad y confidencialidad
	Brechas de seguridad
	Acceso accidental de terceros maliciosos a las bases de datos
	Indebidas prácticas de almacenamiento y compartición no segura –no cifrada– de la información
	Que la persona afectada no sea notificada de fallas de seguridad de sus datos personales
	Ausencia de información sobre las medidas de seguridad de la información recolectada
	Principio de transparencia
	Ausencia de auditorías públicas, transparentes y el seguimiento a sus resultados
	Derecho de acceso, rectificación, cancelación y oposición
	Imposibilidad de su ejercicio por miedo
	Quejas ante agencias humanitarias como ACNUR no tienen mecanismos garantes del anonimato
	No hay información disponible sobre el ejercicio de estos derechos en el idioma de las personas refugiadas
Marcos legales y mecanismos de protección	Ausencia de leyes de protección de datos en países del Sur Global con estándares apropiados en la materia
	Inaplicación de regulaciones que tienen los más altos estándares en protección de datos
	Imposibilidad de accionar por la vía legal contra agencias humanitarias por los regímenes de inmunidad que les protege

Fuente: Elaboración propia.

Estas fallas en la provisión de la información derivan en escenarios en los que las personas refugiadas no comprenden plenamente para qué se recolectan sus datos, cuáles son los objetivos que permiten realizar esos datos; por cuánto tiempo serán conservados; con quiénes serán compartidos y si entre esos terceros se encuentran o no las autoridades de los países de los que huyen o las autoridades de los países que los hospedan; qué mecanismos existen para cuestionar la recolección de datos, o para solicitar la corrección o eliminación de los que ya han sido entregados. En ocasiones ni siquiera se les informa, durante el proceso de la entrevista, quién la está realizando.

En el caso de ACNUR, las dudas aumentan por el uso y despliegue de sistemas de identificación biométrica. Preguntas sobre qué sucede ante la negativa de entrega de datos biométricos, cómo cuestionar los resultados del sistema de identificación biométrica que identifica de manera errónea a la persona; qué mecanismos existen para corregir los datos biométricos que ya han sido entregados, o si existe la posibilidad de retirarlos del sistema una vez registrados; o el tiempo por el que será necesario actualizar los datos biométricos registrados, entre otros.

En la página web de dicha agencia, en la que se proveen guías en el manejo y registro de la identidad de las personas refugiadas, no aparece de manera clara u organizada para la persona refugiada dicha información, ni es accesible para personas que no sean agentes de la organización o de otras organizaciones aliadas. Para ampliar o responder a algunos de esos interrogantes remite en varias ocasiones a la lectura de la política de tratamiento de datos interna, que tiene más de 60 páginas en inglés.[25]

D. Kaurin apunta una crítica en este mismo sentido:

> The *UNHCR Handbook for Registration* (UNHCR 2003) is clearly geared toward humanitarian practitioners, as it misses key points of the process and is available only in English and French, which is not representative of the languages most refugees in the European Union speak (2019: 11).

Por su parte, Duffield (2016) señala cómo la rapidez del proceso de captura de los datos de la persona refugiada puede no solo evitar que la información se entregue de manera clara y plena, sino que la falta de tiempo es también un mecanismo diseñado para evitar que surjan preocupaciones al respecto "the need

25 Al respecto, la guía que se describe en dicha página web se encuentra seccionada en ocho pasos. El quinto paso titulado "implementing registration within an identity management framework" no enseña un modelo de consentimiento informado y coloca en pies de página alguna información relevante (UNHCR, 2018a).
Dice, por ejemplo, en el subpaso 5.2, en el pie de página número cuatro, que "if appropriate, recall that while registration is a prerequisite to recognition of refugee status and assistance in obtaining a durable solution, it does not necessarily lead to either of these outcomes." (UNHCR, 2018c).
En el pie de página número cinco "Where the host government leads registration procedures, the requirement to share personal data including biometrics (and the related right to object) may be determined according to government policy, not UNHCR policy" (UNHCR, 2018c).
En el pie de página número seis "Consent should be informed and freely given. Informed means that the individual is provided information and able to understand the circumstances, purpose, risks and benefits of sharing personal information. Information should cover all of the envisaged data processing activities to be carried out, in particular which data elements will be shared with host government, implementing partners or other third parties. Freely given means that the individual has a genuine choice and is able to refuse or withdraw without adverse consequences." (UNHCR, 2018c).

for speed demanded by the humanitarian imperative has repeatedly been used to override concerns." (Duffield, 2016: 158). Sobre el tiempo, por ejemplo, actores como ACNUR señalan lo siguiente sobre el proceso de registro de una persona refugiada para identificarla:

> [En la provisión de información] It is important *not to rush* through the introduction, despite the fact that staff may do it many times in one day. Individuals should be given ample opportunity to *ask questions* and voice concerns before moving to the data collection stage of the registration interview (UNHCR, 2018a). (Énfasis original)
> [En la captura de los datos biométricos de la persona] Staff should strive to capture all available biometrics. Occasionally, however, fingerprints or irises may be difficult or impossible to capture. A person's biometrics can, in general, be recorded in 90 seconds; *staff should not spend longer than five minutes* on one individual before marking 'unable to capture' in BIMS and identifying the reason (UNHCR, 2018a). (Subrayado propio).

Autoras como Katja Jacobsen (2016), una de las más destacadas en los estudios sobre el despliegue de tecnologías digitales en la acción humanitaria, advierte que la información que se provee a las personas refugiadas sobre la captura de sus datos y su uso, sucede en "campañas de información" de contenido general que se entrega a las personas que habitan en los campos de refugiados. No es un proceso informativo separado, dedicado específicamente a ahondar en las políticas de protección de su privacidad y protección de sus datos por lo que "it is difficult to know exactly what type of information refugees are given when biometric technologies are being introduced" (2016: 168-169).

Autores con preocupaciones sobre el principio de consentimiento dan cuenta de una suerte de brecha entre lo que *debe ser* y lo *que es* en materia de protección de datos, es decir, entre lo que dicen las políticas de tratamiento y protocolos diseñados por los propios actores humanitarios, y lo que es, según se percibe de lo que saben –o no saben– las personas refugiadas una vez se les pregunta si fueron informadas plenamente sobre el tratamiento de sus datos frente a dichos actores. Al respecto, Latonero señala que

> [w]hile many institutions require informed consent protocols, the lived reality on the ground is often far from the ideal. During interviews, it was rare for migrants to say they knew about the kinds of information that would be asked of them when they arrived in Italy. (Latonero *et al.*, 2019: 28)

Sobre actores como ACNUR, Katja Jacobsen pregunta en relación con dicha brecha informativa "[w]hat happens to the biometric data collected by UNHCR? With whom is it shared and in what form? These are the types of questions that UNHCR has not provided refugees with clear answers" (2016: 168-169). En una entrevista a migrantes y refugiados en Italia, Latonero concluyó en relación con ambos grupos de personas que "[t]here was a general confusion about what data is used for what purpose and how such data collection may harm or help [them]" (2019: 33).

Problemas del consentimiento en tanto que expreso. Al final, cuando llega la hora de manifestar el consentimiento para la entrega de datos biométricos ante

agencias como ACNUR, la decisión se reduce a una casilla de *sí/no* que deja una advertencia vaga y abierta sobre la posibilidad de que sus datos sean compartidos con terceros. Al respecto, Kaurin señala (2019):

> The process is similar when the UNHCR runs registration, although it is not any more informative for the asylum seekers. The final question in the general form used to register individual asylum claims is the following:
> *In seeking a durable solution for you in the future, do you authorize UNHCR to share information contained on this form with other agencies and/ or governments as may be required? Yes/No.* (2019: 4) (Subrayado propio)

A veces dicha casilla ni siquiera es marcada por la persona titular de los datos, o no se le informa sobre su significado o contenido que se presenta en otro idioma. Esta situación, sobre la reducción de la autorización a una casilla de *sí/no*, fue también advertida por Human Rights Watch en un informe sobre la compartición de las bases de datos de ACNUR con información personal y biométrica de personas refugiadas del grupo étnico musulmán Rohingya, a las autoridades del Estado hospedador (Bangladesh) que los compartió, a su turno, con las autoridades del país del que estas huían (Myanmar). Allí, la organización de derechos humanos expresó:

> […] on a receipt printed out and given to refugees only in English, had been checked "yes," although he was never asked. He was one of only three among the refugees interviewed who could read English.
> Human Rights Watch viewed the English-only receipt that UNHCR gave to Rohingya refugees after their registration. It includes a box noting "yes" or "no" as to whether the information can be shared with the Myanmar government (2021).

Las consecuencias de una equis sobre una u otra casilla son reales. Según Human Rights Watch, se estima que se compartieron los datos de al menos 830.000 personas con información sobre su composición familiar, lugares de origen e información de familiares en el exterior, así como su información biométrica.

Las personas entrevistadas por dicha organización afirman no haber recibido información alguna sobre los riesgos asociados a las opciones que había que marcar –o que ya venían marcadas– en el formato de consentimiento informado "UNHCR staff told Human Rights Watch that they did not discuss any specific risks with Rohingya before registering them, and the Rohingya interviewed said they were not told about any such risks" (2021).

Problemas del consentimiento en tanto que libre. Las personas refugiadas, por ciertos factores tales como el trauma experimentado en su jornada, las costumbres culturales y las relaciones de poder en las que son la parte más débil en la relación de recolección de sus datos, se abstienen de pedir más información o formular quejas que puedan parecer un cuestionamiento a la autoridad de ese otro extremo que hace las preguntas "asylum seekers often avoid engaging in anything that can be seen as contesting authority or that could ultimately hurt their chances of being granted asylum" (Kaurin, 2019: 15).

En ocasiones, la entrega termina sucediendo en condiciones de fatiga en que la persona se encuentra cansada de que se le requiera la misma información una y otra vez, por lo que ella misma se "automatiza" con resignación en el proceso, pese

a conservar sospechas o dudas sobre la posibilidad de que esa información luego pueda ser injustamente empleada en su contra:

> Migrants [referring also to refugees] exhibited a sense of resignation of giving up data when it was requested in order to access services and get into a system that can provide support. One said organization explained how migrants develop "fatigue" from being asked from their information repeatedly by so many different actors and entities (Latonero *et al.*, 2019: 31).

Esta fatiga puede además ser consecuencia de otros procesos de solicitud de datos personales y biométricos anteriores y que suceden justo cuando las personas refugiadas arriban a la frontera del primer Estado anfitrión.

En Europa, bajo la Regulación de Dublín,[26] las autoridades migratorias reciben a la persona en frontera y, entre las primeras acciones de atención que despliegan se encuentra la de enrolamiento en la base de datos EURODAC[27] en la que están facultadas a forzar la captura de datos biométricos para, en adelante, autenticar a la persona para deportar cuando haga falta en caso de que decida trasladarse a otro Estado distinto al primero al que arribó y en el que tiene la obligación legal de quedarse para solicitar asilo.

Para evitar dicho registro, se ha tenido noticia de personas refugiadas que han decidido quemar sus huellas dactilares y otras que, al haber entregado sus datos biométricos, generan una sensación de frustración y cansancio aumentada por la incertidumbre sobre la posibilidad de solicitar su borrado o eliminación (Reidy, 2017). En sus relatos se percibe un deseo por la invisibilidad y el anonimato que también puede impactar los procesos de entrega de datos biométricos frente a los actores humanitarios (Dembour y Kelly, 2011).

---

26 Desde 2013 se encuentra vigente en Europa la regulación conocida como Dublín III. Es una normativa expedida por la Unión Europea que establece los mecanismos y criterios para la determinación, en cabeza de un Estado Parte de la Unión, de la aplicación y solicitud de protección internacional de personas en búsqueda de soluciones de asilo, entre otras. Dicha regulación habilita a los Estados receptores de los flujos de personas en búsqueda de refugio a la recolección de sus datos biométricos (huellas dactilares) y a compartir dicha información con terceros Estados que lo requieran para la examinar la aplicación a la protección internacional y para determinar las obligaciones y responsabilidad del Estado en que se encuentra transitoriamente la persona (Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 Establishing the Criteria and Mechanisms for Determining the Member State Responsible for Examining an Application for International Protection Lodged in One of the Member States by a Third-Country National or a Stateless Person, 2013).

27 EURODAC es el sistema centralizado de información de la Unión Europea establecido en 2013 como producto de la Regulación de Dublin, en el que se recopilan y reposan los datos personales recogidos de las personas solicitudes de asilo y otras medidas internacionales de protección. Sobre la recolección de datos biométricos (huellas digitales) prevé, en su artículo 9 que "[l]os Estados miembros tomarán sin demora las impresiones dactilares de todos los dedos del solicitante de protección internacional mayor de catorce años y las transmitirán cuanto antes, y a más tardar a las setenta y dos horas siguientes la presentación de una solicitud de protección internacional definida en el artículo 20, apartado 2, del Reglamento (UE) no 604/2013, al Sistema Central", este registro aplica para las personas solicitantes así como de los nacionales de terceros países y apátridas interceptados con ocasión del cruce irregular de una frontera exterior (artículo 14) (Relativo a La Creación Del Sistema «Eurodac» Para La Comparación de Las Impresiones Dactilares Para La Aplicación Efectiva Del Reglamento (UE) No 604/2013, Por El Que Se Establecen Los Criterios y Mecanismos de Determinación Del Estado Miembro Responsable Del Examen de Una Solicitud de Protección Internacional Presentada En Uno de Los Estados Miembros Por Un Nacional de Un Tercer País o Un Apátrida, y a Las Solicitudes de Comparación Con Los Datos de Eurodac Presentadas Por Los Servicios de Seguridad de Los Estados Miembros y Europol a Efectos de Aplicación de La Ley, y Por El Que Se Modifica El Reglamento (UE) No 1077/2011, Por El Que Se Crea Una Agencia Europea Para La Gestión Operativa de Sistemas Informáticos de Gran Magnitud En El Espacio de Libertad, Seguridad y Justicia (Refundición, 2013).

Autores como Latonero y Kaurin analizan conjuntamente los procesos de enrolamiento biométrico efectuado por las autoridades migratorias de los Estados (por ej. Italia y Grecia), junto a los procesos de identificación que tienen lugar con actores humanitarios como ACNUR. Dichos procesos no pueden entenderse de manera separada por el impacto que tienen sobre las salidas de protección para la persona refugiada, y por supuesto, el que tienen para su privacidad cuando entre las dos ocurren eventos de entrega o solicitud de dicha información.

La libertad del consentimiento además de ser producto de un contexto anímico (afectado por la automatización de la persona, el cansancio), es también una manifestación de la voluntad que debe poder ocurrir en contextos libres de presión o violencia. Manifestación que se extiende en el proceso de aceptación como de rechazo o cancelación al tratamiento de los datos personales.

Diversos autores con frecuencia cuestionaron la libertad del consentimiento que queda en entredicho si para la persona refugiada (i) no aceptar al tratamiento de sus datos constituye una causal de rechazo para la entrega de asistencia o de despliegue de acciones de protección en su favor, y (ii) no le son ofrecidas alternativas distintas a la entrega de sus datos personales o biométricos.

Actores como ACNUR y el Programa Mundial de Alimentos, dos de las agencias de la ONU con mayor despliegue en la atención de las personas refugiadas, llevan a cabo la recolección de datos personales y sensibles –incluyendo los biométricos– con fines de identificación para, entre otros, llevar a cabo la asignación de ayuda a las personas que lo necesitan evitando en dicho proceso casos de fraude o suplantación. Son las organizaciones que han efectuado el mayor despliegue de biometría en el ámbito de la acción humanitaria (Madianou, 2019).

Sobre la condición de la asignación de ayuda humanitaria a la previa entrega de datos biométricos, en su guía de registro y manejo de la identidad ACNUR afirma que la negativa a consentir en la entrega de datos personales y biométricos por parte de personas refugiadas no será causal de exclusión de sus programas. La negativa, dice, es un derecho del titular del dato:

> Individuals have the right to refuse the collection of their *biometrics* on legitimate grounds related to his or her specific personal situation. This does not alter their right to international protection and the individual remains of concern to UNHCR. In such cases, individuals may be registered, and alternative methods identified to ensure they can access rights, assistance and solutions (UNHCR, 2018a). (Énfasis original).

Sin embargo, en un pie de página a dicha cita, aclara que el derecho a objetar o negarse al tratamiento de sus datos dependerá, además, de si el liderazgo del proceso de registro biométrico es llevado a cabo por el Estado hospedador, por lo que serán sus términos y condiciones los que rijan y no los de ACNUR.

Pese a que en la cita de más arriba, se menciona la posibilidad de alternativas ante la negativa de la persona, la guía no provee mayor información al respecto ni ahonda en las diferencias que estas alternativas puedan significar para la recepción de asistencia o ayuda.

Una situación parecida sucede con el Programa Mundial de Alimentos. Los datos biométricos obran a manera de moneda de pago en los sistemas de distribución de alimentos o transferencias monetarias a personas refugiadas. El sistema no permite a la persona el retiro de asistencia de los supermercados o cajeros sin la previa verificación de su identidad a través de la lectura de sus datos biométricos. Madianou explica cómo sucede dicho proceso de pago con los datos personales en la experiencia de un refugiado sirio:

> Bassam receives aid through a blockchain application combined with biometric technology that constitutes the WFP's *Building Blocks* scheme. Before visiting the supermarket, Bassam receives an SMS message informing him that his aid entitlement is ready to be collected. *At the registered grocery store, by scanning his iris, Basam verifies his identity on a United Nations High Commissioner for Refugees (UNHCR) database, which releases an electronic payment from WFP to the merchant* (2019: 2-3). (Subrayado propio).

Es decir, para recibir ayuda en especie se precisa la previa entrega de los datos personales y biométricos de la persona para verificar que es quien dice ser, lo cual automáticamente libera el pago que desembolsa el Programa Mundial de Alimentos directamente al supermercado En su escrito, Madianou entrevistó a 35 personas, entre refugiados, miembros del sector humanitario, desarrolladores de software, donantes y voluntarios. Ninguna dio cuenta de la existencia de alternativas menos invasivas para facilitar la recepción de ayudas en dinero o en especie (2019).

Dicha situación que la autora llama como "el ensamblaje biométrico", revela cómo la infraestructura para proporcionar la ayuda humanitaria en especie o dinero depende en exclusivo del funcionamiento de una tecnología digital que justifica la inexistencia de alternativas analógicas por ser, comparativamente, menos eficiente o más susceptibles al fraude y el engaño (Madianou, 2019). Alternativas que, en todo caso, no solo pueden beneficiar a quienes deciden ejercer su derecho a la negativa sino a quienes no logran "ser leídos" por los escáneres biométricos.

A veces la entrega de datos biométricos como condición para la recepción de ayudas en beneficio de las personas refugiadas, es menos sutil, si se quiere. En el caso comentado por Human Rights Watch sobre el despliegue de ACNUR para atender a la comunidad Rohingya, se entrevistó a 24 personas refugiadas sobre lo sucedido, 23 de ellas confirmaron que, para acceder a la ayuda monetaria, miembros de ACNUR les habían dicho que *debían* registrarse:

> All but one of the 24 said that UNHCR staff told them that *they had to register to get the Smart Cards to access aid*, and they did not mention anything about sharing data with Myanmar, or linking it to repatriation eligibility assessments (2021). (Subrayado propio).

Si para obtener un bien necesario es precisa la entrega previa de información biométrica, quiere decir que el consentimiento no solo no es libre, sino que existe una obligación no reconocida como tal por actores del sector humanitario en donde la alternativa ofrecida "lo toma o lo deja" no cuenta como tal. Según la organización de derechos humanos, en los casos en que se consultó a las personas sobre si querían o no que sus datos fueran compartidos con terceros, una dijo que había sentido presión a no negarse, por lo que no expresó su negativa aun cuando sostenía preocupación al respecto:

> The one Rohingya man who said UNHCR did ask his consent to share his data with Myanmar said he felt pressure not to refuse. He added that he assumed, based on UNHCR's mandate to protect vulnerable people, the data would only be shared at a time when safe and dignified repatriations were possible. "We would be very worried to have our full information shared without those conditions, especially now with the Myanmar military in control of the government," he said (Human Rights Watch, 2021).

Comentarios de la literatura revisada al respecto se pueden leer como sigue:

> Refusing to register with a humanitarian agency is to refuse aid -something displaced people can hardly afford. Only those registered can be on distribution lists. The lack of alternatives for displaced people (as work and other opportunities are typically closed to them) can turn consent into coercion (Madianou, 2019: 20).
> Refugees who refuse to give biometric data to the UNHCR are unable to receive assistance from the agency, thereby making the option of providing data a false one (Kaurin, 2019: 13).
> It should be a real choice of the data subject, who may freely revoke his/her consent at any point. However, when providing vital assistance to people in need, the concept of consent might be non-existent. Consent is not freely given–thus not valid–when a person's access to essential services depends on the processing of their data (Gazi, 2020: 4).

Sin embargo, los problemas en torno al consentimiento informado no son nuevos ni exclusivos de la acción humanitaria. Según Kristin Sandvik, Sean McDonald y Katja Jacobsen, dichos problemas han estado presentes en el ámbito de las pruebas médicas de experimentación y en otros en que el sufrimiento humano, aunado a los contextos de crisis y emergencia, da lugar a espacios aparentemente libres de ética, que facilitan el acceso a un conjunto de personas vulnerabilizadas con las cuales experimentar fuera del alcance de la regulación o en excepción de estándares conocidos (2017).

Problemas sobre el garante de que el consentimiento sea lo que debe ser. Los problemas en torno a la información provista a las personas refugiadas, se encuentran aunados a otros que no pertenecen a la esfera intrínseca del tratamiento de datos: los de capacidad de los agentes humanitarios.

En su investigación sobre migrantes y personas refugiadas que arriban a Italia y las preocupaciones en materia de privacidad y recolección de sus datos por parte de las autoridades migratorias y otros agentes humanitarios (incluyendo a ACNUR), Latonero y su equipo de investigación dan cuenta cómo, en algunos momentos, ni siquiera los actores humanitarios saben el qué, el para qué o el cómo de lo que están haciendo, en ese sentido:

> A number of organizations interviewed did not seem to understand how the database they were using worked, were unsure who could access it, did not have a fair knowledge of privacy and data protection, or were instructed to implement data protection law with little guidance (Latonero *et al.*, 2019: 37).

El consentimiento es, por tanto, un elemento central para reconocer los problemas que orbitan en torno a la atención humanitaria que se procura a las personas refugiadas en apoyo del uso de tecnologías biométricas y, en general, de las tecnologías digitales que son intensivas en la recolección de sus datos. La identificación de otros riesgos según la literatura revisada, sugiere, tal y como se verá a continuación que el problema, en todo caso, trasciende al del consentimiento y a la protección de datos en general.

Riesgos para el principio de finalidad y conservación limitada

Los problemas que enunciamos en la sección, anterior en términos generales, se relacionan con los principios de finalidad y difusión limitada cuando la información provista, y sobre la que se orienta el consentimiento, versa sobre los objetivos de la recolección y el tratamiento de los datos, los usos que efectivamente se darán a estos y los terceros que podrán acceder y por qué. En esta sección profundizamos, por lo tanto, en estos déficits de los que adolece la información que ya referimos más arriba.

Como vimos en el contexto general, la finalidad sobre el tratamiento debe ser determinada, precisa, cierta, limitada en el tiempo. La finalidad del tratamiento de los datos de las personas refugiadas debe poder satisfacer la misma expectativa, por lo que el objetivo que justifica el recabamiento de sus datos debiera ser expresado de manera lo suficientemente clara y accesible que no permita el lugar a la duda. La finalidad específica, legítima y clara, traza a su vez, el camino sobre los datos que deben ser recogidos para lograr el cometido propuesto, los usos que se dará a los mismos, y los terceros que podrán tener acceso para apoyar o permitir su realización.

Problemas de brecha sobre lo que dice la política de protección de datos y lo que sucede en la práctica. De conformidad con esa expectativa, por ejemplo, la política de protección de datos de ACNUR dedica un apartado específicamente a este punto. En la sección 2.3 de su política de protección de datos titulada "purpose specification" se afirma que el propósito debe ser específico y el procesamiento debe atender a este "[p]ersonal data needs to be collected for one or more specific and legitimate purpose(s) and should not be processed in a way incompatible with this/those purpose(s)" (UNHCR, 2015: 16).

En contraste, el punto 4.2 de la guía explicativa de la política de tratamiento de datos "[d]ata controllers need to determine and manifest the specific purpose(s) *before the collection of personal data* […] (UNHCR, 2018b:18). Y abunda al aclarar:

> With regard to the level of specificity, *the advice is to be as specific as reasonably possible*. For example, instead of referring to the protection of refugees, the precise activities need to be clearly stated, such as the issuance of asylum-seeker certificates, conducting needs assessments or monitoring the situation of asylum-seekers in detention (UNHCR, 2018b: 18). (Subrayado propio).
> [...]*Further processing needs to be compatible with the initial purpose(s). This logically follows from the Policy. New purposes require a new legitimate basis.* "Function creep", or a situation where the same systems and/or data sets are used for other purposes than the ones originally designated, would be incompatible with the purpose specification principle (UNHCR, 2018b: 19). (Subrayado propio).

Sin duda la guía, a diferencia de la política, da mayor claridad sobre los propósitos de la recolección de los datos. En el caso documentado por Human Rights Watch sobre la comunidad Rohingya, se advirtió que la finalidad de la recolección de sus datos fue todo, menos clara, es decir, que en la práctica ni siquiera la política de tratamiento, escueta y poco específica, fue aplicada (2021).

Según entrevistas efectuadas por dicha organización, las finalidades eran múltiples y no podían concurrir entre sí, o no podía en todo caso llevarse a cabo en un mismo proceso de tratamiento de datos puesto que involucra, además, a terceros con intereses opuestos (Human Rights Watch, 2021).

En su informe, dice que la recolección de datos para la elegibilidad con fines de repatriación voluntaria, así como la recolección de datos para la asignación de asistencia monetaria y en especie, crearon confusión en las personas que fueron entrevistadas pues formalmente consintieron entregando sus datos para postular a la repatriación voluntaria bajo la creencia de que, al hacerlo, estaban postulando a la asignación de dinero o comida (Human Rights Watch, 2021).

