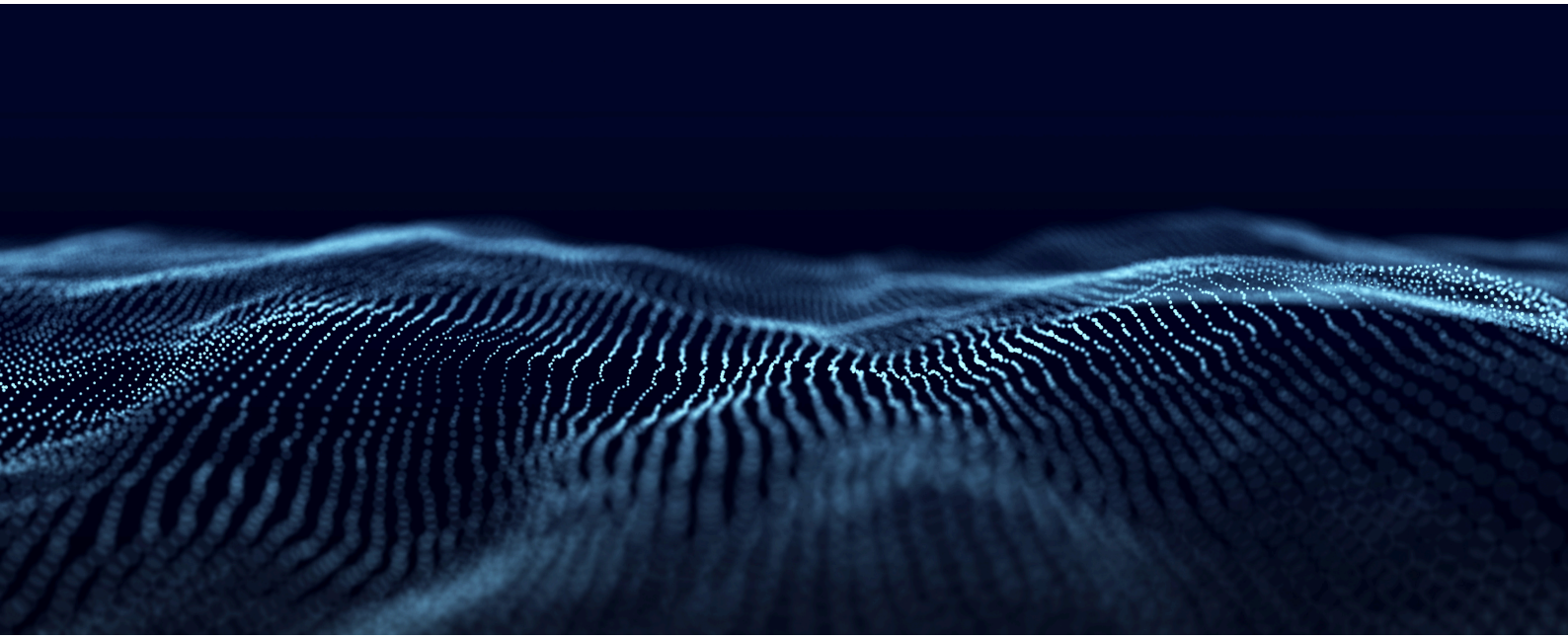
GENEVA GRADUATE INSTITUTE

INSTITUT DE HAUTES ÉTUDES INTERNATIONALES ET DU DÉVELOPPEMENT

GRADUATE INSTITUTE OF INTERNATIONAL AND DEVELOPMENT STUDIES

IOM UN MIGRATION



Data Responsibility and Accountability to Affected Populations

POLICIES AND ETHICS OF ARTIFICIAL INTELLIGENCE IN THE HUMANITARIAN LANDSCAPE

Applied Research Project 2023-2024

Georgina Colomer
Killian Foloppe
María Juliana Rodríguez

June 2024

Graduate Institute of International and Development Studies

Student Research Team
Georgina Colomer
Killian Foloppe
María Juliana Rodríguez

Academic Supervisor
Dr. Erica Moret

International Organization for Migration

Accountability to Affected Populations Team
Christie Bacal-Mayencourt
Pedro Arriaza

Disclaimer: The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the International Organization for Migration (IOM). The designations employed and the presentation of material throughout the publication do not imply expression of any opinion whatsoever on the part of IOM concerning the legal status of any country, territory, city or area, or of its authorities, or concerning its frontiers or boundaries.

Final Report
14 June 2024
Geneva, Switzerland

Word count
11,498

Table of contents

Acronyms and abbreviations

AAP	Accountability to affected populations
AI	Artificial Intelligence
BIMS	Biometric Identity Management System
BRaVE	Biometrics Registration and Verification System
DPIA	Data Protection Impact Assessment
DTM	Displacement Tracking Matrix
EU	European Union
GDPR	General Data Protection Regulation
GDT	Global Distribution Tool
HLCM	United Nations High-Level Committee on Management
HRW	Human