Pese a que las políticas de repatriación de ACNUR señalan que los procesos de captura de información con fines de repatriación nunca deben asociarse a otras actividades, como las de registro para identificar a las personas refugiadas, esto sucedió en la práctica en contra de sus propios lineamientos. Human Rights Watch advirtió sobre la existencia de información contradictoria, confusa y poco accesible que permitiera entender cuál era la finalidad de la recolección de los datos personales y sensibles y para qué estaban siendo compartidos con terceros, como las autoridades Myanmar:

> Human Rights Watch found that UNHCR gave refugees mixed messages about how their data would be used and did not provide enough information for people to understand when, how, and for what purposes their information would be shared with the Myanmar government (2021).

Problemas sobre la finalidad en tanto que debe aclarar si habrá, cómo y para qué eventos de compartición de la información con terceros. Sobre la compartición de datos con terceros, la información debe ser mucho más clara y precisa con los titulares de los datos en tanto que, los intereses de esos terceros pueden significar riesgos para la privacidad de la persona y en ocasiones, peligros reales para su propia vida e integridad física.

En el caso documentado al que hemos aludido más arriba, Human Rights Watch dio cuenta de cómo había personas a las que se les había sido informado que sus datos personales no serían compartidos con las autoridades del gobierno de Myanmar, del que huían, y que la información sería recolectada solo con fines de registro para su identificación. Se les dijo que, de ser compartidos sus datos y se les informaría al respecto, lo cual nunca sucedió:

> UNHCR did not tell us it would be used for anything linked to repatriations. When the registration exercise started, we had said we didn't want to participate because we were worried about repatriations, but the UNHCR staff told us, "We will not share your information with Myanmar until you give us permission to." And then they never came back to us to ask if they could share our information (2021).

La autorización de acceso o transferencias de datos debe poder suceder no solo según los términos de lo consentido por la persona titular del dato, sino que debe requerir de ese tercero como mínimo, el despliegue de una política y un compromiso de cuidado de los datos similar al del responsable inicial. Su acceso debe guardar una finalidad estrecha con la de este último, y todo esto debe ser claramente puesto en conocimiento de la persona antes de que esta consienta, o después, si los términos de lo consentido cambian.

Sin embargo, y volviendo al reciente caso de los Rohingya, conocer de entrada los términos de los acuerdos suscritos con las autoridades del gobierno de

Bangladesh y Myanmar es casi imposible, pues los términos y condiciones se encuentran contenidos en memorandos de entendimiento que están amparados bajo reservas de confidencialidad (Human Rights Watch, 2021).

ACNUR, por su parte, advierte en su política de tratamiento de datos (punto 6.1)[28] que, entre las condiciones generales para que las transferencias de datos a terceras partes sean posible, es preciso que (UNHCR, 2015):

► Esa tercera parte garantiza el mismo nivel de protección o al menos uno comparable al de dicha agencia.

► Que la transferencia suceda bajo una o más razones legítimas (consentimiento de la persona, por ejemplo).

► Que la transferencia suceda bajo uno o más propósitos legítimos.

► Que la transferencia sea adecuada, necesaria y no excesiva en relación con dicho propósito.

► Que se informe a la persona titular del dato.

► Que la tercera parte respete la confidencialidad de los datos transferidos.

► Que la tercera parte mantenga niveles altos de seguridad de los datos.

► Que ACNUR efectúe, antes de la transferencia, un análisis de impacto sobre el nivel de protección de datos garantizado por esta tercera parte, el marco legal que sería aplicable a dicho acuerdo, la implementación efectiva de medidas técnicas y organizacionales que garanticen la seguridad de la información, entre otros.

Se trata de requisitos que se alinean, una vez más, con lo esperado por los principios de protección de datos que fueron descritos en el contexto general. Sin embargo, en el caso concreto de los Rohingya, no solo no se efectuó un análisis de impacto, no se informó claramente a la persona sobre los propósitos de la transferencia, y no se aclaró qué datos serían transferidos y la finalidad de ese tercero una vez los tuviera en sus manos, sino que, al ser confrontada por lo sucedido, Human Rights Watch documentó que la agencia de la ONU negó que hubiera opacidad o falta de información al respecto:

> UNHCR said its protection staff in Bangladesh and Myanmar have monitored whether the sharing of refugee data has resulted in any harm to refugees or their families *and had not identified any harm thus far* (Human Rights Watch, 2021). (Subrayado propio)
> [...] A former senior UNHCR staff member said that while the agency has a policy in place, "UNHCR has not put procedures to enforce the policy. DPIAs are generally not

28 UNHCR may transfer personal data to third parties on condition that the third party affords a level of data protection the same or comparable to this Policy. Given the potential data protection risks involved in transfers to third parties, UNHCR needs to pay particular attention to the following basic principles of this Policy: (i) Transfer is based on one or more legitimate bases; (ii) Transfer is for one or more specific and legitimate purpose(s); (iii) The personal data to be transferred is adequate, relevant, necessary and not excessive in relation to the purpose(s) for which it is being transferred; (iv) The data subject has been informed, either at the time of collection in accordance with Part 3.1, or subsequently, about the transfer of his/her personal data, unless one or more of the restrictions in Part 3.7 ap(v) The third party respects the confidentiality of personal data transferred to them by UNHCR. Whether or not a data transfer agreement has been signed between UNHCR and the third party, UNHCR must seek written agreement from the third party that the personal data will be kept confidential at all times. In order to ensure and respect confidentiality, personal data must be filed and stored in a way that is accessible only to authorized personnel and transferred only through the use of protected means of communication; (vi) The third party maintains a high level of data security that protects personal data against the risk of accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to it (UNHCR, 2015: 35-36).

> conducted." He added that while the policy document seeks "adequacy" with Europe's General Data Protection Regulation, *in practice staff deviate from the requisite standards including informed consent* (Human Rights Watch, 2021). (Subrayado original)

Esta es una situación que la literatura reconoce como problemática. Al respecto, Dragana Kaurin (2019) señala que "the bigger problem for refugees is when the UNHCR shares data with host countries, who in turn share it with their countries of origin, as was the case with Rohinya refugees in Bangladesh" (2019: 13). Raymond, Al Achkar y Bens resaltan cómo esto puede conducir a la abstención en el ejercicio de derechos en el espacio humanitario, lo que podría afectar, a la final, la realización del mandato de dichas agencias:

> Fear of data misuse can prevent individuals from exercising their fundamental rights or increase the risks that such rights be denied. Over time, inappropriate uses of data can have ripple effects, with concerns over security, confidentiality and privacy, among others, expanding resistance to data sharing and undermining humanitarian work in the long run (2016: 4).

Las prácticas, que contrastan con la existencia de una política y una guía orientadora sobre los actos de compartición de datos de ACNUR ya habían sido puesta de presente en un informe de auditoría de 2017. Allí, se analizó el despliegue de BIMS, el sistema de biometría y verificación de la identidad de las personas refugiadas que ya estaba en funcionamiento desde 2010. Se analizaron de cerca los centros de operación de Tailandia, India, República Democrática del Congo, Chad y República del Congo. En cada uno de estos países, la agencia de la ONU compartió información personal y sensible de personas refugiadas sin las medidas de seguridad necesarias, ni los análisis de riesgo previos que dicta su propia política. Al respecto, el organismo auditor:

> Further, in the opinion of OIOS, the following particular instances of data sharing required UNHCR's attention under the requirements of the Policy:
> The Representation in DRC shared with the Representation in Central African Republic lists of refugee students from that country residing in DRC, *for later transmission to the government of the Central African Republic, which posed a potential protection risk to those students.*
> The Representations in India and Thailand periodically shared with the respective host governments lists of refugees containing some of their personal data *but without underlying assessments of the level of data protection applied by the respective governments and without data transfer agreements.*
> The Representation in Thailand had a data sharing agreement in place with an operational partner dating back to 2005 for the provision of personal data of refugees from Myanmar for the purpose of assistance. This agreement included principles of confidentiality, respect of privacy, and protection of personal data, *but the country operation had not conducted a specific assessment to confirm the level of data protection applied by the partner*. (Office of Internal Oversight Services, 2016:11). (Subrayado propio)

En el informe de auditoría el factor humano fue clave: los representantes de ACNUR en terreno no creían o no consideraban que la información compartida tuviera que ser protegida, o no tenían conocimiento de la política ya vigente en materia de protección de datos, o la consideraban muy abstracta y difícil de aplicar. El informe de auditoría concluyó, sobre la compartición de datos con terceros, que

"the recent implementation of BIMS increased the probability of requests of sharing of biometric data by host governments, there were risks related to inadequate data sharing arrangements, and the security and protection of persons of concern could also be compromised" (Office of Internal Oversight Services, 2016: 11).

Una década después de haber iniciado el despliegue de sistemas de biometría, ACNUR seguía sin contar con una política de privacidad que dejara clara la información sobre el tratamiento, mucho menos los términos de compartición de los datos. Al haber solicitado información al respecto para su investigación en 2016, Jacobsen transcribió la respuesta de la agencia de la ONU frente a los críticos de la privacidad "Biometrics will be used at the UNHCR's discretion. Whether or not UNHCR exchanges data with partners is not relevant" (2016: 169).

Esta es una situación que se repite también con la otra agencia de la ONU dedicada a proveer asistencia en alimentación a personas refugiadas y que añade al listado de terceros interesados no solo a los Estados hospedadores y los de huida de las personas refugiadas, sino a grandes empresas tecnológicas de *Silicon Valley* cuyo modelo de negocio al tiempo que se ve beneficiado afirma nuevamente lo advertido en el primer capítulo, sobre la "marketización" de la acción humanitaria y el giro de valores que ello representa.

Así, para 2019, el Programa Mundial de Alimentos suscribió un acuerdo con Palantir, empresa tecnológica que, en el pasado, ha estado involucrada en contratos con la CIA, facilitando eventos de abuso a los derechos humanos (Privacy International, 2019). En dicho acuerdo, cuyos términos son confidenciales, se espera que la recolección intensiva de datos permite hacer mucho más efectiva la entrega de alimentos a más de 90 millones de personas en los 80 países en que dicha agencia tiene presencia. En el comunicado de prensa de dicho anuncio se lee:

> Our work with Palantir will save time and money so we can more effectively and efficiently feed 90 million people on any given day across the globe," said WFP Executive Director David Beasley. "When you work in the complex and volatile environments that we do, *you know that efficient access to data means your operation runs smoother, and together with Palantir, we're going to be even better at saving lives*. (World Food Program, 2019b). (Subrayado propio)
>
> […] In Iraq, for example, it helped reduce food basket costs by more than 10 percent by making small changes, such as swapping out one commodity for something similar or changing procurement sources without reducing nutritional values. *By making operations more efficient and effective, WFP can make the most of every dollar spent* (World Food Program, 2019b). (Subrayado propio)

De hecho, en la presentación de dicha iniciativa, el Programa Mundial de Alimentos llegó a compararse con Uber y Netflix sugiriendo que la acción humanitaria debería poder pensar no en la persona beneficiaria sino en el "cliente", tal y como dichas compañías lo hacen (Parker, 2019).

Frente a dicho comunicado, Privacy Internacional criticó la puerta abierta que esto significa para la explotación de la información de las personas más vulnerables (2019). No solo sus datos personales y biométricos, sino sus metadatos podrían ser accedidos por dicha corporación. Los metadatos[29] tienen la potencia-

29 "Si bien los metadatos pueden aportar beneficios, algunos tipos de metadatos, tomados en conjunto,

lidad de hablar sobre los intereses y hábitos de las personas, su movilidad personal, sus redes de comunicación y de contactos, por lo que incluso han recibido el estatus y protección de los datos sensibles (UN Human Rights Council, 2017a).

Se trata de una preocupación que tiene sentido, si se considera la cantidad de información que el Programa tiene en sus manos. No más en el caso de Líbano, las transferencias monetarias que efectúa a las personas beneficiarias a través de tarjetas de asistencia para que estas compren la comida que necesiten, rastrean todos y cada uno de sus movimientos: cuánto retiran, dónde lo hacen, cuántas veces al día o por semana, entre otros. Solo en ese caso, ha podido recoger hasta 6 millones de registros de este tipo en un período corto de 18 meses, comprendido entre el año 2014 y 2015 (Flaeming *et al.*, 2017).

En respuesta a dicha crítica, el Programa Mundial de Alimentos dijo que, para evitar situaciones de ese estilo, la agencia contaba con una política de tratamiento de datos clara que ayudaría a evitar la concreción de algún riesgo. Afirmó que no habría compartición de datos con Palantir, y que su rol solo estaba destinado a mejorar la eficiencia operacional de la organización (World Food Program, 2019a).

Sin embargo, en una investigación de campo realizada por Madianou en 2019, dos de los participantes en sus entrevistas involucrados en acuerdos público-privados suscritos con el Programa Mundial de Alimentos y otras organizaciones privadas, reconocieron que en alianzas de ese tipo los cruces y transferencias de datos sí tienen lugar, solo que la opacidad de los acuerdos suscritos impiden obtener mayor información al respecto (2019).

Por su parte, Kaurin (2019) advierte que esta práctica del Programa Mundial de Alimentos se remonta más atrás, a 2017. Una auditoría de entonces sobre las prácticas de compartición de la información de dicha agencia con gobiernos y corporaciones privadas, dio cuenta cómo tenía lugar el intercambio de información sin que esta exigiera a terceros ni tomara por su cuenta medidas adecuadas de protección de los datos, o de seguridad de la información de las personas beneficiarias de sus programas, incluyendo por supuesto, los datos de personas refugiadas.

La auditoría de 2017, efectuada sobre el despliegue del sistema de manejo de la identidad del Programa Mundial de Alimentos, SCOPE (que ya funcionaba en 61 de 85 centros de operación y que contaba con los registros personales de más de 24 millones de personas), determinó que, pese a que el Programa contaba con políticas en privacidad y protección de datos bien definidas, estas no eran aplicadas en torno al despliegue de su sistema ambicioso pese a que, en 2011, dicha agencia de la ONU había efectuado un compromiso por fortalecer sus prácticas de rendición de cuentas con las comunidades a las que sus operaciones impactan, incluyendo aquellas relacionadas con su privacidad y protección de datos (Office of the Inspector General, 2017).

Para el sistema SCOPE estaban además siendo recogidos datos innecesarios, sin que fuera advertido un propósito claro o legítimo, como de religión de las personas, un dato sensible, sin justificación para ello:

---

pueden revelar información personal que puede no ser menos delicada que el propio contenido de las comunicaciones y pueden dar indicación del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona" traducción propia (UN Human Rights Council, 2017b:3).

> The agency did not clarify the details, and the report does not say where it happened, but the audit team only visited Malawi, Sudan, and Myanmar. Of the three, only Myanmar has any significant diversity of religious adherence, and religion is a key factor in its recent violence (Parker, 2018).

Dicho informe describe cómo no solo no estaban siendo llevados a cabo los análisis de impacto normativo que habían sido adoptados en la política de protección de datos, y que estaban destinados a analizar los riesgos de la recolección de datos, su almacenamiento y acuerdos con terceros para su compartición.

Además, se estaban conservando datos más allá del tiempo y finalidades prometidas "former beneficiaries are kept in the system to ensure that WFP can respond faster when these beneficiaries are again in need." (Parker, 2018); no se estaba contando con el consentimiento de las personas, y el acceso y transferencia de su información a terceras partes (gobiernos, otras agencias de la ONU y corporaciones privadas) estaba teniendo lugar sin medidas de seguridad mínimas: contraseñas, protocolos de cifrado, etc. (Office of the Inspector General, 2017).

Más recientemente, un informe de auditoría de 2020 proveyó un panorama similar. Allí se reconoció nuevamente que, pese a que SCOPE es la "joya de la corona" de las operaciones de la agencia de alimentos de la ONU, todavía había fallos en materia de privacidad y protección de los datos personales que se recogen para llevar a cabo los procesos de identificación y verificación de las personas beneficiarias de sus programas. Fallos que, para entonces, todavía no habían sido corregidos.

Entre los escenarios de mayor riesgo que identificó el informe de auditoría, se advirtió entre otros el crecimiento exponencial de los acuerdos con terceros sin la implementación de medidas de análisis sobre las prácticas de compartición de la información con estos:

> WFP had not implemented a third-party vendor privacy and security management programme or applied a consistent approach to contracting, assessing and overseeing the data protection, privacy and information security practices of its partners and vendors. Weaknesses highlighted during the audit included: *a lack of third-party risk management governance processes; third-party IT security policies; the absence of a comprehensive inventory of third parties; and the need for a data privacy framework to address privacy risks and identify key areas of control focus.* (Office of the Inspector General, 2020: 4). (Subrayado propio).

Por su parte, autoras entusiastas como Lodinová (2016), Gelb y Krishnan (2018), al tiempo que afirman los beneficios de la biometría y en general, el despliegue de las tecnologías digitales en el espacio humanitario, y que dicen impactar positivamente en la reducción del tiempo de registro de las personas refugiadas, aumentando la seguridad del proceso y la prevención de eventos de fraude; reconocen que las preocupaciones sobre las prácticas de protección de datos y compartición de los mismos necesitan mayor escrutinio, especialmente cuando se trata de actores de alcance global como las agencias de la ONU para los refugiados y los alimentos.

Todas estas preocupaciones mantienen vigencia. Nada más el 10 de noviembre de 2020 la Relatoría de las Naciones Unidas sobre las formas

contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia expresó su preocupación por la falta de claridad de las políticas de compartición de datos de las agencias de la ONU que desdicen del principio de finalidad en su tratamiento. En dicho informe cuestionó además el respeto al principio de consentimiento ante la incertidumbre sobre si las personas refugiadas que habrían de ser registradas en el sistema biométrico del Programa Mundial de Alimentos, contarían o no en la práctica con el derecho de no consentir y cancelar sus datos del sistema (2020).

Afirmó que el tratamiento de datos no es un proceso apolítico "especially when powerful Global North actors collect information on vulnerable populations with no regulated methods of oversights and accountability" (Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, 2020, prr. 10). Preocupaciones que se magnifican cuando se considera, según la Relatora, E. Tendayi Achiume, el escenario desregulado "on which data are extracted from individuals and nations in the global South, by profit-seeking corporate actors in the global North who cannot be held accountable" (2020b).

Riesgos para el principio de seguridad y confidencialidad

Ligado a las políticas de compartición o acceso a los datos personales se encuentran las de seguridad y confidencialidad de la información. Según mencionamos en la sección de contexto general, se trata de medidas exigibles tanto al responsable de los datos como a los terceros con los que este suscribe acuerdos de acceso a estos.

Entre los riesgos en términos de seguridad de la información advertidos por la literatura, se encuentran la ausencia de medidas de seguridad o medidas deficientes, el acceso accidental por terceros a la información y la ausencia de notificación a la persona afectada de los eventos de brecha de seguridad (Jacobsen, 2016; Kaurin, 2019; Latonero *et al.*, 2019; Madianou, 2019; Rahman *et al.*, 2018; Raymond *et al.*, 2016; Willits *et al.*, 2019).

Una misma brecha en materia de seguridad que fue advertida por Rahman, Verhaert, Nyst (2018) y Madianou (2019), fue la del proyecto de conectividad de un campo de refugiados sirios en Grecia. La red de internet, desplegada sin medidas de seguridad, estuvo expuesta a más de 80.000 eventos de malware cada semana durante el año 2015. Eventos de ese tipo fueron reportados por Latonero y su equipo de investigación en Italia y Grecia, a los que se sumaron la ausencia de protocolos de cifrado de las comunicaciones, ya sea en relación con páginas web (protocolo HTTPS) o en otros mecanismos de comunicación (2019).

Rahman cuenta cómo las brechas de seguridad pueden ser producto del fallo no solo de la tecnología, sino del propio descuido humano. Así, cuenta un caso anecdótico sobre la pérdida de computadores o dispositivos de almacenamiento portátil como las USB de diversos actores humanitarios y que contenían información sensible de las personas beneficiarias de sus programas (2018). En la auditoría a ACNUR de 2016, se dio cuenta de cómo algunos de los equipos de registro biométrico de personas refugiadas en Tailandia, eran dejados sin vigilancia ni seguridad, lo que exponía la información a su manipulación y pérdida, y a los equipos a eventos de robo (Office of Internal Oversight Services, 2016).

La ausencia de capacidades humanas en materia seguridad es tal, que los eventos de acceso por terceros a los sistemas de información ni siquiera es previsto como uno posible en la mente de algunos integrantes de agencias humanitarias dedicadas a proveer ayuda a personas refugiadas: "[w]hen asked "Do you worry about other people getting Access to your interview notes [with migrants and refugees]?" one NGO worker responded, "Good question". I've never thought about it" (Latonero *et al.*, 2019: 37).

Dragana Kaurin (2019) también cuenta cómo, en septiembre de 2018, los propios agentes de OCHA publicaron accidentalmente documentos sensibles de la organización tales como contraseñas, acceso a links de conferencias cerradas o de acceso restringido, y otro material asociado a sus operaciones, a través de una aplicación de administración de proyectos. Así, el factor humano en materia de seguridad está influido no solo por la malicia de terceros, sino por el descuido y la impericia propia.

Mirca Madianou (2019) relata en su artículo de investigación que, en diciembre de 2017, se tuvo noticia del *hackeo* de los sistemas de información de 11 agencias humanitarias, algunas de ellas dedicadas a la atención de personas refugiadas.

Adicionalmente, en noviembre de ese mismo año se conoció que la empresa de tecnologías *Mautinoa Technologies* había descubierto serias fallas de seguridad de los sistemas de un proveedor de software de al menos 9 agencias humanitarias, entre las que se encontraba Oxfam, la Organización Internacional para las Migraciones, el Consejo Noruego para los Refugiados, UNICEF, el Comité Internacional de la Cruz Roja, entre otros. El fallo permitía acceder a los sistemas, los nombres de las personas beneficiarias de cada agencia, sus fotografías, detalles familiares, coordenadas geográficas, entre otros datos, permitiendo al intruso la capacidad de editarlos, descárgalos y subir información nueva (Parker, 2017).

En su nota periodística, B. Parker recogió el testimonio de un integrante de una de las organizaciones de ayuda humanitaria afectada, que puso de presente el rol que tienen las personas de una organización y la brecha de capacidad de las mismas en materia de seguridad de la información que recogen y manejan. En su nota se da cuenta de percepción de la persona entrevistada que cree que son las compañías propietarias de las soluciones tecnológica las únicas encargadas de proteger dicha información:

> We don't understand the full implications of the data we hold and share, the same way we didn't when we were doing in-kind distributions via Excel," an NGO manager said. "I think we are too trusting of companies that say they have data protection under control." (2017).

Es más, esa confusión en los roles sobre quién tiene a su cargo el cuidado de la protección de la información, fue documentada recientemente en el informe de auditoría del Programa Mundial de Alimentos de 2020. El procedimiento de auditoría determinó que los procedimientos de control a las transferencias de datos a terceras partes podían ser fácilmente burlados, sin embargo, aclara el texto, la auditoría no pudo ser completada por falta de claridad sobre a quién pertenecen las plataformas y sistemas analizados, quién tiene responsabilidad sobre estos, entre otros (Office of the Inspector General, 2020).

Por otro lado, las brechas de seguridad no solo tienen el potencial de impactar la privacidad de las personas titulares de la información, también, de impactar en el aspecto reputacional de las organizaciones mismas. Al respecto, Rahman y otras investigadoras refirieron, para el caso de Oxfam, lo siguiente:

> A data breach of one of the Oxfam confederation members could affect local partners and beneficiaries trust in Oxfam at large, ultimately jeopardizing Oxfam's ability to meet its mission, *not to mention international trust and perception of the way in which Oxfam do their work* (Rahman et al., 2018:13). (Subrayado propio).

Eventos en seguridad de la información han sido reportados frecuentemente, dando cuenta no solo de la debilidad técnica y organizacional de una extensa cadena de actores (organizaciones de ayuda humanitaria y sus agentes y representantes, proveedores de tecnología, entre otros), sino especialmente, de la ausencia de reacción por parte de entes reguladores en materia de protección de datos que, a la fecha, no han emitido pronunciamiento o comunicado sobre la eventual apertura de investigaciones en la materia.

En julio de 2019, por ejemplo, fue noticia el ciberataque sufrido por la Organización de las Naciones Unidas. En septiembre de ese año, un reporte filtrado al medio *The New Humanitarian* relaciona cómo dicho evento afectó al menos 42 sistemas de información de la ONU y a otros 25 que estaban bajo sospecha de haber sido *hackeados.* Dicho evento, por decisión de la Organización, no fue informado a las personas afectadas pues "[u]nder diplomatic immunity, the UN is not obliged to divulge what was obtained by the hackers or notify those affected" (Parker, 2020b). Ninguna agencia de protección de datos en el mundo reaccionó al respecto.

Otro evento de brecha de seguridad de los sistemas de información del personal de la ONU fue reportado poco después, en enero de 2020 (Montalbano, 2020). En ese mismo año, otro servidor de un proveedor privado de sistemas de información para organizaciones como Human Rights Watch, Save the Children y World Vision, sufrió un ataque de secuestro de la información sobre sus donantes. La reacción que documentaron medios como The New Humanitarian relacionó nada más la del proveedor tecnológico y algunas entidades afectadas (Parker, 2020a).

Se trata de eventos que afirman la importancia del despliegue de las medidas técnicas y de seguridad en los sistemas de información de los que hacen uso agencias del sector humanitario en general, y especialmente las que se dedican a la atención de personas refugiadas pues "data breaches increases the vulnerability of displaced people and the risks of their data being used for discriminatory, involuntary repatriation, resettlement or further persecution" (Madianou, 2019,: 17). Pero dan cuenta, al tiempo, de un factor ausente en la ecuación: la activación de mecanismos de investigación y sanción que no dependan de las entidades involucradas.

Las auditorías de seguridad digital que apuntan al análisis e identificación de los posibles riesgos juegan un papel indispensable, pues permite detectar las vulnerabilidades que pueden llegar a ser explotadas por terceros o que pueden

suceder por la imprudencia humana. Medidas que, en todo caso, debieran ser más intensas cuanto más sensible sea la información almacenada.

En materia de seguridad, sin embargo, la provisión de la información sobre las afectaciones en torno a los datos personales expuestos de las personas beneficiarias, es tanto o más importante que las medidas técnicas de contingencia desplegadas una vez una brecha se reporta, pues impactan en la confianza relacional, clave tanto para la agencia de ayuda humanitaria como para las personas que se benefician de su misión. Notificar a la persona afectada no debería ser solo una opción.

Sin embargo, pese a que esto último es considerado una buena práctica reconocida por la política de privacidad de entidades como ACNUR, su redacción no provee suficientes garantías de que las personas afectadas serán avisadas en la realidad pues, tal y como lo hace notar Kaurin, la política afirma que la decisión de informar dependerá del controlador de los datos quien podrá hacerlo bajo la consideración de que la brecha, a su parecer, genere o no una afectación o daño físico al titular del dato (2019).

Otro aspecto relevante en los riesgos de seguridad de la información tiene que ver con los mecanismos internos de autorregulación y transparencia, así como la creación de autoridades internas encargadas de su cumplimiento que puedan obrar de manera autónoma. Al respecto, el informe de Simon Davies sobre ACNUR provee un ejemplo diciente.

Simon Davies, experto en privacidad y comisionado por ACNUR para realizar un análisis de impacto sobre el despliegue en 2008 de sistemas de biometría para la identificación de personas refugiadas en Kenia, Etiopía, Malasia y Djibouti; publicó en 2012 en el blog "Privacy Surgeon" los hallazgos del mismo, puesto que había sido enterrado en el olvido por la propia agencia de la ONU pese a los hallazgos y advertencias que hacía (2012).

La publicación, efectuada en violación del acuerdo de confidencialidad entre dichas partes, señala cómo no solo se había forzado a las personas refugiadas a su uso, cómo no era claro entonces el propósito de despliegue y uso de dicha tecnología digital, y expuso la ausencia de medidas de seguridad y protección de la información, incluso de las más básicas, que la exponían a usos indebidos, filtraciones, acceso no autorizados, pérdida y robo pese a la advertencia de que se trataba de eventos posibles (Davies, 2012).

Davies señala cómo dicho reporte, luego de haber adquirido forma en ocho versiones distintas, fue sepultado por cuatro años no viendo la luz ni siquiera en versiones resumidas. Una situación que el experto describe como inaceptable en caso de haber sucedido en países con regímenes de protección de datos capaces de echar mano a agencias cobijadas por regímenes de inmunidad (Davies, 2012).

Entonces, los problemas en materia de seguridad y confidencialidad de la información pueden, según hemos visto, agruparse por categorías. La primera de ellas, que reúne los problemas asociados al desconocimiento de buenas prácticas o inaplicación de protocolos existentes en materia de seguridad de los datos, y que reúne eventos como los de exposición de la seguridad de las

redes de conexión wifi, de *hackeo* y de protección de los equipos y dispositivos móviles que resguardan información. Aquí también se agrupan los problemas de capacitación y sensibilización, que se relaciona con el desconocimiento sobre la importancia de las medidas de seguridad para resguardar información de terceros. Y la segunda, que refiere a los problemas de opacidad y ausencia de mecanismos de rendición de cuentas, que se relaciona con la ausencia de notificación a las personas afectadas por eventos que impactan en la seguridad de la información. También, se suma aquí la ausencia de mecanismos de transparencia que den cuenta sobre el tipo de afectación, su alcance y medidas de mitigación desplegadas, así como la ocultación de informes que visibilizan las debilidades de las estrategias de seguridad de la información de los grandes actores humanitarios.

Riesgos sobre el principio de exactitud de los datos

Fueron advertidos por autores como Latonero (2019), Madianou (2019) y Kaurin (2019) los riesgos de inconsistencias e inexactitud en los datos de las personas refugiadas registradas en los sistemas de información de las agencias humanitarias que les proveen de beneficio y asistencia. Eventos que pueden impactar en la utilidad de la información, pero especialmente, en el acceso a la ayuda humanitaria.

Kaurin menciona, por ejemplo, cómo las transliteraciones a los sistemas de escritura del inglés, italiano, griego o español desde el árabe u otros idiomas que utilizan su alfabeto con adaptaciones como el darí y el kurdo, resultan de manera frecuente en errores de deletreo y escritura de los nombres de las personas refugiadas lo que dificulta su localización en las bases de datos. En ocasiones, se registra la nacionalidad equivocada o el lugar de nacimiento de la persona en el campo en que debe ir su nombre. Se trata de errores con consecuencias que impactan en la búsqueda de una solución a largo plazo para la persona, y en el plazo inmediato, en su posibilidad de acceso a ayudas en especie o transferencias monetarias (2019).

En eventos de registro erróneo de la información, Latonero y su equipo de investigación detallan cómo esta información, cuando es accedida por autoridades del policía o migratorias, puede llevar a eventos en los que, por ejemplo, se sustraiga a menores de edad de su familia porque son datos tomados como un indicador de que el menor no pertenece a la que dice ser su familia biológica (2019). La tecnología contribuye en estos casos y a través de errores humanos, a ahondar los cuestionamientos a la credibilidad de los refugiados.

Madianou se enfoca, por su parte, en las inconsistencias en la información producto de la tecnología en donde personas de tez oscura son erróneamente "leídas" por el sistema que indica que estas no son quienes dicen ser, siendo que sí lo son. No se trata propiamente de un "problema en el dato", es decir, la fotografía del rostro de la persona –o el rostro de la persona, si se quiere–, sino uno en su procesamiento por el sistema de reconocimiento biométrico. Sin embargo, por un error tecnológico, la persona refugiada es la que debe asumir la carga de probar su propia identidad dado que la máquina no se equivoca.

Este es un problema que, en todo caso, ya ha sido advertido en la práctica por organizaciones como ACNUR y el Programa Mundial de Alimentos.

El informe de auditoría de ACNUR de 2016, advirtió como riesgo el registro incompleto e inexacto de la información en BIMS, el sistema de información biométrica de dicha organización (Office of Internal Oversight Services, 2016).

El informe de auditoría de 2017 de la agencia de alimentos de la ONU dio cuenta de la carga de información incompleta o inexacta en SCOPE, su sistema de biometría, lo que la hacía inutilizable. Es decir, lo que significaba, en la práctica, personas que no podían acceder a la transferencia monetaria que les permitiría comprar alimentos necesarios. También dio cuenta dicho informe que no solo se reportaron eventos de inexactitud en los datos, sino restricciones en los permisos de edición de la información errónea para actualizar los registros de las personas cuya información era incorrecta (Office of the Inspector General, 2017).

Riesgos sobre el derecho de acceso, rectificación, cancelación y oposición

Kaurin (2019) y Madianou (2019) identifican como riesgo la imposibilidad del ejercicio de los derechos comúnmente conocidos como ARCO por parte del titular cuando este es una persona refugiada. Aspectos asociados a miedos de accionar contra la agencia humanitaria, y que esta pueda tomar represalias en contra de aquella o suspender la ayuda proveída; desconocimiento sobre qué derechos y cómo se ejercen; la ausencia de información disponible sobre su ejercicio en el idioma de la persona, entre otros, son algunas de las razones que obstaculizan las facultades de acceso, rectificación, cancelación y oposición.

Kaurin, por su parte, señala la importancia de que las agencias de ayuda humanitaria cuenten con mecanismos de queja anónima ante esta, dado que puede contribuir a la puesta en conocimiento de la agencia, de hechos que en materia de protección de datos merezcan investigación (2019).

Jacobsen relata cómo las protestas colectivas de oposición a la recolección de datos biométricos han derivado en ciertos casos en actos de violencia, tal y como sucedió en 2006 en Malasia, uno de los primeros países donde se desplegó el sistema de enrolamiento biométrico de ACNUR pues las personas descubrieron que, luego de haber registrado sus huellas digitales, a algunas de ellas les habían llegado avisos de "regrese a su país de origen" (2016).

La importancia de ofrecer mecanismos de este tipo ya ha sido puesta de presente respecto a las agencias de la ONU que hemos revisado de cerca hasta ahora. Así, el informe de 2016 de auditoría al sistema de biometría de ACNUR, señaló en el punto F sobre protección de datos que la agencia debía poder informar a las personas refugiadas sobre sus derechos de acceso y cancelación y a formular quejas o reclamos ante esta. Pese a ello, entonces evidenció la ausencia de provisión de información al respecto (Office of Internal Oversight Services, 2016).

El informe de 2017 de auditoría al sistema de biometría del Programa Mundial de Alimentos al tiempo que resaltó el compromiso que este tiene de rendir cuentas a las personas beneficiarias de sus programas, puso de presente la debilidad de los mecanismos de queja debido al manifiesto conflicto de interés en donde la agencia actúa como parte interesada y única instancia de resolución de las mismas (Office of the Inspector General, 2017).

Señaló así mismo, la ausencia de mecanismos de anonimato para el envío de quejas por parte de los beneficiarios, la redundancia y duplicidad de los mecanismos existentes y la disposición de múltiples canales que "may provide more opportunities for beneficiaries to submit information, [although] there is a potential dilution of the effectiveness of the process and compromising of its integrity if the information is not integrated" (Office of the Inspector General, 2017: 19).

Sin embargo, Jacobsen señala que el problema sobre la ausencia de mecanismos para exigir a agencias como ACNUR, que informen debidamente a las personas que se benefician de sus programas, sobre el ejercicio de sus derechos en materia de protección de datos es un problema mucho más general que supera a los procesos de recolección de datos por dicha agencia, y que se relaciona con la manera en que este, en general, (no) rinde cuentas "hacia abajo".

Al respecto, la autora cita el estudio elaborado por la alianza *Humanitarian Accountability Partnership* sobre los mecanismos de rendición de cuentas de ACNUR en Daab, Kenia, donde se encontraba un complejo de campos para personas refugiadas, y que detectó la ausencia de vías para que las personas pudieran ejercer "the right to complain, without fear of harm or retaliation" (2016: 168).

Rahman, por su parte, en un artículo recientemente publicado titulado "Betrayal and denial from the UN on refugee data", sobre el caso de los Rohingya documentado por Human Rights Watch, dice que el problema sobre el ejercicio de los derechos ARCO va mucho más allá de los mecanismos disponibles para su ejercicio (2021).

La asimetría de poder entre las partes, es decir, el titular del dato y la agencia humanitaria que los recoge, es tal que ni siquiera es posible hablar, en principio, del consentimiento como base legítima para justificar el tratamiento. Luego, pese a que el responsable del tratamiento insista en que el consentimiento es la que habilita la recolección de información personal y sensible, una vez esta se encuentra en manos de un tercero con intereses que impactan negativamente en contra de los del titular, no hay manera de hablar sobre el derecho a la autodeterminación en el que se sostienen las facultades ARCO de la protección de datos.

Si el punto de partida del tratamiento, dice, es la ausencia de procedimientos claros, transparentes y legítimos para recabar el consentimiento de la persona, de ahí en adelante lo que sigue es una larga cadena de eventos que restringen el ejercicio libre de derechos en un escenario en el que la persona refugiada se encuentra obligada a ceder, porque el caso contrario deriva en la desprotección de esta última (2021).

Incluso, pese a que de manera colectiva exista un rechazo expreso como lo hubo en el caso de los Rohingya quienes en noviembre de 2018 protestaron exigiendo detener la recolección de los datos biométricos porque sabían que serían compartidos con el Estado del que huían (una suerte de derecho colectivo de oposición), nadie atendió sus llamados ni detuvo la recolección o compartición de su información. En las demandas de la protesta se leía lo siguiente:

> 4. *Stop the collecting of our biodata, and do not share biodata already collected with the Myanmar government.*

> [...] We are very worried about the bio-data that UNHCR wants to collect (finger prints, iris scans, property documents). We believe UNHCR can share this data for repatriation with Myanmar Government and the Myanmar Government can use it to label us as ARSA [30] or as 'Bengali foreigners' like in the past, or to make trouble for our families (John Quinley III, 2018). (Subrayado propio)

Rahman cuenta cómo se transforma en una suerte de derecho ilusorio el ejercicio de las facultades de cancelación de los datos o de oposición, por ejemplo, a que sean compartidos cuando quien los ejerce es la persona refugiada. Señala que, eventos como el de los Rohingya muestra que, una vez dichos datos han sido accedidos por terceras partes sin el consentimiento de la persona, se trata de información que ya pudo ser usada, copiada y distribuida a otros pese a que el titular ejerza su derecho a la cancelación de los mismos, con el agravante de que particularmente los biométricos no varían, permanecen siempre con la persona no importa a dónde vaya. Apunta que, además, no existen autoridades distintas a la agencia humanitaria que puedan obligar a ese tercero a cumplir con el derecho del titular de los datos (2021).

Riesgos para el principio de responsabilidad y rendición de cuentas

La ausencia de transparencia fue uno de los riesgos más comúnmente referidos en materia de responsabilidad y rendición de cuentas. Puede decirse que es un riesgo que impacta en diferentes niveles.

El primero de ellos es consecuencia directa de lo ya visto sobre la calidad y accesibilidad de la información entregada a los refugiados y que se materializa en la retención, opacidad, parcialidad o retención de la información que esta necesita para saber el qué, el para qué y cómo será llevado del tratamiento de sus datos, así como la información necesaria para ejercer sus derechos al acceso, la cancelación, la rectificación y la oposición (Kaurin, 2019; Latonero *et al.*, 2019; Madianou, 2019; Jacobsen, 2016; Rahman, 2018).

Así como el tipo y calidad de información proveída sobre posibles alternativas menos invasivas, sus consecuencias o impacto en el acceso a la ayuda humanitaria, etc. Por último, el tipo, calidad y apertura de la información sobre eventos de brechas en seguridad digital, sus causas, mecanismos de mitigación desplegados, auditorías efectuadas, sus resultados y acciones de seguimiento, entre otros. Un riesgo que, en definitiva, se relaciona al ciclo de vida del dato.

En un segundo nivel, es un riesgo que se asocia al principio de finalidad, y que se concreta en la ausencia de razones lo suficientemente claras y soportadas en la evidencia sobre por qué se requiere, para la asistencia humanitaria, el despliegue de tecnologías digitales y en concreto, tecnologías de captura de datos biométricos (Jacobsen, 2016; Madianou, 2019). Asunto que abordaremos con algo más de detalle en el capítulo tercero.

En un tercer nivel, se encuentran los riesgos de transparencia en el relacionamiento del responsable y el encargado del tratamiento a nivel interno, es decir,

30 ARSA por las siglas en inglés de *Arakan Rohingya Salvation Army*. Según Faisal Edroos en un reportaje para *Al Jazeera*, el gobierno de Myanmar suele acudir a la existencia del ARSA como una razón para perseguir a los miembros de la comunidad étnica Rohingya pese a que el grupo armado no sea más que un conglomerado de algunas personas que se defienden con medios precarios de los abusos del gobierno de Myanmar (Edroos, 2017).

cómo y qué tipo de procedimientos lleva a cabo para hacer cumplir su propia normativa y políticas de autorregulación, y quién tiene a su cargo dicho trabajo, relacionado igualmente con los problemas asociados a los derechos ARCO.

Y en un cuarto nivel, los riesgos de transparencia del responsable y encargados del tratamiento de los datos con otros actores: los Estados anfitriones, sus donantes, los Estados de los que huyen las personas refugiadas; pero también actores atípicos al escenario humanitario como las empresas y corporaciones privadas (Jacobsen, 2016, 2017; Sandvik, 2016; Sandvik y Jacobsen, 2016). Un riesgo que no solo tiene que ver con los términos y condiciones de dicha cercanía sino con lo que esta reporta en materia de impacto para los derechos de las personas refugiadas (Greenwood, 2017; Marino, 2021; Read *et al.*, 2016; Willits *et al.*, 2019).

La relación de estos riesgos, junto a los otros que hemos advertido sobre otros principios, sostienen una suerte de relación de causalidad circular donde la ausencia de transparencia y rendición de cuentas genera procesos débiles de gestión de la información personal de las personas refugiadas. Y la gestión débil y defectuosa del tratamiento de los datos, afirma la opacidad del actuar de los

Marcos legales de protección de datos ¿aplicables en el contexto humanitario?
Por último, diversos autores concurrieron en apuntar las dificultades asociadas a la aplicación de marcos legales en materia de protección de datos tratándose de agentes humanitarios.

Los problemas, según las posturas revisadas, pueden ser divididos así: (i) los de aplicación de marcos legales existentes, (ii) los de inexistencia de marcos legales adecuados, y (iii) los de debilidad de los mecanismos de autorregulación del propio sector en esa materia.

(i) Los problemas de aplicación de los marcos legales existentes. Al respecto la literatura se centró en la regulación comunitaria europea vigente desde 2018, el RGPD, por ser una de las regulaciones comunitarias más comprensivas de los últimos años. Según Latonero y su equipo de investigación, dicha regulación no tiene previsiones asociadas a su aplicación en contextos de migración o ayuda humanitaria, por lo que hay un vacío en las políticas o lineamientos que orienten el tratamiento de datos, así como el despliegue de tecnologías digitales para su procesamiento en dicho contexto (2019).

En el mismo sentido, Gazi afirma que, como reflejo de lo anterior, la literatura que analiza la aplicación del RGPD en la acción humanitaria es más bien limitada, pese a que el tratamiento tiene características que lo tornan en un reto que debería llamar la atención: el procesamiento a larga escala de cantidades masivas de datos, barreras culturales y de idioma entre el responsable y el titular del dato, la vulnerabilidad de los titulares y el impacto que esta tiene en aspectos como el consentimiento, entre otros (2020).

Al respecto, Gazi también menciona que la extraterritorialidad del RGPD no debería ser un problema pues no solo protege al ciudadano europeo sino al titular del dato cuando el responsable o encargado del tratamiento se domicilian o tienen base de operaciones en la Unión Europea, o que estando fuera de dicho espacio comunitario ofrecen servicios a beneficiarios localizados allí (2020).

Zara Rahman parece sugerir otra arista de naturaleza más bien política. A propósito del caso documentado por Human Rights Watch (2021) sobre el tratamiento de datos de los Rohingya por ACNUR, dice, el problema de las personas refugiadas es que no son europeas, de serlo, importarán en la cuestión de la protección de sus datos y para criterios legales como el de la extraterritorialidad pues "[t]here is no way that the personal data of nearly a million European people would be treated like this without a massive outcry, without resignations and policy overhauls, without fines, firings, and legal ramifications".

Aun si el criterio de la aplicación extraterritorial del RGPD fuera tomado en serio, Kaurin (2019) expresa que, una vez las personas refugiadas cruzan una frontera y arriban al Estado anfitrión o de destino en Europa, aquellas no dejan de tener una condición jurídica precaria en su condición de no-ciudadanos lo que, una vez más, los deja vulnerables a los abusos.

También, según la autora, se trata de un asunto de confianza, pues las personas en búsqueda de refugio y en proceso de solicitud de protección internacional, de tener acceso a mecanismos de defensa de sus datos personales, se abstendrán de ejercerlos por el temor de acudir a las autoridades públicas por el riesgo de que estas las deporten o informen a otra autoridad facultada para ello para que lo haga en su lugar (Kaurin, 2019). A su afirmación no aporta experiencias concretas a diferencia de los otros problemas en materia de protección de datos que respalda con testimonios de personas refugiadas.

La Conferencia Internacional de Comisionados de Protección de Datos y Privacidad aludió, en su conferencia de 2015, a la existencia de un marco de lineamientos dirigidos a abordar el tratamiento de datos, en general, en la acción humanitaria. Mencionan:

> [The] Opinion of the EDPS on the Proposal for a Regulation establishing the European Voluntary Aid Corps (on volunteer management, 2012), Professional Standards for Protection Work adopted through an ICRC-led consultation process (2013), Toward a Code of Conduct: Guidelines for the Use of SMS in Natural Disasters of the GSMA (2013), and the Policy on the Protection of Personal Data of Persons of Concern to UNHCR of the UNHCR (2015) (37th International Conference of Data Protection and Privacy Commissioners, 2015: 3).

Al respecto, concluyen que "[y]et the adoption of such frameworks by the overall humanitarian community is still scarce", por lo que sugieren la necesidad de guías más claras, que no compliquen la acción humanitaria sino que la facilite, sin reflexionar previamente sobre por qué habiendo guías y lineamientos con vigencia de más de una década, los problemas siguen radicando en su adopción y aplicación, o qué es lo que resulta insuficiente de los lineamientos actuales para que sea preciso crear otros (37th International Conference of Data Protection and Privacy Commissioners, 2015: 3).

Finalmente, aunque haya claridad sobre la aplicación de normativas acordes a los estándares mencionados, los regímenes de inmunidad de los que gozan los agentes humanitarios del sistema ONU dificultan la aplicación de un régimen específico de protección de datos, cualquiera que este sea (Gazi, 2020; *Kuner et al.*, 2017). Latonero afirma que "it is important to note that intergovernmental organizations, such as the UN, claim immunity from the GDPR and similar data regulations" (2019: 18).

(ii) Los problemas de inexistencia de leyes de protección de datos adecuadas. Duffield señala que contribuye a la desigualdad internacional la inexistencia de leyes de protección de datos adecuadas a nivel global. En ese sentido, dice que las tecnologías digitales y los procesos de recolección de datos biométricos en los países del Norte Global suelen estar sujetos a más altos estándares por las preocupaciones que generan en materia de privacidad de las personas, al tiempo que estas son desarrolladas o desplegadas sin escrutinio en los países del Sur donde las regulaciones son débiles o no existen (Duffield, 2016a).

Aunado a esto, Kaurin agrega que las agencias y organizaciones de ayuda humanitaria trabajan en contextos en donde el Estado de derecho es débil, o en donde el acceso a la justicia, si lo hay, es limitado, y que en materia de protección de datos los mecanismos de protección pueden ser embrionarios, inexistentes o no exigibles (2019). Esa misma razón la sostienen Bouffet y Marelli quienes, además, hacen notar la falta de acuerdo de algunos estándares sobre el tratamiento de ciertos datos sensibles, como los metadatos asociados a las comunicaciones de las personas, lo cual puede complejizar algunas discusiones sobre la necesidad de regulaciones o estándares de alcance global (2021).

Ante escenarios de este tipo, las brechas creadas por la ausencia de normativa que acoja los más altos estándares, o de haberla y no ser aplicable gracias a los regímenes de inmunidad de los que gozan algunos actores humanitarios, crea el caldo de cultivo ideal para la experimentación y los abusos a los derechos humanos de las personas refugiadas (Akhmatova y Akhmatova, 2020).

(iii) Los problemas de la autorregulación. Alexander Beck, oficial de protección de datos de ACNUR en el 2018, señaló en una entrevista para el blog de esa agencia que la política de protección de datos de la misma se inspiraba en los estándares del GDPR sobre privacidad por diseño y por defecto. Su aplicación, no obstante, no podía ser obstáculo para el imperativo humanitario "[i]n many situations where data protection rules appear to slow down processes, the reality is that they have not been considered and factored in at the beginning" (UNHCR, 2018d).

En materia de autorregulación Oxfam constituye quizá uno de los ejemplos más significativos en la materia. En 2015 decidió imponer una moratoria para detener el despliegue y uso de sistemas de identificación biométrica en sus operaciones. En 2017, encomendó a la organización The Engine Room que evaluará sus impactos para la población beneficiaria de sus programas. Producto de dicho trabajo se publicaron dos documentos, uno que evaluó las brechas de implementación de las políticas de protección de datos a nivel interno (Oxfam y Engine Room, 2017), y otro sobre identificación de riesgos y beneficios de los sistemas de identificación biométrica para la provisión de ayuda humanitaria (Rahman *et al.*, 2018).

Producto de dicho período de análisis y moratoria, el 18 de mayo de 2021 se publicó finalmente la política de privacidad sobre el uso y despliegue de sistemas de biometría por la organización. En su texto se adoptan siete principios: planificación, proporcionalidad y responsabilidad; rendición de cuentas; control compartido con las personas y las comunidades; abordaje de riesgos individuales y comunitarios; abordaje de los riesgos de seguridad; empleo de prácticas responsables en

los sistemas de biometría; y definición de la relación con terceras partes. Política que estará sujeta a revisiones periódicas y procesos de retroalimentación continuos (Eaton-Lee y Shaughnessy, 2021).

Sin embargo, al mirar este triple panorama de manera conjunta, autores como Raymond, Al Ackar y Berens, sostienen que esa fragmentación de las aproximaciones a los marcos reguladores de la protección de datos en la acción humanitaria, ha impedido un mejor entendimiento sobre los procesos de tratamiento de datos en dichos contextos; al tiempo que sostienen que la recolección y análisis de datos personales no debería tener lugar hasta tanto dichos estándares no se hayan acordado y cubran a todos los actores que participan en tal actividad (2016). Kaurin en todo caso recuerda que lo que se necesitan son, además, mecanismos de cumplimiento normativo y exigibilidad de las políticas internas pues de lo contrario, dichos actores no tendrán el incentivo necesario para seguir sus propias normas (2019).

***

En resumen. Al inicio de este capítulo nos propusimos explorar los riesgos en materia de privacidad, más concretamente, de protección de datos para las personas refugiadas que son expuestas al despliegue de tecnologías digitales en la acción humanitaria.

Para ello, se proveyó un contexto general sobre el "deber ser" de la privacidad, un derecho humano de recepción universal que reconoce como titular a todas las personas, sin excepción orientada en su nacionalidad, origen étnico, o estatus migratorio. Y se desarrollaron los estándares de la protección de datos, derecho comprendido en el de la privacidad, orientado por un conjunto de principios de amplia recepción en otros sistemas jurídicos como el europeo, latinoamericano, asia-pacífico y africano.

Los principios recopilados fueron, en concreto, los legalidad y lealtad; finalidad y conservación limitada; transparencia; consentimiento libre e informado; el principio de minimización; el de exactitud; el de seguridad y confidencialidad; el de acceso, rectificación, cancelación y oposición; y el de responsabilidad y rendición de cuentas. Se los empleó como punto de referencia en tanto que no existe una suerte de marco jurídico de la privacidad específico para los espacios o ambientes en los que se despliega la acción humanitaria.

En breve, se mencionó que el principio de legalidad y lealtad del tratamiento implica que el tratamiento de datos debe suceder amparado en un propósito consagrado en un marco legal (como el cumplimiento de un contrato, o la provisión de un servicio o bien necesario, etc.) o atender al consentimiento expreso y libre de la persona.

El de finalidad y conservación limitada busca que el tratamiento se ajuste al objetivo que prometió realizar y que debe ser claramente advertido y expresado de manera transparente a la persona. La finalidad limitada implica describir qué datos se requieren, para qué serán tratados, con quiénes serán compartidos, para qué fin y por cuánto tiempo serán almacenados o conservados.

El de transparencia apunta a que la información proveída sea clara, accesible, comprensible, en términos que se correspondan con las políticas de tratamiento de datos vigentes, pero sobre todo con la práctica de la propia organización. La transparencia debe atravesar todo el ciclo del dato, desde su recolección hasta el momento de su eliminación de una base de datos determinada.

El de consentimiento libre e informado parte por reconocer a la persona como autónoma y autodeterminada, capaz de tomar sus propias decisiones que, en la protección de datos, se manifiesta en aceptar o no la política de tratamiento de datos de ese tercero que pretende acceder a su información personal para proveer al titular a cambio un bien o servicio. El consentimiento, para ser libre, se caracteriza por la previa entrega de información sobre el por qué, el para qué y el cómo del tratamiento de los datos. Su manifestación debe ser expresa, inequívoca, y debe irradiar todo el proceso del tratamiento cuando existan cambios o modificaciones a la política prometida y frente a la cual se consintió en primer lugar.

El de minimización requiere que la información recolectada lo sea en la menor cantidad posible, y que los datos recolectados se correspondan al fin propuesto, su recolección debe evitar la captura de datos sensibles si con otros, de naturaleza menos invasiva, se logra el mismo objetivo inicial que justifica la recolección. El de exactitud prevé que la recolección y tratamiento del dato sea veraz, precisa, esté actualizada y sea información completa. El de seguridad y confidencialidad, requiere el despliegue de medidas técnicas, organizacionales y administrativas para garantizar el almacenamiento seguro de los datos personales, prevenir accesos o usos no autorizados, así como filtraciones, pérdidas, modificaciones o eventos de divulgación de la información. Medidas que deben ser más intensas cuando más sensible sea la información recolectada y almacenada. El de acceso, rectificación, cancelación y oposición prevé como titular para su ejercicio a la persona quien debe poder acceder a mecanismos ágiles, sencillos, eficaces y gratuitos para extender al responsable del tratamiento sus solicitudes.

Se trata, en definitiva, de un conjunto de principios aplicables al tratamiento de datos, incluyendo los sensibles. Estos últimos reciben, en los estándares internacionales revisados, una protección mucho más intensa, no solo por su capacidad para revelar información que alude a aspectos *sensibles* para la persona, sino por los efectos que puede producir su uso, acceso o recolección no autorizada y que puede derivar en eventos de discriminación contra su titular, entre otros.

Referimos también que la recolección de datos personales para facilitar el despliegue de la acción humanitaria es indispensable para la realización del mandato de organizaciones dedicadas a atender y beneficiar a la población refugiada, por ejemplo, llevar registro de la ayuda entregada y hacer trazabilidad desde la entrega, entre otros. Datos de diversa naturaleza que comprenden igualmente a los sensibles, específicamente los biométricos. Un tipo de dato que en las últimas décadas ha sido recabado especialmente por actores como ACNUR y el Programa Mundial de Alimentos a través de tecnologías digitales para, en teoría, evitar los eventos de fraude y suplantación de la identidad, así como identificar a las personas refugiadas que han perdido sus documentos durante su jornada de huida y migración.

Ante dicho escenario, la literatura revisada apuntó riesgos frente a algunos de estos principios, concretamente, los de consentimiento informado; finalidad y conservación limitada; exactitud; acceso, rectificación, cancelación y oposición; seguridad y confidencialidad; y transparencia.

Los riesgos advertidos sobre el principio de consentimiento enfatizan en la ausencia de información proveída a la persona sobre el por qué, el para qué, y el cómo del tratamiento de sus datos. Adicionalmente a ello, fue advertida una brecha de la información profundizada por barreras de idioma, la rapidez con la que es conducida el proceso de recolección, y barreras de tipo cultural así como la experiencia traumática de la huida de su país y la fatiga de recolección de sus datos por otros actores que impactan, en su conjunto, en lo que significa para la persona refugiada la privacidad y la protección de datos cuando se encuentra en un ambiente en el que se relaciona con agentes humanitarios.

También fue señalado como un riesgo la ausencia de consentimiento libre y expreso, pues los autores apuntaron que, si el recibimiento de ayuda humanitaria era condicionado a la entrega previa de los datos personales del titular, incluyendo los biométricos, la libertad era a la final artificiosa pues en los casos revisados no se ofrecía a la persona alternativas que no derivaran en su exclusión.

Los riesgos sobre el principio de finalidad y conservación limitada se caracterizaron por las preocupaciones de los autores en aspectos como la ausencia de claridad sobre los objetivos por los cuales se lleva a cabo la recolección de datos personales, especialmente los biométricos, sobre los usos que se dará a dicha información y por cuánto tiempo, y los terceros que tendrán acceso a la misma y cómo dicho acceso se relaciona a la realización de los fines iniciales que justificaron la recolección.

Los riesgos para el principio de seguridad y confidencialidad se centraron en los temores hacia brechas de seguridad, el acceso accidental de terceros a la información sensible que conservan y tratan las agencias humanitarias, la ausencia de despliegue de medidas de seguridad por dichas organizaciones, y la ausencia de notificación a la persona afectada de los eventos de seguridad que comprometan su información y puedan impactar en su integridad física o el ejercicio de otros derechos.

En el principio de exactitud de los datos, los eventos de transliteración de otros idiomas al inglés, como al árabe, el darí y el kurdo impacta en la veracidad y precisión de los datos reportados. Aquello, sin embargo, va más allá de la introducción de datos imprecisos en campos equivocados en los formatos de registro de la persona refugiada, y se traduce especialmente en la imposibilidad de acceso a la ayuda humanitaria, así como en la imposibilidad técnica de los sistemas de registro para permitir efectuar su corrección o ajuste.

Los riesgos en materia de acceso, rectificación, cancelación y oposición recogen aquellos otros que se asocian a los defectos de entrega de información clara, accesible y completa, aunados a los miedos –fundados o no– de accionar y elevar solicitudes de queja o denuncia por el indebido tratamiento de datos ante la misma agencia humanitaria que provee de ayuda y asistencia a las personas refugiadas.

Y finalmente, los riesgos recogidos en la literatura sobre el principio de responsabilidad y rendición de cuentas fueron indicados sobre distintos niveles.

Un primer nivel, sobre todo el ciclo de vida del dato, en la ausencia de información que deja claros los términos desde su recolección hasta su eliminación o cancelación. Un segundo nivel, a la ausencia de razones y evidencia que propiamente soportan y justifican la existencia de los sistemas de registro biométrico de las personas refugiadas. Un tercer nivel, los riesgos de transparencia en el relacionamiento a nivel interno de los actores humanitarios, la difusión y correspondencia entre sus prácticas en materia de tratamiento de datos y lo que dicen sus políticas que debieran hacer. Y un cuarto nivel, asociado a la claridad sobre los términos y alcance del relacionamiento de los actores humanitarios con otros del mismo tipo, con Estados, así como con actores atípicos en la escena humanitaria como las empresas privadas del ámbito tecnológico y cómo impacta cada uno y sus intereses en la protección de la privacidad y los datos de la persona refugiada.

Un riesgo, ajeno a los principios de protección de datos pero relacionado a su vigencia, tuvo que ver con las dificultades asociadas por los autores a (i) la ausencia de marcos jurídicos de protección de datos aplicables a los actores humanitarios, (ii) la existencia de marcos jurídicos con estándares elevados de cuya aplicación escapan los actores humanitarios por la existencia de los regímenes de inmunidad que les favorece y los (iii) defectos de los sistemas de autorregulación en donde el diseño de la norma y su aplicación depende del mismo actor en su doble rol de juez y parte.

En este recorrido sobre los riesgos, sin embargo, los autores coincidieron en preocupaciones asociadas al despliegue de la tecnología de reconocimiento biométrico y su despliegue por dos actores humanitarios que más han impulsado su uso en la última veintena, sobre las personas refugiadas y sus datos más sensibles: ACNUR y el Programa Mundial de Alimentos.

Lo que este conjunto de riesgos parece sugerir, en el fondo, es que el problema de la protección de datos va más allá del diseño de las políticas de privacidad y tiene que ver con otros, ajenos a dicho campo –sin demeritar en todo caso su gravedad e impacto–.

Así, pese a que existen mecanismos de autorregulación que parecen adaptarse y corresponderse con los estándares de protección de datos a los que referimos al inicio, y no obstante los hallazgos de las auditorías de sistemas biométricos de ACNUR y el Programa Mundial de Alimentos que han visibilizado fallos importantes sobre la aplicación de dichas políticas en la práctica, el despliegue de la tecnología biométrica continúa, sin que en el fondo haya mediado hasta ahora un proceso autorreflexivo sobre si los riesgos valen la pena de cara a los beneficios esperados, la pregunta es ¿por qué?, ¿qué es lo que empuja con tanta fuerza a dicha tecnología en un contexto complejo como el de la atención humanitaria de personas que huyen por diversos motivos de sus países de origen, pese a que la literatura revisada llama la atención sobre una diversidad de riesgos latentes que en varios casos ya han acaecido?

Entender cuál es el problema subyacente al de la protección de datos obliga a reconocer, en todo caso, cuáles pueden ser los intereses en juego y los riesgos para

los actores, más allá de los que vimos en materia de privacidad para las personas refugiadas; así como examinar de cerca la promesa de las tecnologías digitales de mayor despliegue, las biométricas, para entender por qué, a pesar de los riesgos y fallos advertidos en nuestra revisión se sigue desplegando y masificando su uso. Situación que exploraremos en el capítulo siguiente.

Capítulo 3

EL PROBLEMA DETRÁS DEL PROBLEMA. LA PROMESA TECNO-ENTUSIASTA EN LA ACCIÓN HUMANITARIA

Hasta ahora nuestra atención estuvo centrada en la revisión de la literatura dedicada a advertir riesgos en materia de protección de datos para las personas refugiadas, cuando se despliegan tecnologías digitales en la acción humanitaria por agentes cuya misión es proveer asistencia y ayuda.

Vimos cómo los riesgos advertidos se centran en ciertos principios de la protección de datos: consentimiento; finalidad y conservación limitada; seguridad y confidencialidad; exactitud de los datos; el principio de acceso, rectificación, corrección y cancelación; y el principio de responsabilidad y rendición de cuentas.

Las preguntas que surgen ahora tienen que ver con los problemas más allá del problema: (i) los riesgos y ventajas que reportan las tecnologías digitales en la acción humanitaria para el resto de actores, más allá de la privacidad de las personas refugiadas, y en definitiva (ii) cuál es la promesa que, pese a los riesgos advertidos, sigue empujando su despliegue masivo en la acción humanitaria.

1. ¿Quién obtiene qué del despliegue de tecnologías digitales en la acción humanitaria?

Responder a la pregunta sobre quién obtiene qué del despliegue de las tecnologías digitales en la acción humanitaria para la atención de personas refugiadas puede permitir una mayor comprensión sobre por qué, pese a los riesgos advertidos en materia de protección de datos, sigue siendo una opción válida para algunos actores de dicho ecosistema.

En esta sección no habremos de desentrañar con profundidad las razones, "reales" sobre por qué la presencia de tecnologías, como la biometría, es cada vez mayor y más envolvente de la acción humanitaria que se procura a las personas refugiadas, pero las razones a las que apunta la literatura revisada y que obran como motivadores para ello, pueden ampliar el acercamiento al problema de esta tesis como uno que se enfoca en la protección de datos, pero que para explicarse debe ir más allá.

Para ello, al igual que en el capítulo anterior, se diseñó una tabla de recolección de información. En ella se relacionan los actores, intereses y beneficios que fueron apuntados por la literatura revisada. Veremos, en su orden, el listado de intereses y riesgos para los actores del sector privado, los actores humanitarios, y las personas refugiadas.

Tabla 2. Identificación de intereses y riesgos: sector privado

Actor / Criterios	Sector privado
Composición	Facebook, Amazon, Google, Palantir, Accenture, Proveedores de telefonía e internet móvil, Mastercard, Carrefour, Western Union, Iris Guard, Microsoft
Intereses y beneficios	Conferir a las personas refugiadas con identificación legítima y confiable
	Proveer servicios esenciales para la jornada de migración y para el manejo de las migraciones
	Ayudar a superar barreras de idiomas
	Conectar a refugiados con otras redes de personas refugiadas y con sus familias
	Proveer servicios financieros a personas refugiadas a través de apps móviles
	Asistir a refugiados en su integración en lugar de destino para acceder a empleo, seguros, servicios de salud
	A través de la biometría una mayor eficiencia en la provisión de un bien o servicio
	Oportunidades de branding
	Acceso a datos del sector humanitario
	Aumento de su visibilidad
	Oportunidades para pilotear nuevas tecnologías
Riesgos	No fueron advertidos riesgos para estos actores

Fuente: Elaboración propia.

Un amplio *set* de tecnologías digitales en el ambiente humanitario pueden ser provistas desde abajo, por comunidades de personas refugiadas o comunidades técnicas de voluntarios y que han recibido el nombre de "*digital humanitarians*", que desarrollan alternativas para facilitar la jornada de huida y arribo al país de tránsito o destino de otras personas refugiadas y, que en ocasiones, se dirigen a aportar en las situaciones de emergencia una vez una crisis humanitaria nueva ha estallado (Benton y Glennie, 2016; Marino, 2021).

Así como también pueden ser provistas por grandes compañías tecnológicas que (i) ofrecen sus productos sin diferenciar en si la población que la usa es refugiada o no, o que (ii) desarrollan tecnologías específicas o proveen de usos específicos a tecnologías ya existentes para la atención de la población refugiada. Actores a los que refiere la tabla de más arriba.

Por ejemplo, compañías como Facebook, proveen acceso a su red social para interconectar a las personas refugiadas entre ellas, como lo haría con cualquier otro grupo usuario de su plataforma (Gelb y Krishnan, 2018; Latonero y Kift, 2018). Lo mismo sucede con las compañías proveedoras del servicio de telefonía móvil y con Google a través de su servicio de traducción, cuya beneficio según Latonero y su equipo de investigación, es el de proveer servicios esenciales para la jornada de

migración y huida de las personas refugiadas, sin que sus productos tecnológicos hayan sido diseñados en concreto para la población de este tipo (2019).

Compañías como MasterCard, Palantir, Microsoft, Accenture, IBM, IrisGuard entre otras, dotan de usos específicos a tecnologías digitales ya existentes para satisfacer acuerdos contractuales, suscritos con agentes humanitarios del sistema ONU dedicados a la atención de las personas refugiadas.

Varios ejemplos dan cuenta de esta tipología de desarrollos existentes trasladados a la arena humanitaria, más concretamente, a lo que constituye el escenario articulador del proceso de huida de las personas refugiadas y que se materializa en la existencia de los campos de refugiados –y en la existencia de centros urbanos de atención a las personas refugiadas– (Jacobsen, 2016). Destacan el caso del Programa Mundial de Alimentos, beneficiaria de la tecnología de pagos electrónicos de MasterCard el cual habilita las transferencias monetarias a tarjetas pre-pagadas. Dichas tarjetas son entregadas a las personas refugiadas para acceder a los alimentos al tiempo que están dirigidas a dinamizar con cada transacción a la economía local (Development Assistance Roadmap Portal in the Middle East, 2018).

Sucede también con Iris Guard, la compañía que ofrece los sistemas de reconocimiento biométrico y que se articula con las tecnologías digitales de pagos electrónicos de ACNUR y la agencia de alimentos de la ONU. Y con Microsoft, que provee de los servicios de almacenamiento en la nube en el que se hospeda el servicio de autenticación biométrica del Iris Guard (Access Now, 2021; Thomsen, 2019).

Estos ejemplos del despliegue de algunas tecnologías digitales en la acción humanitaria, operan de la misma manera que el "ensamblaje biométrico" al que refiere Mirca Madianou (2019) para denominar la articulación de las tecnologías y empresas que proveen servicios cuya promesa es lograr la automatización de procesos, aumentar su eficiencia, optimizar recursos o evadir eventos de fraude en los procesos de identificación y verificación de las personas refugiadas, entre otros. Ensamblaje que, según la literatura revisada, tiene un hilo común: la de la percepción de numerosos beneficios con ningún riesgo a la vista.

El hecho de que autores como Latonero (2019), Gelb y Krishnan (2018), y Madianou (2019) adviertan ventajas y beneficios, pero ningún riesgo para compañías de este calado es sugerente. Incluso, los riesgos asociados a dichas compañías no se refieren al impacto que pueden sufrir sino al impacto que su presencia ocasiona en la acción humanitaria para otros actores, y que tienen que ver con preocupaciones en materia de privacidad, de rendición de cuentas y transparencia, de discriminación, de mercantilización y erosión de los principios de la acción humanitaria, entre otros.

Katja Jacobsen (2016) apunta a la ausencia, hasta hace poco, de una contranarrativa exploratoria de los debates, riesgos, desencuentros y problemas que representa la incursión de estos actores en el escenario humanitario; opuesta a esa otra narrativa dominante de la innovación y que Scott Smith denomina también como la "neofilia" del humanitarismo.

La narrativa de la innovación está acompañada del entusiasmo y la expectativa sobre el poder inherentemente positivo de las tecnologías digitales, acompañada de algunos lugares comunes como la noción de lo disruptivas que pueden ser para adaptarse a escenarios complejos y dinámicos, así como su potencial para revolucionar la acción humanitaria en múltiples aspectos (Rahman *et al.*, 2018; Scott-Smith, 2016).

Más recientemente, dicha narrativa ha sido encapsulada bajo nombres llamativos que dicen apoyarse en la realización de los Objetivos de Desarrollo Sostenible. El eslogan del *Data for Good*, es la más reciente propuesta de las grandes compañías tecnológicas para contribuir con sus desarrollos innovadores al bien social en el marco de la acción humanitaria. Desde una mirada crítica, G. Hosein (2018) apunta:

> Of course, Facebook and others want to sell the idea of Data for Good. It helps launder their business model. And it needs cleaning. Facebook was caught recently collecting vast amounts of telephone records from Facebook users without meaningful controls against this practice (particularly in older Android phones, which I bet most of the people who are seeking protection are using). Is that amongst the data that Facebook is offering to 'share' with the humanitarian sector under the aegis of Good?

Sara Marino (2021) en su libro *Mediating the Refugee Crisis: Digital Solidarity, Humanitarian Technologies and Border Regimes*, aclara que *Data for Good* o *Data for social Good* es el lenguaje de la innovación de un sector que tiene poco que ver con los principios de independencia, imparcialidad o neutralidad, pero que encuentra arraigo en la acción humanitaria por la promesa para asegurar un impacto positivo que garantice su sostenibilidad y financiación.

Sandvik, Jacobsen y McDonald son críticos de la narrativa de la innovación pues resulta fértil para promover tecnologías digitales experimentales y en desarrollo que, en el escenario humanitario, no han sido sometidas a un análisis crítico sobre su impacto en las personas ni en los peligros que dicha agenda pueda implicar a nivel organizacional y en la realización del mandato de agencias dedicadas a la atención de personas refugiadas (2017).

La narrativa de la innovación, según Madianou, se sobrepone incluso a evaluaciones iniciales que debieran poder determinar si una tecnología digital es o no la solución a un problema en dicho terreno (2019b). Scott-Smith, bajo la idea de la neofilia del humanitarismo, aclara:

> However, this 'love of the new', with its triumphant narrative of progress, makes humanitarian innovators blind to the often mundane humanitarian practices that really change people's lives; *it produces a disconnect between the enthusiasms of innovators and the lives of the people they are meant to assist* (2016: 5). (Subrayado propio)

Autores como Duffield (2016) van un paso más allá, apuntando que la narrativa de la innovación termina produciendo una suerte de encerramiento de las personas afectadas en una frontera digital que, en vez de permitir el ejercicio de la libertad y su adaptación a contextos de incertidumbre, la enclaustran en "soluciones" de las que no tienen salida. Latonero y Kift, en un sentido similar, apuntan

cómo las tecnologías digitales en ambientes de migración –refiriendo también a la migración como un ejercicio de movilidad de las personas refugiadas–, pueden llegar a instrumentalizar una forma de frontera más allá de la pared, del muro, de la cerca (2018).

Uno de los riesgos aparejados a la narrativa de la innovación tiene que ver con el pase libre que adquieren las grandes empresas tecnológicas fruto de los acuerdos que suscriben, a su vez, con grandes agentes humanitarios de la ONU que atienden a población refugiada. Pase libre que se traduce no solo en la extensión, hacia estos actores, de los beneficios asociados a los regímenes de inmunidad legal de los que gozan los actores humanitarios, doblemente blindados por el escudo del "imperativo moral" que su rol en el ámbito humanitario satisface. Ventaja ampliada, pues abre de par en par la posibilidad de experimentar con tecnologías digitales en escenarios en los que los niveles de riesgo aceptable se ubican en otro umbral distinto del que regirá en contextos regulados y de normalidad (Sandvik *et al.*, 2017).

Una situación que, según Sandvik, Jacobsen y McDonald (2017), se explica en tanto que los contextos humanitarios han constituido tradicionalmente una especie de periferia o estados de excepción en donde se justifica el "hacer cualquier cosa mejor que no hacer nada", que conlleva a la flexibilización de ciertos estándares por la urgencia que los rodea, y en el que la innovación sirve como amalgama para combinar los valores que mueven al sector privado de las tecnologías, enfocado en la eficiencia y la respuesta de un mercado determinado, con los valores del humanitarismo.

Amalgama que cada vez más limita la lectura de los problemas de la acción humanitaria presuntamente solucionables a partir de la intervención tecnológica y que, como resultado, modifica las relaciones entre los actores humanitarios y sus beneficiarios al convertirlos en sujetos de experimentación/clientes. Situación que diluye las oportunidades de supervisión y regulación de sus actividades y que tiene el potencial de sacrificar los principios de la acción humanitaria, entre otros (Sandvik *et al*., 2017).

Que los contextos en que se desenvuelve la acción humanitaria puedan ser leídos como "theatres of proof" o escenarios de experimentación, según los mismos autores, no es producto de la suma reciente de las grandes compañías de *Silicon Valley* a la ecuación (Sandvik *et al.*, 2017: 326). Es una lectura con antecedentes que remontan al pasado colonial y postcolonial de la acción humanitaria (Jacobsen, 2015).

Sin embargo, la participación de grandes empresas tecnológicas que, a la fecha, siguen siendo cuestionadas por cómo sus modelos de negocio se distancian de los estándares en derechos humanos (Brown, 2020; Morozov, 2012; Pasquale, 2015), torna más sensible su participación en un contexto jurídicamente inestable (Jacobsen, 2015). Más recientemente, el Relator para la Pobreza Extrema de las Naciones Unidas reconoció, sin medias tintas, que la realidad de los derechos humanos de cara a las grandes compañías tecnológicas, no es una de distancia amplia sino de desregulación[1] deliberada promovida por los Estados (2019).

1 "The reality is that Governments have certainly not regulated the technology industry as if human rights

Además, dicho pase libre se ve complementado con el acceso a las grandes cantidades de datos de las personas beneficiarias de la acción humanitaria que permitan a los actores privados entrenar y probar nuevas tecnologías a cambio del despliegue de capacidades y recursos que urgen a la acción humanitaria. Recursos con los que no cuenta ante un escenario de desfinanciación progresiva y de retirada de los Estados como donantes.

Otros autores añaden a dicho pase libre elementos como la posibilidad de efectuar campañas de *branding* o promoción de sus marcas, y lograr el aumento de su visibilidad a partir del uso corporativo del lenguaje humanitario (Burns, 2019; Madianou, 2019). A cambio, los actores humanitarios –especialmente los que pertenecen al sistema ONU– externalizan en estos actividades de investigación y el impulso del desarrollo en los territorios en que se despliegan, evadiendo con ello la posibilidad de rendir cuentas a terceros (Sandvik *et al.*, 2017).

Pese a esto, autoras como Marino, invitan a la aproximación a este tipo de actores con distancia, pues la literatura que suele advertir el rol de la participación de las grandes compañías tecnológicas en la acción humanitaria, lo suele proyectar en uno dos extremos: como increíblemente poderoso y positivo, o como inherentemente discriminatorio y problemático (2021).

Su visión, centrada especialmente en las tecnologías digitales para la acción humanitaria en beneficio de las personas refugiadas y desarrolladas por actores más pequeños, comunitarios y comunidades técnicas; tiene lugar a partir de la revisión de literatura, observaciones en campo y entrevistas a personas cuyos testimonios advierten sobre los riesgos que tiene el despliegue de tecnologías digitales en la acción humanitaria, sin importar tanto el tamaño del actor como el interés que los motiva.

Riesgos que van desde la datificación de la persona refugiada –que dice la autora, no hay que rechazar porque no puede ser resistida–, la amplificación de brechas preexistentes, riesgos en materia de privacidad y rendición de cuentas, entre otros (Marino, 2021).

Jacobsen añade, por su cuenta, los riesgos de cómo una mirada presuntamente neutral de esta incursión, como la pretendida por Marino (2015), puede llegar a despolitizar el impacto de los actores del sector tecnológico y sus tecnologías digitales aplicadas a la acción humanitaria, desconociendo el ejercicio del poder –instrumental y narrativo– que su despliegue significa sobre la vida de personas en condiciones de vulnerabilidad e indefensión.

Entonces, en el balance de más arriba, el sector privado aprovecha los beneficios de su aterrizaje al escenario humanitario, reportando pocos o ningún riesgo para estos y sus modelos de negocio, según la literatura revisada. Pasemos ahora al balance de riesgos y beneficios para los actores humanitarios.

were at stake, and the technology sector remains a virtually human rights-free zone. The big technology companies (frequently referred to as "big tech") and their governmental supporters have worked hard to keep it that way" (Special Rapporteur on extreme poverty and human rights, 2019, prr 35).

Tabla 3. Identificación de actores e intereses: actores humanitarios

Actores / Criterios	Actores humanitarios
Composición	Agencias ONU (ACNUR, Programa Mundial de Alimentos), los Estados hospedadores que actúan como tal, organizaciones no gubernamentales de tipo local y sociedad civil
Intereses y beneficios	Para todos los actores humanitarios
	Identificación y trazabilidad de todas las personas refugiadas para facilitar acceso a derechos
	Conferir a las personas refugiadas con identificación legítima y confiable frente a la pérdida, extravío o hurto de sus documentos de identidad
	Obtener más y mejor información centralizada sobre las zonas de intervención humanitaria
	Para los Estados
	Facilitar, a través de la identificación de personas refugiadas, su contacto con las autoridades del país en que se encuentran
	Fortalecer la capacidad de los Estados para manejar la migración (migrantes y personas refugiadas) de manera ordenada, segura y eficiente
	Para los agentes humanitarios no estatales
	Identificar a las personas refugiadas para proveerles de comida, albergue, entre otras formas de ayuda humanitaria de manera más eficiente para evitar casos de fraude y duplicación de personas beneficiarias
	Aumentar a través de los procesos de identificación de personas refugiadas, la responsabilidad y rendición de cuentas hacia los Estados donantes
	Informar a las personas refugiadas sobre el proceso de migración y refugio
	Ayudar a encontrar la familia de personas refugiadas extraviadas y rastrear migrantes y refugiados menores de edad no acompañados
	Aumentar la satisfacción del cliente (persona refugiada)
Riesgos	Para los actores humanitarios no estatales
	Ausencia de conectividad en el lugar en el que se hacen los procesos de identificación biométrica
	Condiciones climáticas complejas que dificulten funcionamiento de la tecnología biométrica (calor, polvo, humedad)
	Ausencia de condiciones favorables a la interoperabilidad
	Poner en juego los principios de la acción humanitaria
	Riesgos reputacionales, de legitimidad y eventuales litigios
	Desvío de recursos
	Seguridad y fiabilidad de los sistemas tecnológicos (false matches)
	Una carga mayor en materia de recursos para sostener las tecnologías digitales desplegadas

Fuente: Elaboración propia.

El panorama de intereses dista del que fue revisado sobre el sector privado. El despliegue de las tecnologías digitales para actores humanitarios de origen diverso –en el que se cuenta a los propios Estados–, denota una necesidad común de identificar a las personas refugiadas que huyen de sus países sin documentos o que los pierden en el camino.

La identificación, tal y como se la lista más arriba, obra como medio y fin en sí mismo para (i) proveer a las personas refugiadas de algún método para

permitirles probar que son quienes dicen ser, (ii) llevar a cabo los procesos de asignación de ayuda humanitaria evitando el fraude y (iii) asignar ayuda de manera que facilite la rendición de cuentas ante los donantes (Gelb y Krishnan, 2018; Jacobsen y Sandvik, 2018; Kaurin, 2019; Latonero *et al.*, 2019; Madianou, 2019; Rahman, 2021; Sandvik *et al.*, 2017).

También, se encuentran intereses que importan especialmente a los Estados. Entre esos, el mejoramiento de su capacidad para gestionar la crisis de movilidad humana, y facilitar a través de los procesos de identificación el contacto de la persona –referido esencialmente a aspectos sobre su búsqueda y detención– por las autoridades. No nos detendremos en estos actores –tal y como advertimos igualmente en el primer capítulo–, pues el despliegue de tecnologías digitales por los Estados tienen implicaciones y riesgos que merecen un análisis propio debido, entre otros, a su enfoque destinado al fortalecimiento de las capacidades de control fronterizo[2] y no tanto a la acción humanitaria (Duffield, 2016b; Kent, 2019; Latonero *et al.*, 2019).

Por su parte, los riesgos listados, que solo se refieren a los actores humanitarios, pueden agruparse en tres.

(i) Los riesgos que impactan a las tecnologías digitales que estos despliegan, y que se relacionan a los de tipo técnico (de conectividad y brecha digital que dificultan el funcionamiento especialmente de los sistemas de reconocimiento biométrico, su funcionamiento defectuoso por condiciones ambientales, y riesgos de tipo operativo que derivan en falsos positivos); así como los riesgos sociales de la tecnología o cómo su uso puede ampliar brechas, discriminar a las personas por razones de edad, sexo, raza, etc. (Crawford y Finn, 2015; Jacobsen, 2016; Madianou, 2019; Rahman *et al.*, 2018).

(ii) Los riesgos que impactan a la organización a nivel interno/externo, como los que podrían afectan su reputación, por ejemplo, por el indebido tratamiento de la información de la persona beneficiaria; y eventos de desviación de recursos y de aumento del gasto debido a la demanda de mayor inversión y capacidad que requiere el mantenimiento de las tecnologías desplegadas (Latonero *et al.*, 2019; Sandvik *et al.*, 2017; Slavin *et al.*, 2021).

Y (iii) los que impactan en la razón de ser de la acción humanitaria, que se materializan en la puesta en jaque de sus principios (Akhmatova y Akhmatova, 2020; Crawford y Finn, 2015; Dette, 2018; Gazi, 2020; Greenwood, 2017; Raymond y Al Achkar, 2016; Sandvik *et al.*, 2017).

Una revisión cercana de los riesgos sugeridos por la literatura permitiría incluso reducir este amplio listado solamente a los de tipo reputacional, pues es el único tipo de riesgo que impactan en la percepción de dicho actor, lo cual podría traducirse eventualmente en la reducción de la posibilidad que tenga de desplegarse en terreno o en la aceptación que tenga en la población que pretende impactar.

Como sea, y sin descartar los hallazgos relacionados más arriba, hay que advertir que ninguno de los autores revisados en el estado del arte refirió por qué,

2 Al respecto, sugiero consultar el informe "Raza, Fronteras y Tecnologías Digitales" de 2020 elaborado por la Relatoría Especial de las Naciones Unidas en formas contemporáneas de racismo, xenofobia e intolerancia que se dedica especialmente a este tipo de actor.

los riesgos que recaen sobre las tecnologías digitales desplegadas en la acción humanitaria se endosan, no a los actores del sector privado que las desarrollan y diseñan, sino a los actores humanitarios. Situación que puede deberse –cosa que habría que poder someter a una revisión más extensa de literatura–, a la percepción que se tiene sobre el primer responsable en una larga cadena de intervinientes, donde los que se relacionan de manera directa con las personas refugiadas son estos, y no las grandes compañías tecnológicas.

Tampoco se encontró ninguna indicación o advertencia sobre por qué, pese a que los Estados fueron referidos como actores en este grupo, no se les atribuyó ningún riesgo asociado, por ejemplo, al uso y despliegue de las tecnologías digitales. Lo que puede deberse a la diferencia que existe en las condiciones de despliegue y uso que, al contrario de lo que sucede con las agencias humanitarias, se caracterizan, por ejemplo, por ser ambientes fijos y acondicionados, menos expuestos al clima, y donde la brecha digital se encuentra si no resuelta reducida, para facilitar precisamente su funcionamiento en el punto de recepción de la persona refugiada. Hipótesis que, en todo caso, habría que poder someter a revisión más adelante.

Ahora bien, a los actores humanitarios no estatales fue posible atribuir, a su vez, un listado de los problemas que, dicen, serán resueltos por ciertas tecnologías digitales, así como los usos concretos que se dará a las mismas. Usos y problemas que deben poder ser leídos en clave de los intereses y beneficios listados más arriba.

Tabla 4. El qué, para qué y el cómo del despliegue de tecnologías digitales por actores humanitarios no estatales

Problemas que dicen resolver (qué)	Qué usos (para qué)	Qué tecnologías digitales (cómo)
El desconocimiento sobre quién es la persona refugiada y si es quien dice ser	Probar la identidad de una persona refugiada para determinar alcance y titularidad en el ejercicio de derechos Rastrear migrantes y refugiados menores de edad no acompañados	Sistemas de reconocimiento biométrico (huellas, iris, rostro); cámaras digitales; computadores, ***laptops***, tabletas; redes de conexión a internet
La ausencia de métodos de identificación confiable es propicia para eventos de fraude, así como casos de duplicación de la identidad en el sistema de protección internacional a refugiados	Simplicidad y eficiencia en el proceso en el proceso de identificación de la persona refugiada Fortalecer mecanismos de rendición de cuentas hacia los donantes Agilizar y hacer más efectivos y precisos los procesos de protección internacional a personas refugiadas Más justa distribución de recursos escasos Dotar de credibilidad a las operaciones humanitarias de cara a los donantes Facilitar la inclusión financiera de la persona y con ello aumentar sus chances de reintegración	Sistemas de reconocimiento biométrico (huellas, iris, rostro); tecnologías para la transferencia digital de dinero (tarjetas e-prepago, blockchain, machine learning, etc.)

Problemas que dicen resolver (qué)	Qué usos (para qué)	Qué tecnologías digitales (cómo)
Obtención lenta, descoordinada, incompleta o tardía de la información sobre zonas humanitarias	Conducir a la toma de decisiones basadas en datos Identificar las zonas y flujos en los que se movilizan las personas refugiadas que requieren asistencia Aumentar las capacidades para la destinación y coordinación en la entrega de ayuda Proveer más y mejor información a otras organizaciones, Estados y personas refugiadas	Acceso a servicios de geolocalización e imágenes satelitales a través de la telefonía móvil; sistemas de analítica predictiva; desarrollo de aplicaciones móviles y ***chatbots***; ***webscrapping***; drones

Fuente: Elaboración propia

Esta tabla pone de presente dos cosas. La primera, que los riesgos que advertimos en materia de protección de datos en el capítulo segundo se enfocan tan solo en una de las múltiples tecnologías digitales que están siendo desplegadas para la atención de las personas refugiadas por actores humanitarios, lo cual obliga en investigaciones posteriores a realizar un acercamiento mayor sobre cómo estas otras amplifican o profundizan algunas de las preocupaciones vistas.

La segunda, y que visibilizan las dos primeras filas de la tabla anterior, en las que se apunta nuevamente a la necesidad de identificar a la persona para prevenir eventos de fraude o duplicación que conduzcan a la destinación inefectiva de recursos que pueda impactar, finalmente, en la sostenibilidad y financiación de la acción humanitaria. Problema que se resuelve con la puesta en marcha de tecnologías biométricas.

La última fila de la tabla se refiere a un problema adicional, advertido por algunos autores a partir de una categoría de análisis distinta a la nuestra pero no por ello ajena a los problemas y riesgos que hemos advertido que aquejan a los actores humanitarios en el despliegue de tecnologías digitales intensivas en el tratamiento de datos. Según Greenwood, dicha categoría de análisis recibe el nombre de "humanitarian information activities",[3] es decir, las actividades que

3 Sobre esta expresión dicho autor sostiene: "Activities and programs which may include the collection, storage, processing, analysis, further use, transmission and public release of ta and other forms of information by humanitarian actors and/or affected communities" (Greenwood, 2017: 5). En su texto, Greenwood también apunta a la necesidad de que para dichas actividades y programas se adopte un enfoque orientado en los derechos humanos de las personas beneficiarias de la acción humanitaria, puesto allí también se visibiliza la presencia de los mismos problemas sobre participación de actores del sector privado sin que existan suficientes estándares éticos que orienten dichas prácticas, dice al respecto "humanitarians today lack sufficient ethical guidance adapted to the realities of humanitarianism in the information age to responsibly navigate the challenges and realities of the digital age" (24). También refiere a la importancia de que se implementen prácticas y políticas respetuosas de la privacidad de las personas antes, durante y después de que una "actividad de información humanitaria" se despliegue.

Scarnecchia, en el mismo sentido advierte sobre riesgos similares a los que trabajamos en el capítulo anterior al decir que "The urgent need for an accepted rights-based framework and approach to these activities is becoming painfully clear. The most acute gap in current humanitarian doctrine is a lack of clarity about what human rights people have relating to information in disaster, and what obligations humanitarian actors, governments, and the private sector have for realizing these rights." (2017).

En su informe "Ebola: A Big Data disaster. Privacy, property and the law of disaster" analiza el despliegue de herramientas de *big data* para la atención de la crisis del ébola en África, su autor, Sean McDonald, da cuenta cómo el despliegue articulado de sistemas de procesamiento y análisis masivo de la información personal de miles de personas en medio de crisis humanitaria –sus Call Detail Records o registros de llamadas para ser exactos, datos sensibles que el autor refiere como "the world's most sensitive data"

implican acceder, recoger, cruzar, transmitir y compartir fuentes de información públicas y privadas para tener una imagen precisa de lo que sucede en terreno y se precisa en la atención humanitaria (2017), y que no se orienta tanto en la tecnología empleada como en la naturaleza de la información obtenida.

Pero volvamos a lo advertido especialmente en las primeras dos filas de la última tabla. Autoras como Rahman, Madianou, Jacobsen y Sandvik (2018) levantan serias dudas sobre si los problemas que dicen justificar el despliegue de sistemas biométricos, se encuentran o no soportados en la evidencia y si dicha narrativa es temporalmente consistente con el uso de dichas tecnologías en terreno.

En su investigación sobre el sistema biométrico de Oxfam, y otros que estaban en funcionamiento en contextos humanitarios, Rahman (2018) entrevistó a diferentes tomadores de decisión que decían percibir el fraude en la distribución de recursos como un problema real. Sin embargo, dice la autora, se trataba más de anécdotas de casos específicos que de información soportada en la evidencia. Menciona cómo entre los respondientes se mantenía la percepción de que la biometría era capaz de evitar el fraude en la distribución de la ayuda humanitaria, pero no se la pensaba como tecnología para controlar el riesgo de fraude a nivel interno de la organización. Es decir, los promotores de estas tecnologías despliegan sistemas de reconocimiento biométrico bajo la idea de que el beneficiario es el único con la capacidad de engañar "el sistema", y trasladan a este no solo el deber de probar, en sacrificio de su privacidad, que es quién en efecto dice ser, sino el deber de demostrar que es quien dice ser a pesar de que el sistema señala, por algún error técnico, otra cosa.

Según Rahman (2018), sin evidencia sobre cómo impacta el fraude a la destinación eficiente de la ayuda humanitaria a personas que lo necesitan, antes del aterrizaje de la biometría como después de su puesta en marcha en escenarios de este tipo, es difícil medir no solo la efectividad de la medida propuesta, sino la adecuación de la misma para resolver, el que se dice, es el problema que justifica su funcionamiento.

Slavin, Putz y Korkmaz (2021) elevan además la pregunta sobre el balance de costos asociados a este tipo de tecnologías. En su informe sobre el despliegue de tecnologías de identificación digital en la acción humanitaria recuerdan que, en el acceso limitado a medios de financiación de organizaciones humanitarias, la adopción de tecnologías de este tipo (su manutención, soporte y capacidades requeridas para su uso) puede requerir una inversión mucho mayor en comparación con los recursos desperdiciados por eventos de fraude. Situación por la cual recomiendan apoyarse en la filantropía y capacidad económica de los actores públicos para llevar a cabo su puesta en marcha de manera sostenible, sin acoger en todo caso una visión crítica como la de Rahman (Slavin *et al.*, 2021). En el mismo

(2016: 2)–, y que fueron explotados de manera intensiva por actores humanitarios y del sector privado supuestamente para llevar a cabo actividades de rastreo digital del contacto entre las personas a partir de su ubicación obtenida por la señal de sus teléfonos móviles. Explotación infructuosa pues no permitió conseguir el objetivo propuesto en sacrificio de aspectos como el consentimiento y privacidad de las personas, pues dice el autor, no se desplegaron medidas apropiadas ni se fijaron estándares que orientaran sobre el cuidado en la protección de los datos de estas pese a que dichos actores colaboraron de manera conjunta con los Estados.

sentido, Willits-King, Bryant y Holloway (2019) sostienen "there has been no publicly available effort to compare the cost to organisations of establishing and operating biometrics systems with the cost of fraud."

Por otro lado, la inquietud sobre los costos es también una de las personas refugiadas, impactadas por dicho sistema. Madinou en su proceso de entrevistas cuenta que "[o]ne of my interviewees wondered if identifying a proportionately small number of 'two-timers', justified the enormous investment in biometric technologies" (2019: 21), de manera que la pregunta sobre la proporcionalidad y los costos no es una sola que gira en torno al aspecto financiero, mucho menos gira en torno a un solo actor.

Jacobsen y Sandvik, así como Madianou, van mucho más allá y sostienen que la narrativa de la prevención del fraude, así como la necesidad de identificar a las personas refugiadas que no cuentan con medios para probar que son quienes dicen ser, es mucho más reciente. Es más, que aterrizó al menos 10 años después de que los primeros sistemas de identificación biométrica de personas refugiadas estuvieran en marcha, en los casos particulares de actores como ACNUR y el Programa Mundial de Alimentos.

Así, para 2002 ACNUR puso en funcionamiento su sistema de reconocimiento biométrico al repatriar personas desde Pakistán a Afganistán, en 2003 y en 2006 lo hizo en campos de refugiados en Tanzania y Malasia respectivamente, en 2007 desplegó la más extensa campaña de registro biométrico en Pakistán en colaboración con el gobierno de ese país. Entre 2005 y 2009 lo desplegó en los campos de refugiados de Dadaab y Kakuma en Kenia. Para 2007 su sistema de reconocimiento biométrico proGres (que luego se transformaría en BIMS y más recientemente en PRIMES), ya operaba en más de 51 países y tenía los datos sensibles y personales de más de 2.5 millones de personas (Duffield, 2016b; Gelb y Krishnan, 2018; Jacobsen, 2015; Jacobsen y Sandvik, 2018; Madianou, 2019).

Tanto Jacobsen y Sandvik (2018) como Madianou (2019) refieren que solo hasta 2010 ACNUR adoptó su política de biometría para los procesos de registro y verificación de las personas refugiadas que declara que la biometría provee mecanismos de identificación confiable previniendo el fraude, falsas solicitudes de ayuda y robo de la identidad. Antes de esa época, las autoras apuntan a otras razones que parecen haber justificado el despliegue de dicho sistema: la de aumentar la rendición de cuentas ante los donantes (Jacobsen y Sandvick) y la creciente securitización de los procesos de protección internacional de personas refugiadas (Madianou).

Sandvik (2016) en su texto *How accountability technologies shape international protection: results-based management and rights-based approaches revisited,* rastrea el cambio de visión de ACNUR en los procesos de protección internacional de las personas refugiadas que empieza a emplear el lenguaje de la eficiencia y la efectividad ante la amenaza de reducción de su presupuesto por los Estados donantes que en la década de los 90 venían insistiendo en problemas asociados a su capacidad de rendición de cuentas. Amenaza que hizo a dicha agencia tornar la mirada hacia mecanismos que permitieran medir la generación de sus resultados a través de estadísticas e indicadores. Las tecnologías digitales aparecen en escena con

la promesa de contar personas para facilitar la transparencia hacia los donantes, situación que significó desde entonces una distorsión de la rendición de cuentas donde la agencia se removió a sí misma de la ecuación de la responsabilidad bajo la lógica de que, si la que cuenta los resultados es la máquina, y la máquina no se equivoca, lo que esta dice es lo que es, y punto (Sandvik, 2016).

Katja Jacobsen (2016) continúa la misma línea de razonamiento trazada por Sandvik. Respalda el argumento sobre el nacimiento de las tecnologías digitales como respuesta para resolver problemas de responsabilidad ascendente, ante la presión creciente de los donantes que acusaban a la agencia de la ONU de estar inflando los números de personas beneficiarias de sus programas, y de su incapacidad de dar cuenta sobre en qué y en quiénes se estaban invirtiendo los recursos. Dicha autora señala que fueron los propios Estados donantes los que promovieron el vínculo entre biometría-rendición de cuentas. La autora al respecto cita un informe del Departamento de Estado de los Estados Unidos que urgía en 2004 a ACNUR a "hacer todo lo que pudiera" para implementar sistemas de biometría para identificar apropiadamente a las personas beneficiarias de sus programas, todo para que esta tuviera mejores números sobre cuánta ayuda se requería y a quiénes había que destinarla.

La biometría aparece en escena "[b]ecause biometric characteristics are unique to every individual, the same individual cannot be registered twice and, thus, inflated numbers as a result of double-registration can be minimized" (Jacobsen, 2016: 164). Una vez desplegada, la biometría no solo permite tener información sobre cuántas personas necesitan la ayuda que dicen precisar, sino que ayuda a disminuir la preocupación de los donantes en torno al supuesto gasto desmesurado:

> concerns about inflated refugee population figures appear to have lessened; donors are presented with results so they can see how since the introduction of biometrics, 'the numbers of people receiving assistance from the GFD [General Food Distribution] has dropped significantly (Jacobsen, 2016: 164-165).

Luego de que ACNUR presentara oficialmente su política en 2010, la ocurrencia del 11 de septiembre de 2001 obró como una suerte de gasolina a la narrativa de la identificación, pues dicho evento apuntó nuevamente las acusaciones a dicha agencia de estar beneficiando a terroristas en lugar de verdaderas personas en necesidad. Por tal motivo, era preciso saber en adelante cuántas personas recibían asistencia humanitaria pero, sobre todo, *quiénes eran* esas personas. La biometría fue desde entonces la tecnología digital ideal, capaz de responder a ambas preguntas (Jacobsen, 2016). Luego, como si se tratara de una bola de nieve, la influencia ejercida por los Estados donantes sobre ACNUR y, de este actor sobre otros del ecosistema de protección internacional a las personas refugiadas, se ha apoyado en la última década en la narrativa de la identificación, no como verdadera razón de despliegue, sino como una de masificación en su uso por lo que "it becomes apparent that 'digital identity' policies aren't about refugees after all" (Madianou, 2019: 24).

Madianou apunta por su cuenta, a cinco razones estructurales que han justificado el despliegue de los sistemas de identificación biométrica en actores como

ACNUR y el Programa Mundial de Alimentos. La lógica de la responsabilidad, de la auditoría, del capitalismo, del solucionismo y de la securitización. Las lógicas de la responsabilidad y la auditoría surgen como reacción a los cuestionamientos sobre responsabilidad ascendente y la efectividad de la intervención humanitaria, profundizadas por la reciente mercantilización que ha ido significando la participación del sector privado en la acción humanitaria destinada a la atención y ayuda de personas refugiadas. Es decir, retoma la propuesta de Sandvick (2016) y Jacobsen (2016). Sin embargo, advierte que hay ciertas lógicas que prevalecen por encima de otras: la del solucionismo y la securitización que, combinadas con la lógica del capitalismo, han convertido del despliegue de sistemas de biometría en una práctica de experimentación sobre las poblaciones más vulnerables (Madianou, 2019).

La lógica del solucionismo, en un sentido similar al que advertimos en el primer capítulo, se refiere al deseo de resolver problemas sociales complejos a partir del despliegue y uso de las tecnologías digitales. La complejidad de los escenarios humanitarios no torna menos intenso ese deseo, sobre todo de cara a los problemas de sostenibilidad de las acciones de ayuda y socorro a poblaciones de personas refugiadas que cada vez más va en aumento (Madianou, 2019).

Así, el deseo de hallar soluciones de múltiple tipo, para problemas de naturaleza diversa, se encierra bajo una mirada reduccionista de la realidad en el que los actores del sector privado promueven sus productos y servicios con la promesa de hallar una sola respuesta que dice ser infalible, inequívoca y efectiva (Madianou, 2019).

La lógica del capitalismo se refiere a la participación cada vez más abierta e intensa de compañías del sector privado que, como vimos en el cuadro de beneficios de este, encuentra en el sector humanitario un atractivo sin igual: el de la experimentación sin riesgo a ser responsables, y de acceso a grandes cantidades de datos personales sin guardián a la vista (Madianou, 2019). Y finalmente, la lógica de la securitización, que recuerda cómo la presión inicial por desplegar sistemas de identificación biométrica encontró su momento más intenso en la lucha contra el terrorismo global impulsado por Estados Unidos luego del 11 de septiembre. La autora advierte que la lógica de la securitización se asocia, en el fondo, a las finalidades de control, expulsión y rechazo en materia migratoria, así como a la vigilancia de las poblaciones en procesos de movilidad humana (Madianou, 2019).

Entonces, actores humanitarios–con un énfasis en los de naturaleza no estatal–, mantienen interés en el despliegue de tecnologías digitales para saber quién es la persona que se beneficia de sus programas, es decir, identificar de manera uniforme, sea que haya perdido o no sus papeles. Y al identificarla a partir de sus características biológicas únicas facilitar de manera verificable, auténtica y transparente, la asignación de la ayuda humanitaria requerida.

Sin embargo, las autoras vistas hasta ahora señalan que, pese a la narrativa de la identidad digital y el fin de la prevención y evitación del fraude, esta no se asocia a las razones reales que sostienen los orígenes fundacionales de estos sistemas. La narrativa de la responsabilidad ascendente y la rendición de cuentas ante los Estados donantes que exigen saber a quiénes se destina la ayuda, y quién es en

concreto la persona que se beneficia de esta, es la que ha motivado desde el inicio de siglo la existencia de los sistemas de identificación biométrica en la acción humanitaria.

Veamos ahora los riesgos e intereses que se asocian a las personas refugiadas para seguir llevando el balance de intereses en juego que, como dijimos al inicio de este capítulo, mantienen el despliegue de tecnologías de identificación biométrica pese a los riesgos en protección de datos que fueron advertidos en el segundo capítulo.

Tabla 5. Identificación de riesgos e intereses de las personas refugiadas

Actores / Criterios	Personas refugiadas
Composición	Personas que huyen de su Estado o lugar de origen y se trasladan a otro en busca de ser reconocidas bajo medidas de protección que les permitan rehacer sus vidas
Intereses y beneficios	Recibir la identificación que les condiciona conseguir bienes y servicios
Riesgos	Afectación capacidad de conseguir bienes o servicios por indebida clasificación de los sistemas de ID digital
	Afectación al derecho a la protección de datos (vistos en detalle en el capítulo segundo)
	Ausencia de confianza en otros actores involucrados en ID digital
	Sesgos burocráticos que impiden despliegue de sistemas de ID justos y, al tiempo, tecnologías de ID digital pueden agravar sesgos burocráticos
	Vigilancia masiva de personas de lugar de origen, pero también de destino
	Evadir activamente sistemas de ID digital si sienten que están siendo rastreados, a veces incluso a expensas de no recibir un servicio
	Tecnologías en la jornada y el manejo de la migración pueden ocasionar efectos de la "paradoja de la distancia", afectando la humanización del proceso de huida
	Ansiedad en torno al decomiso de sus teléfonos móviles y vigilancia de sus actividades en línea, así como la entrega forzosa de las contraseñas de sus redes sociales para que su identidad y nacionalidad sea verificada
	Falsos positivos o falsos negativos en los procesos de identificación y autenticación soportados en biometría
	Discriminación o sesgos en la tecnología contra personas de tez oscura, personas con discapacidad, personas con huellas desgastadas por labores manuales, entre otros.
	Function creep de los sistemas de biometría
	Que no haya conectividad en el lugar en el que se hacen los procesos de identificación biométrica
	Condiciones climáticas complejas que dificulten funcionamiento de la tecnología biométrica (calor, polvo, humedad)
	En ambientes urbanos la tecnología biométrica puede limitar la movilidad de las personas refugiadas

Fuente: Elaboración propia.

Así como lo hicimos de cara a los actores humanitarios, los riesgos para las personas refugiadas pueden agruparse así: en (i) los riesgos de la tecnología, como su avería o no funcionamiento por condiciones climáticas, ambientales, de brecha digital, los sesgos producto del diseño y funcionamiento de la tecnología, o su uso y despliegue hacia fines distintos de los originalmente advertidos o *function creep*;

y (ii) los riesgos directos e indirectos que causa la intermediación tecnológica en la acción humanitaria.

Los riesgos directos, como la negativa de acceso a la ayuda humanitaria por falsos positivos y negativos, los de vigilancia de las actividades de las personas refugiadas, los de discriminación, los de impacto en la protección de sus datos, etc.; y los riesgos indirectos, como los de tecnologización de la burocracia, y los de ocurrencia de la "paradoja de la distancia" en donde cada vez más tecnologías y menos personas se involucran en el proceso de atención a las personas refugiadas. Sobre algunos de estos riesgos la literatura ya ha advertido casos reales. Por ejemplo, en 2013, en Mauritania, se reportaron al menos 6,500 casos de personas refugiadas a las que les fue negado el acceso a la ayuda humanitaria de ACNUR, debido a un error que fue detectado en el sistema de registro biométrico (Kaurin, 2019). En el registro de personas afganas en 2002, ACNUR rechazó hasta 390.000 entre los meses de marzo y octubre, de un total de 1.8 millones de personas registradas. De aquellas a las que se negó el acceso a la ayuda se estima que al menos 11.800 personas pudieron haber sido incluidas como *two-timers* como producto de falsos positivos inadvertidos en el sistema (Madianou, 2019).

Los falsos positivos pueden, además, tener un impacto mucho más profundo cuando, por ejemplo, no se los considera como un problema tecnológico sino de la persona. Así, el informe de auditoría de 2017 del sistema biométrico del Programa Mundial de Alimentos, expresó que las estimaciones sobre el porcentaje de error del sistema habían sido omitidas, es más, que no se consideraba a la ocurrencia de falsos positivos como un problema del desempeño del sistema que afecta su eficiencia o efectividad (Office of the Inspector General, 2017).

Madianou recuerda que los sesgos, un riesgo en torno al funcionamiento de los sistemas de identificación biométrica, han sido harto documentados. No solo hay partes del cuerpo más difícilmente legibles, como las huellas digitales de personas de la tercera edad, las mujeres afrodescendientes, latinas y asiáticas. También hay segmentos poblacionales que directamente no son legibles por el sistema o su legibilidad lleva directamente a errores de identificación, entre los que se incluyen los trabajadores de labores manuales o los del sector del cuidado, la salud o la belleza que tienen crestas dactilares borradas por la labor manual que desempeñan o producto de la interacción con agentes químicos (2019).

La autora señala que los sistemas biométricos de reconocimiento facial no escapan a los cuestionamientos por sesgos basados en el género, sexo o raza de la persona. Al respecto señala que "[d]espite the assumption that biometrics are impartial and scientific, biometric data codify existing forms of discrimination while the discourse of science masks racist, sexist and classist practices" (Madianou, 2019: 16).

Incluso, hay eventos en que los riesgos de la tecnología pueden afectar a la totalidad de un grupo de personas, más allá de la persona afectada. Así sucedió en Kenia, donde la interrupción y demoras en el proceso de registro biométrico de personas llevó a la cancelación de la distribución de alimentos (Jacobsen, 2016). Los riesgos en materia de brecha digital son igualmente latentes. Así, por ejemplo, en el informe de auditoría al sistema de registro biométrico del Programa Mundial de Alimentos de 2017, se advirtió cómo había personas beneficiarias

que aun no habían sido registradas en el sistema debido a problemas de conectividad (Office of the Inspector General, 2017). En el informe de auditoría del sistema biométrico de ACNUR se describe cómo en la India los tiempos de registro biométrico de las personas era mayor por problemas asociados a la fluctuación del servicio de internet (Office of Internal Oversight Services, 2016).

En su texto *The humanitarian divide*, Willits-King, Bryant y Holloway (2019) apuntan que, pese a la expectativa de que las tecnologías digitales automáticamente son generadoras de inclusión, la brecha digital aunada a la de género, geográfica, económica y etaria en los contextos humanitarios, dificulta la realización de la promesa asociada a su despliegue. El riesgo de utilización de estos sistemas para fines distintos de los inicialmente advertidos, sea de manera intencionada o no, persiste no solo por las lógicas que subyacen al despliegue de estos y que se orientan, entre otros, en la securitización de la movilidad humana (Jacobsen, 2015; Madianou, 2019), sino por la ausencia de consenso sobre el listado cada vez más creciente de las actividades humanitarias que precisan del registro biométrico de la persona para condicionar la entrega de una ayuda o beneficio (Office of the Inspector General, 2017).

De hecho, eventos imprevistos que derivan en usos no advertidos de sistemas de este tipo, están teniendo lugar ahora mismo en Afganistán. Según *Reuters* y *The Intercept*, la toma del poder por los Talibán significó, entre otras cosas, la incautación por estos de los sistemas de registro biométrico que habían sido desplegados por el Ejército de los Estados Unidos y se teme que lo mismo suceda con los de las agencias de ayuda humanitaria presentes en ese país (Chandran, 2021; Klippenstein y Sirota, 2021).

No solo se trata de la retención de la tecnología sino del acceso a las bases de datos con las que estas se conectan. Los usos para los que serán destinados, según se advierte, apuntan a la verificación de la identidad de las personas para rastrear y perseguir a defensores de derechos humanos, agentes humanitarios, miembros del antiguo gobierno, entre otros (Chandran, 2021; Klippenstein y Sirota, 2021). Un riesgo adicional que la situación en Afganistán pone de presente, es la imposibilidad que tienen las personas ante eventos de este tipo, de llevar a cabo acciones de borrado de su huella digital cuando se trata de sus datos biométricos. Una vez se crea una base de datos con registros biométricos de las personas, la posibilidad de evadirlos se reduce en tanto que la existencia de dicha información implica la rastreabilidad prolongada de la persona, al menos hasta tanto conserve la característica biológica registrada –la huella, el iris, el rostro– (Chandran, 2021).

Jacobsen junto a Steinacker (2021) reflexionan, de hecho, sobre las lecciones que debe dejar para las agencias de la ONU para los refugiados, como ACNUR, el evento reciente de apropiación de los sistemas biométricos y bases de datos de agencias humanitarias y militares por parte de los Talibán. La respuesta, según los autores, debiera ser la de conducir a su eliminación y borrado de la información biométrica en manos de dicho actor, así como a la suspensión de los sistemas de registro biométrico a los que las personas refugiadas no solo no han consentido, sino cuyos usos para propósitos y tiempos más allá de lo prometido, significan hoy un riesgo para la vida de al menos 4 millones de personas registradas.

Sin embargo, formas más comunes en que el riesgo de *function creep* se materializa en la práctica tienen que ver con los accesos que tienen Estados y, en general, terceras partes no autorizadas para usar su información personal para fines distintos a los que justificaron su recolección (Willits *et al*., 2019).

Sobre los riesgos directos, ya hemos aproximado a lo largo de este texto algunas ideas. Quizá valga la pena añadir, sobre el riesgo de vigilancia de las personas, el caso al que refiere Pierrick Devidal sobre cómo las transferencias monetarias que se apoyan en la autenticación biométrica como "forma de pago" facilitan su ocurrencia. Señala que, sin medidas de seguridad debidamente implementadas, las alianzas entre actores humanitarios y terceros, como compañías tecnológicas y grandes bancos, que operan bajo regímenes legales de alcance dispar, permite el flujo libre de los datos sensibles de las personas que se benefician de esta modalidad de ayuda y cuya información es empleada en contradicción a los estándares aceptados en materia de protección de datos, lo que pone en duda la independencia operacional de los agentes humanitarios y los principios de la acción humanitaria (Devidal, 2021).

La vigilancia se concreta cuando rastrear, monitorear o prevenir el fraude se convierte en una necesidad para los actores que despliegan este tipo de sistemas, sin garantías para que las personas puedan cuestionar su vigencia (Devidal, 2021). Sobre los riesgos indirectos, algunos autores ponen de presente el de tecnologización de la burocracia, es decir, el traslado de procesos e instancias administrativas soportadas en la tecnología y cuyo uso dota a estos últimos de una suerte de aire de eficiencia pese a que, en verdad, no lo tengan (Jacobsen, 2015, 2017; Jacobsen y Sandvik, 2018). Ello constituye un riesgo para la persona refugiada, en tanto que dicha relación se afirma en la narrativa de la presunta neutralidad e indemnidad que trae consigo el uso de las tecnologías digitales, lo que torna a la tecnología y al proceso burocrático en condiciones irrebatibles o incuestionables.

Autores como Read, Taithe y Ginty (2016) añaden, en lo que denominamos riesgos, indirectos, el de la paradoja de la distancia. Según estos, el despliegue de tecnologías para hacer más eficiente la acción humanitaria, desplaza el contacto humano por la facilidad que ofrecen sistemas como los biométricos para llevar a cabo su administración o manejo de manera remota. Duffield, en el mismo sentido apunta que "[r]emoteness is inseparable from the increasing sophistication of the global North's atmospheric ability to digitally rediscover, remap and importantly, govern a new a now distant South" (2016b: 149).

Entonces, la privacidad no es un riesgo aislado ni comparativamente superior a otros que concurren para las personas refugiadas. El balance de riesgos, hasta ahora, es mucho mayor para las personas refugiadas si se tiene en cuenta que ninguno fue advertido para los del sector privado y tan solo algunos para los actores humanitarios. Afirmar que las personas refugiadas se encuentran en el extremo más débil no es baladí.

Resulta llamativo cómo una vez más los errores o fallos de la tecnología, no alcanzan a los actores del sector privado que los diseñan y fabrican. Recaen de manera intensa en las personas refugiadas en sus efectos más crudos, como la negativa de acceder a la ayuda solicitada, por ejemplo, con el peso adicional que significa la supuesta infalibilidad de la tecnología que revierte la carga de probar

el error en hombros de la persona afectada, y no del actor que lo despliegue, impulsa o promueve.

Los actores humanitarios, en comparación con las personas refugiadas, apenas si pueden llegar a experimentar riesgos en "carne propia", pues los riesgos más significativos o bien recaen sobre la tecnología (condiciones climáticas, técnicas, de brecha digital) o sobre entidades más abstractas como los principios de la acción humanitaria. Los riesgos organizacionales de tipo interno/externo apuntan a aspectos de reputación, de desviación del dinero, pero no orbitan en torno a la posibilidad de llegar a ser responsables frente a las personas beneficiarias de sus operaciones. Sin el riesgo de la responsabilidad hacia los beneficiarios –responsabilidad descendente– no hay incentivos que justifiquen el despliegue de medidas de cuidado hacia, por ejemplo, la privacidad de las personas refugiadas (Kaurin, 2019).

2. Cuál es la promesa que sigue empujando el despliegue de las tecnologías digitales a la acción humanitaria

Ahora, es llamativo el texto *From digital promise to frontline practice: new and emerging technologies in humanitarian action* publicado recientemente por la Oficina para la Coordinación de Asuntos Humanitarios OCHA, porque apunta en dirección a la promesa más importante de las tecnologías digitales en los escenarios humanitarios.

Se trata de un informe que evalúa los beneficios y desventajas de diversas tecnologías, no solo la biométrica, y apunta a los requerimientos que deben ser puestos en marcha para sacar a cada una el mayor provecho. Y afirma la narrativa de la innovación así "[n]ew and emerging technologies can support this paradigm shift from reaction to anticipation by enabling earlier, faster and potentially more effective humanitarian action" (Arendt-Cassetta, 2021: 2). Se trata de una afirmación que pone de presente la última promesa que va más allá de la efectividad, la eficiencia, la prevención del fraude, incluso de la identificación: la predicción. Es decir, poder anticiparse a las crisis humanitarias para cuidar mejor el gasto, en tanto que las crisis cada vez son mayores y más extendidas, y el financiamiento cada vez más escaso. Sostiene dicho texto, en palabras del Subsecretario General de la Coordinación de Asuntos Humanitarios y Alivio de Emergencias, que

> It would be nice to think we can fill the gap just by raising more money. But we can't. We also have to make the money we have go further. The best way to do that is to change our current system from one that reacts, to one that anticipates (Arendt-Cassetta, 2021: 01).

Predicción, que, según el informe, es posible a través del despliegue de tecnologías digitales de diverso tipo, desde la inteligencia artificial, la biometría, los vehículos aéreos autónomos (drones), así como la biometría, el internet de las cosas, el blockchain, las aplicaciones móviles y las redes sociales, entre otras (Arendt-Cassetta, 2021).

Para el logro de la promesa de la predicción, el informe propone apuntar, por ejemplo, al empoderamiento de las comunidades a través de su inclusión que implica, de manera prioritaria, el cierre de la brecha digital. Brecha que el informe enfoca

principalmente en la cuestión del acceso a internet, dejando de lado otras aristas que tienen que ver con la brecha en su uso, las habilidades para emplearlas, y la cuestión motivacional del acceso (J. A. G. M. van Dijk, 2005; J. van Dijk y Hacker, 2003).

También, a la necesidad de adoptar una mirada de diseño centrado en el usuario; a la mejora de las políticas y principios en materia de protección de datos, así como la capacidad y habilidades para analizarlos; al aumento de la colaboración y coordinación en las alianzas público privadas; a la aplicación de los derechos humanos en las actividades en línea y que se apoyan en el uso de las tecnologías digitales; y a la inversión y escalamiento de las soluciones tecnológicas que deben poder tener una vocación de largo plazo en que se analice su impacto, entre otros (Arendt-Cassetta, 2021).

Al dejar de lado las posibles críticas formuladas, como la amplitud con la que se revisa cada tecnología digital sugerida, la promesa de la predicción ¿qué es en términos concretos y para qué se quiere? , ¿para llegar más temprano al sitio de la emergencia?, ¿para prevenir su ocurrencia?, ¿para determinar quienes pueden llegar a "repetir" como refugiados para decidir sobre su inclusión/exclusión del sistema?, ¿para determinar qué lugares precisarán del despliegue de ayuda humanitaria y con ella, de sistemas de identificación y registro de personas refugiadas? Como sea, vale la pena mirar de cerca a la promesa de la predicción.

Sin intención de exhaustividad, hay que decir que la predicción es una promesa con tradición en distintas áreas, como la salud, el comercio, en materia de predicción del crimen, entre otros. Al respecto vale la pena rescatar algunas críticas que han sido formuladas por algunos autores entre la vasta literatura que ha estudiado de cerca ese tema, enfocándonos en la que apunta a lo que sucede en la predicción del crimen. Así, podríamos decir que, tanto en la predicción del crimen como en la predicción de las crisis humanitarias existe, en apariencia, una misma urgencia: la de saber el quién y el dónde. ¿Quién es propenso a delinquir nuevamente? ¿Quién es propenso a acudir a la ayuda humanitaria –por primera vez o como *recycler*–? ¿Dónde habrá de ocurrir un delito, una crisis o una emergencia? Nuevamente, podríamos decir que se trata superficialmente de objetivos compartidos, realizables a través de la capacidad predictiva de la tecnología.

La promesa de la predicción, según Sandra Mayson (2018), es aquella en donde, en ausencia de intervención de variables ajenas a una determinada historia, la misma habrá de repetirse. La predicción es producto de la identificación de patrones pasados para ofrecer proyecciones de eventos futuros. No importa, dice la autora, el nombre o tipo de algoritmo que se emplee, la disparidad de los datos significa también una disparidad en la predicción, por lo que su potencial es, a lo mucho, el de un espejo que proyecta el pasado como guía para el futuro, con todo lo que ello implica.

Los datos, en materia de predicción, son un insumo clave. Más allá de la discusión sobre su calidad, exactitud o actualización, los sistemas de predicción en materia del crimen, en su mayoría proveídos por el sector de las *Big Tech*, operan de manera opaca o poco transparente, no advierten, en ocasiones, qué tipo de datos están siendo procesados, cuál es su origen y si involucra el tratamiento de datos personales y sensibles o no (Richardson *et al.*, 2019).

A pesar de la supuesta objetividad con que se cree que funcionan los sistemas de predicción del crimen, las prácticas de obtención de los datos y su procesamiento por estos, se encuentran embebidos en sesgos de múltiple tipo: políticos, sociales, raciales, entre otros. En palabras de Egbert y Leese "predictive policing software perceives the world exclusively on the basis of the data it is presented with. Even a 'perfect' algorithm –if there was such a thing– would produce biased results based on biased data". Sesgos que se encuentran ocultos, son agravados o pasan inadvertidos por la "racionalidad del sistema"(2021: 395).

Pero más importante aún, se trata de tecnologías digitales que, a pesar de su despliegue en el mercado por más de una década, siguen sin ser reguladas en países como Estados Unidos, donde tiene presencia en más de trece jurisdicciones. Desde entonces y hasta ahora, siguen siendo cajas negras ajenas al escrutinio, la rendición de cuentas o el alcance regulatorio de los Estados, salvo algunos casos concretos de litigio (Brayne, 2021; Mayson, 2018; Richardson *et al.*, 2019).

Las críticas también apuntan a las preocupaciones desatendidas en materia de privacidad y protección de datos. Brayne, en su texto sobre predicción aplicada a la prevención del crimen, entrevista a varios oficiales de policía y civiles que trabajan en estaciones de policía donde funcionan este tipo de tecnologías. En ellas se leen preocupaciones en torno a cuán invasivos son los datos que se recogen por estos para introducir en el sistema, entre estos muchos datos innecesarios o datos personales que fueron recabados con otros propósitos y que terminan alimentando. Uno de sus entrevistados habló de un supuesto "mantra" de los departamentos de policía que usan sistemas de predicción: "collect now; analyze later". Según la autora, se trata de una práctica común en torno a este tipo de sistemas aplicados a tareas sensibles que involucran la detención de una persona, el despliegue de cuerpos de policía a ciertas zonas o barrios, etc (Brayne, 2021: 194).

De hecho, es interesante ver cómo Brayne da cuenta en su texto (2021), *Predict and Surveil,* de la intensificación de los problemas en torno a la privacidad cuando los mismos sistemas de predicción son trasladados a la medición de la productividad laboral de los agentes civiles y de la policía. Preocupaciones sobre el origen de los datos, el tiempo de su almacenamiento, pero especialmente, los de su asociación a razones de equidad. Los entrevistados apuntaron a cuestionar por qué la productividad debía estar basada en datos de desempeño viejos, a cómo estos sistemas reforzaban bajo la "neutralidad" de su funcionamiento, prácticas de vigilancia y sospecha sobre la persona que debía rendir cuentas sobre sus actividades y paradero, etc.

Esta situación ¿no sería igualmente extensible al contexto humanitario?, ¿dicha sospecha no pesaría sobre la persona humanitaria?, ¿preocupaciones similares sobre la privacidad no serían advertidas allí? Al menos así debe poder sugerir la aplicación del principio de precaución según el cual, ante la incertidumbre sobre el funcionamiento de sistemas con la misma racionalidad y vocación, habría (i) que poder presumir la ocurrencia de los mismos riesgos, hasta que indicadores y evidencia suficiente puedan probar que su efectividad no solo es posible sino que en el medio no se sacrifican los principios de la acción humanitaria y claro, los derechos de las personas; y (ii) delegar en alguien (¿quién?) la carga costosa tanto

de prevención de los riesgos inciertos que vienen aparejados al despliegue, como de generación de evidencia sobre su impacto.

Así, la promesa predictiva que habrá de extenderse a la acción humanitaria precisa un seguimiento de cerca, una mirada igualmente crítica no solo de cómo impactaría en la privacidad de las personas refugiadas, en sus costos y beneficios, pero especialmente en cómo su funcionamiento podría terminar de ensamblar estereotipos negativos en contra de las personas en contextos de movilidad humana, impactando en la manera en cómo estas ejercen sus derechos en situaciones de vulnerabilidad y desigualdad en la que son la parte más débil de las relaciones de poder.

***

Al inicio advertimos dos preguntas que habrían de orientar este capítulo. La primera sobre los riesgos y beneficios que reportan las tecnologías digitales en la acción humanitaria para el sector privado, los actores humanitarios –especialmente los no estatales–, y las personas refugiadas sobre los riesgos enfocados en la protección de sus datos. Y la segunda, sobre cuál es la promesa que, pese a los riesgos advertidos, sigue llevando adelante la puesta en marcha de las tecnologías digitales en dicho escenario.

En torno a la primera pregunta, abordamos los riesgos y ventajas, en su orden, del sector privado, actores humanitarios y personas refugiadas. Sobre el sector privado se expuso de entrada que el listado de beneficios era extenso mientras que la literatura no advertía para este ningún riesgo. Consideración que podía deberse, en todo caso, a que se trata de un sector representado por grandes compañías que al tiempo que acaparan la economía digital se encuentran lejos del alcance regulatorio de los Estados, incluyendo la aplicación de los derechos humanos. Vimos cómo el aterrizaje de dicho sector a la acción humanitaria se hizo posible a través de la narrativa de la innovación, aparejada a promesas sobre la efectividad y la eficiencia de los procesos, y atractiva a los actores humanitarios que se enfrentan a la disminución progresiva de sus recursos al tiempo que la demanda de la ayuda crece año a año.

La narrativa de la innovación, que ha sido vendida bajo el eslogan del *Data for Good* o *Data for Social Good*, según vimos, es favorable al despliegue de tecnologías de experimentación en contextos social y regulatoriamente frágiles. Es un discurso con una mirada triunfante de la tecnología que se enfoca en sus ventajas y que desconecta a sus promotores de las necesidades de las personas.

Vimos también que, la llegada de estos actores a la acción humanitaria, reporta al menos dos grandes beneficios para las *Big Tech*: la posibilidad de acceder a grandes cantidades de datos sin guardián a la vista y desplegar tecnologías bajo prueba sin la obligación de rendir cuentas; y al hacerlo, de beneficiarse de los regímenes de inmunidad legal que se extiende a estos por trabajar junto a los actores humanitarios. Luego hicimos un balance de riesgos y beneficios para los actores humanitarios según lo sugerido por la literatura revisada. Allí, el interés común de los actores no estatales de este tipo se orientó en la necesidad de identificación de las personas refugiadas que viajan sin papeles o que los han perdido

en el proceso, así como en la necesidad de llevar a cabo el uso de tecnologías digitales de identificación para la asignación de la ayuda, evitar casos de fraude y suplantación de la identidad para su recepción.

Sin embargo, revisamos literatura que cuestionó la validez de dicha promesa que no solo no se encuentra validada por la evidencia, sino que es temporalmente inconsistente con el período inicial de puesta en marcha de los sistemas de identificación biométrica –la tecnología a la que mayor referencia hizo la literatura en relación con la atención a personas refugiadas–.

La verdadera razón por la que se empezó a desplegar la biometría en el escenario humanitario, fue la de introducir mecanismos que permitieran rendir cuentas a los financiadores debido a los cuestionamientos sobre la incapacidad de algunas agencias dedicadas a la atención de personas refugiadas para transparentar cuánto y en quién se estaba destinando el gasto.

Al tiempo, la asociación entre biometría-rendición de cuentas fue promovida desde los mismos Estados, interesados en las tecnologías de identificación para facilitar sus actividades de control migratorio. Y así, a manera de bola de nieve, los grandes actores humanitarios para la atención de personas refugiadas, presionaron a otros en dicho ecosistema para adoptar tecnologías del mismo tipo. En 2002 se desplegó el primer sistema biométrico para la atención de personas refugiadas y solo hasta 2010 surgió la narrativa de la identificación que obró desde entonces y hasta ahora, no como motivo de despliegue, sino de masificación en su uso.

Así, las tecnologías digitales capaces de dar cuenta de cuánto y en quién –con nombre y apellido– se invierte la ayuda humanitaria, fortalecen, según los actores humanitarios, a los financiadores, es decir, favoreciendo la rendición ascendente de cuentas. La literatura, además, agrega que ello en apariencia es así, en desmedro en todo caso de la rendición de cuentas descendente, es decir, dirigida a las personas beneficiarias.

Luego nos detuvimos en el listado de riesgos y vimos que para este actor no se incluye el de ser responsable o *be held accountable* ante las personas beneficiarias, por lo que es esperable que, en ausencia de dicho riesgo, los mecanismos de autorregulación, de haberlos, no sean puestos en marcha. La responsabilidad como riesgo es, ante todo, un incentivo que debería motivar hacia el despliegue de mecanismos de protección. Este no es el caso para los actores humanitarios, mucho menos para los del sector privado.

Y finalmente, los riesgos y beneficios para la persona refugiada. Riesgos que son múltiples, y beneficios que, por el contrario, escasean. Es más, el único supuesto beneficio de recibir identificación para conseguir bienes y servicios en escenarios de ayuda humanitaria, no es sino producto de la necesidad que introdujo en ese contexto el despliegue de la biometría que condiciona el acceso a la entrega previa de los datos biométricos de la persona. El listado de riesgos es múltiple, comprenden los que se derivan de la tecnología, y los que causa la intermediación tecnológica en la atención humanitaria. No son de mejor calado en comparación con los advertidos en materia de privacidad. Sin embargo, son las personas refugiadas a diferencia de los otros dos actores los que cargan el peso del fallo de las tecnologías digitales, así como los que derivan de la intermediación tecnológica.

A diferencia de los casos del sector privado y los actores humanitarios, los eventos de falsos positivos (riesgos de la tecnología) en los que se identifica a una persona de manera errónea como *two timer* o suplantadora, no son riesgos para ninguno de estos dos actores más fuertes. Incluso, pueden no ser percibidos como un fallo endosable a la tecnología sino exclusivamente a la persona. Situación que revierte la carga de la prueba y la torna en una "diabólica" donde la persona refugiada, sin medios ni conocimiento para hacerlo, debe comprobar quien dice ser, y que es la máquina la que se equivoca, pese a la pretendida infalibilidad con que la narrativa de la innovación promueve su uso.

Por último, nos abocamos a la segunda pregunta que formulamos al inicio de la mano de la lectura del más reciente documento de OCHA sobre las ventajas y beneficios que trae el despliegue de las tecnologías digitales en la acción humanitaria. Allí, de manera sutil, fue posible entrever la promesa detrás de esas otras sobre efectividad, eficiencia, prevención del fraude e identificación de la persona refugiada. Se trata de la promesa de la predicción en la acción humanitaria. Predicción que dicho documento aborda sin dotar de mayor contenido sobre su alcance u objetivos, pero que puede presumirse que apunta a la identificación del quién y el dónde: quién necesitará por primera o segunda ocasión de la ayuda humanitaria, y en dónde habrá que desplegar dichos esfuerzos. Predicción dirigida, una vez más, al ahorro del gasto.

Sin ahondar en la extensa literatura sobre la capacidad, la funcionalidad ni las críticas variadas que han sido formuladas sobre las tecnologías digitales predictivas, retomamos solo algunos comentarios de manera general y que podrían extenderse a la acción humanitaria. Comentarios asociados a riesgos que vienen aparejados a la más intensa presencia de las *Big Tech* en dicho contexto, como al aumento de la opacidad en el funcionamiento de tecnologías que operan como cajas negras, ajenas al escrutinio social, o cuyo despliegue refuerza o amplifica sesgos de las realidades que se proyectan en los datos.

La promesa de la predicción –a lo que apunta el despliegue de tecnologías biométricas junto con otras con las que opera a manera de ensamblaje tecnológico en la acción humanitaria–, debe ser vista de cerca en otras investigaciones posteriores que ahonden en la intención de masificación de tecnologías cuya aplicación en otras áreas –como la predicción del crimen– ha generado cuestionamientos serios en materia de derechos humanos.

La tarea pendiente es una dedicada a la prevención de riesgos inciertos y de recabamiento de pruebas y evidencia sobre su impacto y logro de su finalidad, añadiendo a la ecuación los impactos que genera en derechos humanos. Una tarea que el documento de OCHA no delega en manos de nadie en concreto, y que enfrenta múltiples retos: de transparencia, de rendición de cuentas sobre las alianzas entre actores, de impactos en la privacidad de las personas, entre otros.

CONCLUSIONES

Iniciamos este escrito con el objetivo general de indagar en el estado del arte de la literatura que, desde 2015 y hasta la actualidad, se ha enfocado en referir a los beneficios y riesgos que tiene el despliegue de tecnologías digitales en la acción humanitaria. Tales tecnologías digitales intensivas están enfocadas en la recolección de datos personales y destinadas a la atención de las personas refugiadas. Para abordar tal objetivo, propusimos un plan que se dividió en tres capítulos.

El primer capítulo estuvo destinado a proveer un contexto de partida sobre la filosofía de la acción humanitaria que se enmarca, básicamente, en la delimitación conceptual e histórica de sus principios: humanidad, neutralidad, imparcialidad, independencia. Principios que sirven, a manera de brújula, para orientar el trabajo de los actores que se dedican a proveer socorro y ayuda en contextos de crisis, que demandan acción rápida para promover el bienestar de las personas en condición vulnerable.

Luego de ese marco más amplio, fuimos cerrando en ese mismo capítulo nuestra aproximación de contexto para enfocar en la acción humanitaria que se provee a las personas refugiadas. Al respecto, describimos muy rápidamente el marco regulatorio en esa materia. Luego, algunos retos producto de la crisis reciente de refugiados que ha dotado a la acción humanitaria en ese campo de una visión restrictiva, securitizada y excluyente de ese ideal que expresan por su parte los principios.

Entre los problemas que enfrenta la gestión de la acción humanitaria en beneficio de las personas refugiadas, destacamos particularmente los de financiamiento y aumento creciente de la demanda global de ayuda. Situación que ha impactado no solo en la mayor participación de actores atípicos de la acción humanitaria, como el sector privado de las *Big Tech*, sino a la instalación también aquí de una narrativa que no es nueva, pero que refuerza la importancia sobre la efectividad y eficiencia del gasto que ha masificado recientemente el uso de tecnologías digitales destinadas a la prevención del fraude y la suplantación de la identidad de las personas beneficiarias. Eventos que, se dice, impactarían positivamente en cómo se invierten los recursos de actores globales que se desempeñan en ese campo, como ACNUR y la agencia de la ONU para los alimentos.

En este ejercicio planteamos acotar el contexto a una situación que denominamos como el aterrizaje de las tecnologías digitales en la acción humanitaria, y pusimos la atención en la narrativa tecnoentusiasta que acompaña el arribo de compañías de *Silicon Valley* a dicho terreno.

Los problemas más relevantes asociados a dicho fenómeno tienen que ver con la puesta en peligro de los principios fundantes de la acción humanitaria, que compiten ahora con los valores del mercado y los modelos de negocio de grandes compañías que ven, en esta, un escenario ideal para la experimentación de sus propios desarrollos. Pero más especialmente, con los riesgos que dichos actores y alianzas representan para la privacidad y protección de datos de las personas refugiadas.

Dijimos que la narrativa tecnoentusiasta se caracteriza, en principio, por depositar en las tecnologías digitales una fe incondicional sobre sus bondades, y por carecer de una visión crítica sobre sus riesgos o impactos. Una mirada que obscurece la rendición de cuentas, la responsabilidad de los intervinientes, que obvia los análisis sobre el impacto de las relaciones de poder, las desigualdades preexistentes, y que la tecnología puede legitimar por su supuesto papel neutral y objetivo. Esta mirada crítica de las tecnologías digitales, pretendió servir como anteojos con los que mirar el análisis y revisión que se efectuó en el segundo capítulo.

En el segundo capítulo se propuso una primera sección dedicada a recuperar los estándares en materia de protección de datos que permitieran entender cuál es el *deber ser* de dicho derecho para facilitar la comprensión sobre qué tanto se distancia o no del *ser* en esa materia advertido por la literatura revisada.

Así, organizamos la literatura según los riesgos que fueron advertidos para cada principio. En general, la literatura que se analizó y refirió a la protección de datos, el despliegue de tecnologías digitales en la acción humanitaria, y las personas refugiadas, se caracterizó en términos generales por abundar en los riesgos en materia de consentimiento y seguridad, que son los más destacables o en los que convergen una buena cantidad de autores, y en sugerir la manera cómo la 'contaminación' del consentimiento informado debilita el resto de principios de la protección de datos. También se apuntó el papel que han tenido dos agencias de la ONU en dicha materia: ACNUR y el Programa Mundial para los Alimentos. Ambas son, a su vez, los dos actores no gubernamentales que más tecnologías digitales en la acción humanitaria han desplegado, y que más han presionado a otros actores de dicho ecosistema para que efectúen su puesta en marcha. También se abordaron de cerca contextos de despliegue de tecnologías digitales en África, escaseando la literatura que refiere a otras experiencias como la latinoamericana. En este caso, se hace evidente, cuando el titular del derecho a la protección de datos es una persona refugiada, las garantías a sus derechos son más débiles: los escándalos sobre entregas deliberadas de sus datos sensibles a los países de los que huyen no reciben sanción o reproche más allá de los titulares de prensa, o la reacción de la academia y las organizaciones de sociedad civil. Distintos autores parecen coincidir en que, si la discusión versara sobre otros contextos, la aplicación de los estándares vigentes y la aplicación de sanciones estrictas no se harían esperar.

Igualmente, los textos leídos sugirieron que el problema de la protección de datos en la acción humanitaria es uno que trasciende a la política de privacidad que pudieran tener grandes actores, como las agencias de la ONU que atienden a la población refugiada. De hecho, fue posible observar cómo contaban en el papel con buenas políticas internas en ese sentido, pese a que en la práctica no se las pusieran en marcha.

El problema de la aplicación débil de políticas que, en el papel parecen satisfacer los estándares vigentes, se relaciona de manera cercana con una situación que expusimos en el primer capítulo sobre la debilidad de la rendición de cuentas, la responsabilidad, así como la ausencia de otros actores distintos a los humanitarios que se encargaran de la aplicación de las políticas vigentes. A partir de la idea según la cual los problemas de la protección de datos en dicho escenario se explican también a partir de otros factores, distintos a los de seguridad de la información o el consentimiento, por citar un par de casos, decidimos volcarnos al desarrollo del capítulo tercero.

En dicho capítulo hicimos una caracterización de riesgos y beneficios de tres tipos de actores a los que habíamos referido hasta ese momento: el sector privado, los actores humanitarios –no estatales– y las personas refugiadas.

La intención de dicha caracterización fue la de ir más allá de los riesgos en protección de datos para las personas refugiadas, para permitir entender qué había en juego para los otros dos actores, pero, sobre todo, indagar en cuáles eran las razones que, pese a los riesgos de protección de datos referidos en el capítulo segundo, apuntaban a la intención de los actores humanitarios por seguir masificando el uso de tecnologías digitales como la biometría.

Entendimos que los actores del sector privado tienen mucho por ganar y nada por perder. Que les resulta favorable la crisis de la acción humanitaria en beneficio de las personas refugiadas, pues cuentan con la capacidad y recursos de la que cada vez más estos carecen por la retirada de sus financiadores más importantes: los Estados. Dichos actores humanitarios parecen estar dispuestos a llevar a cabo un intercambio entre algunos de los principios que orientan la razón de ser de su trabajo, con tal de contar con una capacidad en terreno ampliada, fortalecida por la presencia de tecnologías digitales cuya presencia está destinada a tratar de convencer a los Estados de que los recursos no se invierten en quien no lo merece o necesita.

Al tiempo, confirmamos que quienes menos se benefician de esta dinámica de relacionamiento de poder e intereses sin supervisión o vigilancia, son las personas refugiadas. Su privacidad y protección de datos se encuentran en riesgo, pero también sucede con otros derechos igualmente importantes, como el de ser tratados en condición de igualdad a otros o el de no ser discriminados. Fruto de todo lo anterior, proponemos las siguientes ideas a modo de conclusión.

En primer lugar, que los *problemas estructurales de la acción humanitaria en beneficio de las personas refugiadas pueden ser amplificados por el uso y despliegue de tecnologías digitales, como la biometría*.

El sesgo de confirmación lleva a creer que, cuando las tecnologías digitales son desplegadas en un contexto específico, dotan de objetividad a procesos

mediados por el ser humano pues este se encuentra cargado de sesgos cognitivos y puede llegar a discriminar a los otros. Situación que, en la práctica, termina petrificando eventos de desigualdad y relaciones de poder análogas que, tecnologías como la biometría, tornan luego en incuestionables, irrebatibles pues "la máquina no se equivoca".

En materia de responsabilidad, el problema no-tecnológico que explotan las tecnologías digitales es probablemente el de la continuación de la ausencia de mecanismos de reclamo. La presencia de tecnologías digitales sugiere que, en tanto que objetivas y neutrales, pueda no haber necesidad de reclamar por el error, lo que acarrea dos efectos: desincentivar la creación de mecanismos para exponer eventuales fallos o mecanismos para hacerlos visibles pues de ocurrir, en todo caso, serían endosables a la persona; y el de imposibilitar a la persona la prueba del error.

Ambos efectos no son propios de las tecnologías digitales desplegadas en la acción humanitaria, sino en general, de las que se despliegan con ánimo de hacer eficiente un proceso que bien puede ser el de determinación de la asignación de un beneficio social, de predicción de reincidencia en materia criminal, entre otros. Se trata en sí mismo de un riesgo de las tecnologías digitales que se diseñan y ponen en marcha de manera poco transparente, accesible, auditable o revisable por la razón que sea: cajas negras, la protección de la propiedad intelectual, la vigencia de acuerdos de inmunidad o confidencialidad, entre otros.

En relación con lo anterior, el despliegue de tecnologías digitales en la acción humanitaria ha consolidado una práctica de evasión activa de la responsabilidad atribuible a agentes como ACNUR. Según vimos, la razón fundacional al despliegue de las tecnologías digitales de identificación biométrica tiene que ver, en verdad, con el aumento de la responsabilidad ascendente que debe dicha agencia con sus financiadores, en sacrificio de procesos de responsabilidad descendente dirigidos a la persona refugiada. La evasión activa de la responsabilidad pudo ser constatada recientemente en el caso que Human Rights Watch documentó sobre la comunidad Rohingya, respecto de la cual ACNUR no solo negó que hubiese indebidas prácticas de tratamiento de la información, sino que evitó referirse al impacto que tenían las tecnologías de identificación biométrica para condicionar el acceso a la ayuda humanitaria. Evasión que, en todo caso, no recibió ninguna sanción más allá de un par de titulares de prensa e informes de organizaciones de la sociedad civil.

Las tecnologías digitales como la biometría refuerzan, bajo la narrativa de la eficiencia, una racionalidad de sospecha de la persona vulnerable. Su objetivo no es apuntar al empoderamiento de las personas, sino someterlas a la vigilancia prolongada de sus cuerpos bajo la presunción inversa de que toda persona no es quien afirma ser hasta que se disponga a probarlo. No hacerlo la excluye, en principio, de la órbita de alcance de los actores humanitarios, situación que de paso disloca la razón de ser de la acción humanitaria apoyada en principios que afirman todo lo contrario.

Otro problema no tecnológico que se ve amplificado es el de la cesión de ciertos derechos, a cambio del acceso a ciertos bienes y servicios. Ese tipo de relaciones es común en la relación entre la ciudadanía y sus Estados. En dicha cesión,

sin embargo, le son exigibles a estos últimos la satisfacción de ciertos estándares cuyo incumplimiento habilitan a la persona, titular de derechos, a reclamar a través de los recursos disponibles para ello.

La pregunta que esta situación genera es ¿qué deberes puede exigir una persona en un extremo grado de vulnerabilidad a ese tercero que le provee de ayuda, no en la condición de derecho sino de "beneficio facultativo"? ¿Qué hay cuando la negativa a dicho "beneficio facultativo" se sustenta en el despliegue de tecnologías digitales cuyos desarrolladores y responsables no parecen ser alcanzados plenamente por estándares vigentes en derechos humanos?

El segundo problema tiene que ver con el *doble estándar con el que se juzga la protección de datos y el despliegue de tecnologías digitales en la acción humanitaria en relación con los escenarios ordinarios de tratamiento de datos a cargo de los Estados*. El tratamiento de datos personales, tanto en el ámbito estatal como en el ámbito de la acción humanitaria cuenta con figuras responsables, ambas han llegado a adoptar estándares y buenas prácticas en la materia a través de políticas de protección de datos en el ámbito legal, para el caso de los Estados, y a nivel organizacional, para el caso de los actores humanitarios.

Ambos actores procesan información personal y sensible con la promesa de realizar unos fines determinados asociados a la entrega de ciertos bienes o la provisión de determinados servicios. Dicho tratamiento, en términos generales, no introduce excepciones para su aplicación en tiempos de normalidad o crisis y emergencia, por lo que sigue rigiendo la aplicación de los estándares y buenas prácticas adoptados.

En principio, visto así no habría razón para juzgar con una vara distinta el tratamiento de datos que ocurre en el ámbito humanitario cuando se trata de una persona que, pese a su condición vulnerable, sigue siendo titular de derechos en condición de igualdad con el resto de personas.

Aun cuando esto es así, se ha consolidado en la práctica, según lo demuestran los informes de auditoría y casos documentados en los capítulos segundo y tercero, una suerte de doble estándar que juzga como inocuo el despliegue de cierto tipo de tecnologías digitales y prácticas en materia de datos en la acción humanitaria. Así, por ejemplo, los sistemas de identificación biométrica han sido sometidos a intensos escrutinios en diversas jurisdiccionales en donde el Estado de Derecho está vigente y en donde legislaciones de protección de datos se encuentran en firme. Dicho escrutinio ha llevado, en más de una ocasión, a la prohibición o moratoria de sistemas de identificación biométrica, como la facial, por los impactos que esta tiene en la protección de los datos de las personas, así como en su privacidad para el ejercicio de otros derechos. ¿Por qué dichas preocupaciones no llaman la atención de los actores humanitarios que impulsan su despliegue y masificación?, ¿no se podría esperar que los problemas de una tecnología, cuando se aplica con un mismo fin en otro escenario, pueden llegar a producir los mismos impactos negativos para el ejercicio de derechos de la persona?

Los hallazgos de las auditorías a los sistemas biométricos de actores humanitarios de las Naciones Unidas, así como los comentarios de la literatura que duda sobre la narrativa que empuja a su masificación, parecen sugerir que, el propósito

humanista de estos actores cobija a las tecnologías que estos despliegan, dotándolas por su uso y contexto de un aparente potencial benéfico. Presunción que, en últimas, podría inhibir la adopción de miradas críticas.

También llama la atención la ausencia de reproche simbólico y jurídico de los Estados frente a los eventos de indebido tratamiento de la información que se han documentado en la acción humanitaria en beneficio de las personas refugiadas. La poca atención que prestan autoridades estatales especializadas en la materia se comprueba, por ejemplo, en la lectura de la resolución de la Asamblea Global de Privacidad de octubre de 2020, la cual es patrocinada por más de una docena de autoridades de protección de datos en el mundo entre los que se incluye el Comisionado de Protección de Datos del Consejo de Europa, entre otros.

Dicha resolución afirma que la Asamblea ayudará a coordinar esfuerzos con las múltiples partes interesadas para crear un ambiente regulatorio global, consistente en la materia y aplicable a la acción humanitaria. Pese a ello, no provee contextos sobre el estado actual de cosas que permitan comprender que, de hecho, algunos actores humanitarios ya adoptan estándares reconocidos en la materia, pese a que subsiste una brecha operativa en la práctica. La propuesta que sugiere, no obstante, es la de creación de más estándares (Global Privacy Assembly, 2020).

Y, por último, el *derecho a la protección de datos no puede ser visto de manera aislada a las relaciones de influencia y de poder que subyacen a su ejercicio*.

La protección de datos como derecho debe poder superar la mirada que posa su atención exclusivamente en las formalidades del consentimiento informado, es decir, en lo que se marca o no en una casilla de "sí" o "no" de un formulario. Una mirada crítica sobre su ejercicio debe trascender hacia las relaciones entre los actores, calculando lo que estos ponen en riesgo y lo que obtienen del despliegue de tecnologías digitales que de manera intensiva recogen o capturan los datos personales de terceros.

Dicha mirada debe poder reconocer y sopesar los problemas estructurales del ecosistema en el que se lleva a cabo el tratamiento masivo de la información de poblaciones en condición de vulnerabilidad o desventaja. La recolección y tratamiento de datos no sucede en ambientes asépticos. Por tanto, las prácticas en materia de responsabilidad, de rendición de cuentas y transparencia tienen la potencialidad de extenderse al tratamiento de datos tanto como existan previo a este.

El análisis de las relaciones de poder debiera poder sopesar el listado de riesgos y beneficios en juego según cada actor, así como la posición en que estos se encuentran. Las empresas tecnológicas, los Estados y los actores humanitarios sin importar su capacidad, rol o contexto, se ubican de manera indistinta en el extremo más favorecido en comparación con ese otro extremo débil, la persona refugiada. Esta, a su turno, se ve obligada a ceder su información personal más sensible, producto de la presión en que se traduce su posición frente a diversos actores con los que no tiene capacidad para negociar los términos y alcance de su consentimiento, mucho menos para hacerles rendir cuentas.

Este relacionamiento desigual, que torna al consentimiento en un ejercicio de adhesión a cláusulas o condiciones que no terminan siendo del todo conocidas por la persona, desde luego no orbita exclusivamente alrededor de la acción

humanitaria o la protección de datos. Las lecciones recogidas al respecto en otros ámbitos igualmente sensibles y de desigualdad informativa, como el sanitario, debe poder llevar a reflexiones que permitan afirmar la centralidad del consentimiento como manifestación de la autonomía de la voluntad de la persona bajo prácticas que la condición de emergencia y excepcionalidad del contexto humanitario no puedan tornar en imposibles.

Igualmente, este tipo de análisis precisan ser vistos a través de los lentes de la humanidad, neutralidad, imparcialidad e independencia. La lógica principialista de la acción humanitaria, según vimos en el primer capítulo, apunta a la afirmación de ciertas reglas de acción que se basan en el juicio y experiencia de los actores humanitarios. Reglas que deben poder ser aplicadas tanto como sea posible en las condiciones de crisis y riesgo en que estos se desenvuelven. Es imperativo imaginar vías que permitan hacer compatible su vigencia con el tratamiento ético de los datos personales de personas vulnerables.

Por último, entendemos que este trabajo no hace sino confirmar la importancia de la materia y la necesidad de seguir investigando. Por ello, proponemos las siguientes líneas para continuar.

Primero: evaluar otras tecnologías digitales, distintas a la biométrica, para reconocer cuáles son los riesgos y beneficios ante sus aplicaciones concretas, que permitan entender el panorama completo sobre lo que significa el despliegue de las tecnologías digitales en la acción humanitaria.

Segundo: vale la pena poder, a futuro, ampliar la perspectiva geográfica y temporal en el abordaje del problema que estudiamos en este escrito, para mejorar la comprensión de un fenómeno que va más allá de la existencia de escáneres de huellas digitales y rostros en contextos de crisis. Esto es preciso, en tanto que permitirá ahondar en las causas y la relación de las variables que influencian la existencia y continuidad de la masificación de tecnologías en la acción humanitaria, lo cual puede facilitar más adelante el diseño de soluciones acorde con la vigencia plena de los derechos humanos.

Tercero: adquiere importancia poder analizar más adelante la necesidad de aumentar los estándares en materia de protección de datos para ser aplicados en la acción humanitaria, o la conveniencia de diseñar regímenes específicos y con estándares menos rigurosos para ser aplicados por estos, así como la revisión de los estándares actuales que ya han sido adoptados y las razones por las que subsiste una brecha entre su acogida y aplicación en la práctica.

Cuarto: plantear un proceso de revisión sobre la posible compatibilidad entre los regímenes de inmunidad legal de los que gozan los actores humanitarios, con la puesta en marcha de mecanismos de responsabilidad y rendición de cuentas en materia de protección de datos. Revisión que implica, de paso, el estudio cercano de las bases estructurales del humanitarismo, así como de sus dinámicas más asentadas.

Finalmente, el abordaje a futuro del problema al que dedicamos esta investigación, exige mirar los problemas sociales más allá de lo tecnológico y así mismo las soluciones que apunten a generar cambios. La amenaza que representa para el ejercicio de los derechos humanos el uso y despliegue de las tecnologías digitales

debe poder aumentar nuestro sentido de la urgencia para estudiarlas, así como nuestra responsabilidad para hallar nuevas y mejores vías de protección de las personas que se encuentran en condiciones de vulnerabilidad, y que tienen que poder ser pensadas con todas las múltiples partes interesadas a bordo.

REFERENCIAS BIBLIOGRÁFICAS

Access Now (2021). "Iris scanning of refugees is disproportionate and dangerous– What's happening behind IrisGuard's closed doors?". *Access Now*. Recuperado de https://www.accessnow.org/irisguard-refugees-jordan/

ACNUR (2010). *La Protección de los Refugiados y la Migración Mixta: El Plan de los 10 Puntos en Acción*. s. d.

ACNUR (2018). *Declaración de Nueva York sobre Refugiados y Migrantes*. Recuperado de https://www.acnur.org/declaracion-de-nueva-york-sobre-refugiados-y-migrantes.html.

African Union (2020). *Convention on Cyber Security and Personal Data Protection*. Recuperado de https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

Akhmatova, D.-M., y Akhmatova, M.-S. (2020). "Promoting digital humanitarian action in protecting human rights: Hope or hype". *Journal of International Humanitarian Action*, *5*(1), p. 6. https://doi.org/10.1186/s41018-020-00076-2.

Amnistía Internacional (2016). *Atajar la crisis global de refugiados. De eludir a repartir la responsabilidad*. s. d. Amnesty International.

APEC (2015). *APEC Privacy Framework* (APEC#217-CT-01.9). https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).

Arendt-Cassetta, L. (2021). *From digital promise to frontline practice: New and emerging technologies in humanitarian action*. Office for the Coordination for Humanitarian Affairs.

Benton, M., y Glennie, A. (2016). "Digital Humanitarianism: How Tech Entrepreneurs Are Supporting Refugee Integration". *Migration Policy Institute*, 35.

Betts, A. (2014, June 1). *International Relations and Forced Migration*. The Oxford Handbook of Refugee and Forced Migration Studies. https://doi.org/10.1093/oxfordhb/9780199652433.013.0004.

Binder, A., y Koddenbrock, K. (2013). *Reflections on the Inequities of Humanitarian Assistance*. Global Public Policy Institute. https://www.gppi.net/2013/06/01/reflections-on-the-inequities-of-humanitarian-assistance-possible-courses-of-action-for-germany.

Binder, M. (2017). *The United Nations and the Politics of Selective Humanitarian Intervention*. Springer International Publishing. https://doi.org/10.1007/978-3-319-42354-8.

Bohmer, C., y Shuman, A. (2008). *Rejecting Refugees: Political Asylum in the 21st Century*. Routledge. https://www.routledge.com/Rejecting-Refugees-Political-Asylum-in-the-21st-Century/Bohmer-Shuman/p/book/9780415773768.

Bouffet, T., y Marelli, M. (2021). "The price of virtual proximity: How humanitarian organizations' digital trails can put people at risk". *Humanitarian Law & Policy Blog*. https://blogs.icrc.org/law-and-policy/2018/12/07/price-virtual-proximity-how-humanitarian-organizations-digital-trails-put-people-risk/

Brayne, S. (2021). *Predict and Surveil. Data, discretion, and the future of policing*. Oxford University Press.

Brown, D. (2020). "Big Tech's Heavy Hand Around the Globe". *Human Rights Watch*. https://www.hrw.org/news/2020/09/08/big-techs-heavy-hand-around-globe.

Burns, R. (2019). New Frontiers of Philanthro-capitalism: Digital Technologies and Humanitarianism. *Antipode*, *51*(4), 1101–1122. https://doi.org/10.1111/anti.12534.

Chandran, R. (2021, August 17). *Afghans scramble to delete digital history, evade biometrics*. Reuters. https://www.reuters.com/article/afghanistan-tech-conflict-idUSL8N2PO1FH.

Charles Raul, A., & Porath, S. (2020). *The Privacy, Data Protection and Cybersecurity Law Review: APEC Overview*. https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/apec-overview.

Churruca-Muguruza, C. (2018). "The Changing Context of Humanitarian Action: Key Challenges and Issues". En H.-J. Heintze y P. Thielbörger (Eds.), *International Humanitarian Action: NOHA Textbook* (pp. 3-18). Springer International Publishing. https://doi.org/10.1007/978-3-319-14454-2_1.

Comisión Interamericana de Derechos Humanos (2020). *Debido proceso en los procedimientos para la determinación de la condición de persona refugiada, y apátrida y el otorgamiento de protección complementaria* (p. 159). Organización de Estados Americanos.

Comité asesor del Consejo de Derechos Humanos (2021). *Impactos, oportunidades y retos que pueden entrañar las tecnologías digitales nuevas y emergentes en relación con la promoción y la protección de los derechos humanos* (A/HRC/47/52). https://undocs.org/es/A/HRC/47/52.

Council of Europe (2018). *Convention for the Protection of Individuals with regard to the processing of personal data*. https://www.coe.int/es/web/data-protection/convention108-and-protocol.

Council on Foreign Relations (s. f.). *The World's Swelling Refugee Population Has Shrinking Options*. Council on Foreign Relations. Recuperado el 23 de junio de 2021 de https://www.cfr.org/refugee-crisis/

Coyne, C.J. (2013). *Doing bad by doing good: Why humanitarian action fails*. Stanford Economics and Finance, an imprint of Stanford University Press.

Crawford, K., y Finn, M. (2015). "The limits of crisis data: Analytical and ethical challenges of using social and mobile data to understand disasters". *GeoJournal*, *80*(4), pp. 491–502. https://doi.org/10.1007/s10708-014-9597-z.

Davies, S. (2012). *How a United Nations agency buried a security report that warned*

of potential genocide. The Privacy Surgeon. Recuperado de http://www.privacy-surgeon.org/blog/incision/how-a-united-nations-agency-buried-a-security-report-that-warned-of-potential-genocide/

Davison, R., Vogel, D., Harris, R., y Jones, N. (2000). "Technology Leapfrogging in Developing Countries–An Inevitable Luxury?". *The Electronic Journal of Information Systems in Developing Countries*, *1*(1), pp. 1-10. https://doi.org/10.1002/j.1681-4835.2000.tb00005.x.

Dembour, M.-B., y Kelly, T. (2011). *Are Human Rights for Migrants?: Critical Reflections on the Status of Irregular Migrants in Europe and the United States*. Routledge.

Dette, R. (2018). "Do No Digital Harm: Mitigating Technology Risks in Humanitarian Contexts". En S. Hostettler, S. Najih Besson y J.-C. Bolay (Eds.), *Technologies for Development* (pp. 13-29). Springer International Publishing. https://doi.org/10.1007/978-3-319-91068-0_2.

Development Assistance Roadmap Portal in the Middle East (2018). *Mastercard and The World Food Program 100 Million Meals Commitment*. Recuperado de https://darpe.me/mastercard-and-the-world-food-programme-announce-100-million-meals-commitment/

Devidal, P. (2021, March 2). "Cashless cash: Financial inclusion or surveillance humanitarianism?". *Humanitarian Law & Policy Blog*. Recuperado de https://blogs.icrc.org/law-and-policy/2021/03/02/cashless-cash/

D'Ignazio, C., y Klein, L.F. (2020). *Data feminism*. Recuperado de https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=2378911.

DLA PIPER (2021). *Data protection laws of the world. Full handbook*. DLA PIPER. https://www.dlapiperdataprotection.com/index.html?t=about&c=BD.

DuBois, M. (2018). *The new humanitarian basics*. Humanitarian Policy Group. www. odi.org.uk/hpg.

Duffield, M. (2016). "The resilience of the ruins: Towards a critique of digital humanitarianism". *Resilience*, *4*(3), 147–165. https://doi.org/10.1080/21693293.2016.1153772.

Eaton-Lee, J., y Shaughnessy, E. (2021). "Oxfam's new policy on biometrics explores safe and responsible data practice–World". *ReliefWeb*. https://reliefweb.int/report/world/oxfam-s-new-policy-biometrics-explores-safe-and-responsible-data-practice.

Edroos, F. (2017). *Suu Kyi is lying, there is no al-Qaeda in Rakhine.* https://www.aljazeera.com/news/2017/9/13/arsa-who-are-the-arakan-rohingya-salvation-army.

Edwards, S. (2018). *Accountability in the aid sector: Humanitarians can no longer be above the law*. Devex. https://www.devex.com/news/sponsored/accountability-in-the-aid-sector-humanitarians-can-no-longer-be-above-the-law-92133.

European Data Protection Supervisor (2015). "Resolution on Privacy and International Humanitarian Action". En *37th International Conference of Data Protection and Privacy Commisioners.* Documento electrónico recuperado de:
https://edps.europa.eu/sites/default/files/publication/15-10-27_resolution_privacy_humanitarian_action_en.pdf.

Egbert, S., y Leese, M. (2021). *Criminal Futures: Predictive Policing and Everyday Police Work*. Routledge.

Europe Union (2013). *Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person*. Recuperado de https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02013R0604-20130629.

Fairhust, M. (2018). *Biometrics. A very short introduction*. Oxford University Press.

Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja (2016). *Principios fundamentales del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja. Ética y herramientas para la acción humanitaria*. Comité Internacional de la Cruz Roja.

Feldman, I. (2015). "What is a camp? Legitimate refugee lives in spaces of long-term displacement". *Geoforum*, *66*, pp. 244–252. https://doi.org/10.1016/j.geoforum.2014.11.014.

Ferris, E.G. (2011). *The politics of protection: The limits of humanitarian action*. Brookings Institution Press.

Fiori, J. (2013). "The discourse of Western Humanitarianism". *Observatoire Des Questiones Humanitaries*, s. d.

Flaeming, T., Sandstrom, S., Caccavale, O.M., Bauer, J.M., Halma, A., y Poldermans, J. (2017). *Using big data to analyse WFP's digital cash programme in Lebanon*. Humanitarian Practice Network. Recuperado de https://odihpn.org/blog/using-big-data-to-analyse-wfps-digital-cash-programme-in-lebanon/

Gazi, T. (2020). "Data to the rescue: How humanitarian aid NGOs should collect information based on the GDPR". *Journal of International Humanitarian Action*, *5*(1), p. 9. https://doi.org/10.1186/s41018-020-00078-0.

Gelb, S., y Krishnan, A. (2018). "Technology, migration and the 2030 Agenda for Sustainable Development". *Overseas Development Institute*, 20.

Ginty, M., y Peterson, J. (Eds.). (2015). *The Routledge Companion to Humanitarian Action*. Routledge.

Global Privacy Assembly (2020). *Adopted Resolution on the Role of Personal Data Protection in International Development aid, International Humanitarian Aid in Crisis Management* (42nd Closed Session). https://edps.europa.eu/sites/default/files/publication/final_gpa_resolution_international_aid_en.pdf.

Greenwood, F. (2017). "The Signal Code: A Human Rights Approach to Information During Crisis". *Harvard Humanitarian Initiative*, 74.

Guevara Patiño, R. (2016). "El estado del arte en la investigación: ¿análisis de los conocimientos acumulados o indagación por nuevos sentidos?". *Folios*, *44*, pp. 165-179.

Hammerstadt, A. (2014, June 1). *The Securitization of Forced Migration*. The Oxford Handbook of Refugee and Forced Migration Studies. https://doi.org/10.1093/oxfordhb/9780199652433.013.0033.

Hathaway, J. (2005). *The Rights of Refugees under International Law*. Cambridge University Press.

Hosein, G. (2018). "Protecting the digital beneficiary". *Humanitarian Law & Policy Blog*. https://blogs.icrc.org/law-and-policy/2018/06/12/protecting-digital-beneficiary/

Human Rights Watch (2021). *UN Shared Rohingya Data Without Informed Consent*. Human Rights Watch. https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent.

Islam, M.R., y Bhuiyan, J.H. (Eds.). (2013). *An introduction to international refugee law*. Martinus Nijhoff Publishers.

Jacobsen, K.L. (2015). *The Politics of Humanitarian Technology: Good intentions, unintended consequences and insecurity*. Routledge. https://doi.org/10.4324/9781315777276.

Jacobsen, K.L. (2016). "UNHCR, accountability and refugee biometrics". En *UNHCR and the Struggle for Accountability*. Routledge.

Jacobsen, K.L. (2017). "On Humanitarian Refugee Biometrics and New Forms of Intervention". *Journal of Intervention and Statebuilding*, *11*(4), 529-551. https://doi.org/10.1080/17502977.2017.1347856.

Jacobsen, K.L., y Sandvik, K.B. (2016). "Introduction: Quest for an accountability cure". En *UNHCR and the Struggle for Accountability* (pp. 125). Routledge.

Jacobsen, K.L., y Sandvik, K.B. (2018). "UNHCR and the pursuit of international protection: Accountability through technology?". *Third World Quarterly*, *39*(8), 1508-1524. https://doi.org/10.1080/01436597.2018.1432346.

Jacobsen, K.L., y Steinacker, K. (2021). *Contingency Planning in the Digital Age: Biometric Data of Afghans Must Be Reconsidered*. https://blogs.prio.org/2021/08/contingency-planning-in-the-digital-age-biometric-data-of-afghans-must-be-reconsidered/

Jain, A.K., Ross, A.A., y Nandakumar, K. (2011). *Introduction to Biometrics*. Springer US. https://doi.org/10.1007/978-0-387-77326-1.

John Quinley III (2018, November 25). *Full press release about the #Rohingya refugee strike in the camps*. Recuperado de Https://t.co/wqXmF1fNnV [Tweet]. *@john_hq3*. https://twitter.com/john_hq3/status/1066914392384532480.

Kaurin, D. (2019). "Data Protection and Digital Agency for Refugees". *World Refugee Council Research Paper,* 12, 30.

Kent, J. (2019). *The role of technology in addressing the Global Migration Crisis*. Centre for International Governance Innovation.

Klippenstein, K., y Sirota, S. (2021, August 17). "The Taliban Have Seized U.S. Military Biometrics Devices". *The Intercept*. https://theintercept.com/2021/08/17/afghanistan-taliban-military-biometrics/

Kuner, C., Svantesson, D.J.B., Cate, F.H., Lynskey, O., y Millard, C. (2017). "Data protection and humanitarian emergencies". *International Data Privacy Law*, *7*(3), 147-148. https://doi.org/10.1093/idpl/ipx012.

Latonero, M., Hiatt, K., Napolitano, A., Clericetti, G., y Penagos, M. (2019). *Digital identity in the Migration & Refugee Context: Italy case study*. Data & Society.

Latonero, M., y Kift, P. (2018). "On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control". *Social Media + Society*, *4*(1), 2056305118764432. https://doi.org/10.1177/2056305118764432.

Lodinová, A. (2016). "Application of biometrics as a means of refugee registration". *Focusing on UNHCR's strategy*, *2*(2), 10.

Loescher, G. (2014, June 1). *UNHCR and Forced Migration*. The Oxford

Handbook of Refugee and Forced Migration Studies. https://doi.org/10.1093/oxfordhb/9780199652433.013.0003.

Madianou, M. (2019). "The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies". *Television & New Media*, *20*(6), 581-599. https://doi.org/10.1177/1527476419857682.

Marino, S. (2021). *Mediating the Refugee Crisis: Digital Solidarity, Humanitarian Technologies and Border Regimes*. Springer International Publishing. https://doi.org/10.1007/978-3-030-53563-6.

Mayson, S.G. (2018). "Bias in, Bias out". *Yale Law Journal*, *128*, 2218.

McDonald, S.M. (2016). *Ebola: A Big Data Disaster. Privacy, property and the law of disaster experimentation*. The Centre for Internet and Society. https://cis-india.org/papers/ebola-a-big-data-disaster.

Montalbano, B. (2020). *Ethical Hackers Breach U.N., Access 100,000 Private Records*. https://threatpost.com/hackers-breach-un-access-records/162944/

Morozov, E. (2012). *The Net Delusion: The Dark Side of Internet Freedom*. PublicAffairs.

Morozov, E. (2015). *La locura del solucionismo tecnológico*. Katz.

Obarrio, J. (2013). "Pensar al Sur| Intersticios de la política y la cultura. Intervenciones latinoamericanas". *Cuerpo, Subjetividad y Espacio de lo Político*, *2*(3). https://revistas.unc.edu.ar/index.php/intersticios/article/view/5362.

OCHA (2018). *Strategic Plan 2018-2021*. https://www.unocha.org/sites/unocha/files/OCHA%202018-21%20Strategic%20Plan.pdf.

OEA (2021). *Principios actualizados sobre la privacidad y la protección de datos personales* (CJI/RES 266, XCVIII/21).

OECD (1980). *Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales*.

OECD (2020). *What is the impact of the COVID-19 pandemic on immigrants and their children?* OECD. https://www.oecd.org/coronavirus/policy-responses/what-is-the-impact-of-the-covid-19-pandemic-on-immigrants-and-their-children-e7cbb7de/

Office of Internal Oversight Services (2016). *Audit of the Biometric Identity Management System at the Office of the United Nations High Commisioner for Refugees. Report 2016/181*. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwizyMzplIjyAhX_RDABHXjMD0QQFjAGegQIGhAD&url=https%3A%2F%2Foios.un.org%2Ffile%2F6506%2Fdownload%3Ftoken%3Dh8ejKFap&usg=AOvVaw08izhcYd9eQkQvNm4R8An4.

Office of the Inspector General (2017). *Internal Audit of Beneficiary Management. Internal Audit Report AR/17/17*. https://docs.wfp.org/api/documents/WFP-0000040084/download/?_ga=2.18686585.1326768420.1516256388-1682848339.1511261484.

Office of the Inspector General (2020). *Internal Audit of Third-Party Access to WFP's Data and Systems. Internal Audit Report No. AR/20/02*. World Food Program. https://www.wfp.org/audit-reports/internal-audit-third-party-access-wfps-data-and-systems-january-2020.

Oxfam, & Engine Room (2017). *Responsible Data at Oxfam: Translating Oxfam's Responsible Data Policy into practice, two years on*. Oxfam; The Engine Room. https://doi.org/10.21201/2017.9569.

Papagianni, G. (2015). *Asylum in the twenty-first century*. Routledge Handbooks Online. https://doi.org/10.4324/9781315759302.ch36.

Parker, B. (2017). *Security lapses at aid agency leave beneficiary data at risk*. The New Humanitarian. https://www.thenewhumanitarian.org/investigations/2017/11/27/security-lapses-aid-agency-leave-beneficiary-data-risk.

Parker, B. (2018). *Exclusive: Audit exposes UN food agency's poor data-handling*. The New Humanitarian. https://www.thenewhumanitarian.org/news/2018/01/18/exclusive-audit-exposes-un-food-agency-s-poor-data-handling.

Parker, B. (2019). *New UN deal with data mining firm Palantir raises protection concerns*. The New Humanitarian. https://www.thenewhumanitarian.org/news/2019/02/05/un-palantir-deal-data-mining-protection-concerns-wfp.

Parker, B. (2020a). *Donor details hacked in NGO data breach*. The New Humanitarian. https://www.thenewhumanitarian.org/news/2020/08/04/NGO-fundraising-database-hack.

Parker, B. (2020b). *Exclusive: The cyber attack the UN tried to keep under wraps*. The New Humanitarian. https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Pictet, J. (1979a). "The Fundamental Principles of the Red Cross". *International Review of the Red Cross (1961-1997)*, *19*(210), 130-149. https://doi.org/10.1017/S0020860400019872.

Pictet, J. (1979b). "The Fundamental Principles of the Red Cross (II)". *International Review of the Red Cross*, *19*(211), 184-197. https://doi.org/10.1017/S0020860400066523.

Pictet, J. (1979c). "The Fundamental Principles of the Red Cross (III)". *International Review of the Red Cross*, *19*(212), 255-258. https://doi.org/10.1017/S0020860400066675.

Pictet, J. (1979d). "The Fundamental Principles of the Red Cross (IV)". *International Review of the Red Cross*, *19*(213), 301–312. https://doi.org/10.1017/S0020860400066808.

Pictet, J. (1980a). "The Fundamental Principles of the Red Cross (V)". *International Review of the Red Cross*, *20*(214), 29-34. https://doi.org/10.1017/S002086040006695X.

Pictet, J. (1980b). "The Fundamental Principles of the Red Cross (VI)". *International Review of the Red Cross*, *20*(215), 70-78. https://doi.org/10.1017/S0020860400067061.

Privacy International (2019). *One of the UN's largest aid programmes just signed a deal with the CIA-backed data monolith Palantir*. Privacy International. http://privacyinternational.org/es/node/2712.

Rahman, Z. (2021, June 21). *Betrayal and denial from the UN on refugee data*. The New Humanitarian. https://www.thenewhumanitarian.org/opinion/2021/6/21/rohingya-data-protection-and-UN-betrayal.

Rahman, Z., Verhaert, P., y Nyst, C. (2018). "Biometrics in the Humanitarian Sector". *The Engine Room, Oxfam*, 22.

Raymond, N., y Al Achkar, Z. (2016). *Data preparedness: Connecting data, decision-making and humanitarian response*. Harvard Humanitarian Initiative.

Raymond, N., Al Achkar, Z., y Berens, J. (2016). *Building data responsibility into humanitarian action* (Think Brief). OCHA.

Read, R., Taithe, B., y Ginty, R.M. (2016). "Data hubris? Humanitarian information systems and the mirage of technology". *Third World Quarterly*, *37*(8), 1314-1331. https://doi.org/10.1080/01436597.2015.1136208.

Reidy, E. (2017). *How a fingerprint can change an asylum seeker's life*. The New Humanitarian. https://www.thenewhumanitarian.org/special-report/2017/11/21/how-fingerprint-can-change-asylum-seeker-s-life.

Richardson, R., Schultz, J.M., y Crawford, K. (2019). "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data Predictive Policing Systems, and Justice". *New York University Law Review*, *94*, 42.

Sandvik, K.B. (2016). "How accountability technologies shape international protection: Results-based management and rights-based approaches revisited". En *UNHCR and the Struggle for Accountability*. Routledge.

Sandvik, K.B., y Jacobsen, K.L. (2016). *UNHCR and the Struggle for Accountability. Technology, law and results-based management*. Routledge.

Sandvik, K.B., Jacobsen, K.L., y McDonald, S.M. (2017). "Do no harm: A taxonomy of the challenges of humanitarian experimentation". *International Review of the Red Cross*, *99*(904), 319-344. https://doi.org/10.1017/S181638311700042X.

Scarnecchia, D.P., Raymond, N.A., Greenwood, F., Howarth, C., y Poole, D.N. (2017). "A Rights-based Approach to Information in Humanitarian Assistance". *PLOS Currents Disasters*. https://doi.org/10.1371/currents.dis.dd709e442c659e97e2583e0a9986b668.

Scott-Smith, T. (2016). "Humanitarian neophilia: The 'innovation turn' and its implications". *Third World Quarterly*, *37*(12), 2229-2251. https://doi.org/10.1080/01436597.2016.1176856.

Slavin, A., Putz, F., y Korkmaz, E.E. (2021). *Digital Identity. An analysis for the humanitarian sector* [Data set]. Oxford Centre for Development & Technology, International Federation of Red Cross and Red Crescent Societies. https://doi.org/10.1163/2210-7975_HRD-9813-2015012.

Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance (2020a). *Racial and xenophobic discrimination, emerging digital technologies in border and immigration enforcement.* (A/75/590). https://undocs.org/A/75/590.

Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance (2020b). *Racial discrimination and emerging digital technologies: A human rights analysis.* (A/HRC/44/57). https://undocs.org/en/A/HRC/44/57.

Special Rapporteur on extreme poverty and human rights (2019). *Extreme poverty and human rights* (A/74/493). https://undocs.org/A/74/493.

Stevens, G.P., y Eberechi, O.E. (2019). "A critical analysis of article 16 of the UN refugee convention in relation to victims of sexual violence in refugee camps in

Africa". *De Jure*, *52*(1). https://doi.org/10.17159/2225-7160/2019/v52a10.
Tan, Y.S.A., y Schreeb, J. von (2015). "Humanitarian Assistance and Accountability: What Are We Really Talking About?". *Prehospital and Disaster Medicine*, *30*(3), 264-270. https://doi.org/10.1017/S1049023X15000254.
Thompson, A. (2015). "Humanitarian principles put to the test: Challenges to humanitarian action during decolonization". *International Review of the Red Cross*, *97*(897-898), 45-76. https://doi.org/10.1017/S1816383115000636.
Thomsen, M. (2019). *UNICC Assists UNHCR with Migration of IrisGuard to Microsoft Azure*. UNICC. https://www.unicc.org/news/2019/11/14/unicc-assists-unhcr-with-migration-of-irisguard-to-microsoft-azure/
UN Committee on Economic, Social and Cultural Rights (2000). *General comment no. 14 (2000), The right to the highest attainable standard of health (article 12 of the International Covenant on Economic, Social and Cultural Rights)*. UN. https://digitallibrary.un.org/record/425041.
UN General Assembly (1995). *Guidelines for the Regulation of Computerized Personal Data Files.* (Res.45/95). https://digitallibrary.un.org/record/162033.
UN General Assembly (2019). *The right to privacy in the digital age* (A/RES/73/179). UN,. https://digitallibrary.un.org/record/1661346.
UN High Commissioner for Human Rights (2014). *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights* (A/HRC/27/37). UN. https://digitallibrary.un.org/record/777869.
UN High Commissioner for Human Rights (2015). *Progress report of the United Nations High Commissioner for Human Rights on legal options and practical measures to improve access to remedy for victims of business-related human rights abuses* (A/HRC/29/39). UN. https://digitallibrary.un.org/record/798713.
UN Human Rights Committee (1988). *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*. https://www.refworld.org/docid/453883f922.html.
UN Human Rights Committee (2000). *CCPR General Comment No. 28: Article 3 (The Equality of Rights Between Men and Women)*. https://www.refworld.org/docid/45139c9b4.html.
UN Human Rights Council (2017a). *Resolution adopted by the Human Rights Council on 23 March 2017 "The right to privacy in the digital age"*. https://digitallibrary.un.org/record/1307661.
UN Human Rights Council (2017b). *The right to privacy in the digital age* (A/HRC/34/L.7/Rev.1). UN. https://digitallibrary.un.org/record/1307661.
UN Human Rights Council, y Special Rapporteur on the Promotion and Protection of the Right to Freedom of opinion and expression (2011). *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue* (A/HRC/17/27/Add.1). UN. https://digitallibrary.un.org/record/706200.
UN Human Rights Council, y Special Rapporteur on the Promotion and Protection of the Right to Freedom of opinion and expression (2013). *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom*

of Opinion and Expression (A/HRC/23/40/Add.1). UN. https://digitallibrary.un.org/record/756268.

UN Human Rights Council Special, y Rapporteur on the Right to Privacy (2019). *Right to privacy: Report of the Special Rapporteur on the Right to Privacy* (A/HRC/40/63). UN. https://digitallibrary.un.org/record/3853352.

UNCTAD (2020). *Data Protection and Privacy Legislation Worldwide*. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

UNHCR (2015). *Policy on the protection of personal data of persons of concern to UNHCR*. https://www.refworld.org/pdfid/55643c1d4.pdf.

UNHCR (2018a). "Chapter 5, UNHCR". En *Guidance on Registration and Identity Management*. https://www.unhcr.org/registration-guidance/chapter5/

UNHCR (2018b). *Guidance on the protection of personal data of persons of concern to UNHCR*. https://www.refworld.org/docid/5b360f4d4.html.

UNHCR (2018c). "Registration as an Identity Management Process". En *UNHCR. Guidance on Registration and Identity Management*. https://www.unhcr.org/registration-guidance/chapter5/registration/

UNHCR (2018d, May 23). "Data protection is part and parcel of refugee protection". *UNHCR Blog*. https://www.unhcr.org/blogs/data-protection-part-parcel-refugee-protection/

UNHCR (2020a). *Consequences of underfunding in 2020*. UNHCR. https://www.unhcr.org/underfunding-2020/

UNHCR (2020b). *Global trends. Forced displacement in 2020*. UNHCR.

UNHCR (2020c). *Procedural standards for Refugee Status and Determination under UNHCR's mandate.Unite: Reception and registration for mandate RSD*. https://www.refworld.org/docid/5e87075b2.html.

UNHCR (2020d). *UNHCR's 2020-2021 financial requirements*.

UNHCR (2020e). *Biennial programme budget 2020-2021 (revised) of the Office of the United Nations High Commissioner for Refugees* (A/AC/96/1202). UN. https://digitallibrary.un.org/record/3908002.

Unión Europea (2013). "Relativo a la creación del sistema 'Eurodac' para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) no. 604/2013". https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32013R0603&from=EN.

Reglamento General de Protección de Datos, Pub. L. No. 32016R0679, 119 OJ L (2016). http://data.europa.eu/eli/reg/2016/679/oj/spa.

United Nations (Ed.). (2014). *The economic, social and cultural rights of migrants in an irregular situation*. United Nations.

Unwin, T. (2017). *Reclaiming Information and Communication Technologies for Development* (Vol. 1). Oxford University Press. https://doi.org/10.1093/oso/9780198795292.001.0001.

van Dijk, J.A.G.M. (2005). *The Deepening Divide*. Sage Publications. https://us.sagepub.com/en-us/nam/the-deepening-divide/book226556.

van Dijk, J., y Hacker, K. (2003). "The Digital Divide as a Complex and Dynamic Phenomenon". *The Information Society*, *19*(4), 315-326. https://doi.org/10.1080/01972240309487.

Wacks, R. (2015). *Privacy: A Very Short Introduction* (2.da ed.). Oxford University Press.

Willits, B., Bryant, J., y Holloway, K. (2019). *The humanitarian "digital divide"*. Humanitarian Policy Group.

World Food Program (2019a). *A statement on the WFP-Palantir partnership | by World Food Programme | World Food Programme Insight | Medium*. https://medium.com/world-food-programme-insight/a-statement-on-the-wfp-palantir-partnership-2bfab806340c.

World Food Program (2019b). *Palantir and WFP partner to help transform global humanitarian delivery | World Food Programme*. https://www.wfp.org/news/palantir-and-wfp-partner-help-transform-global-humanitarian-delivery.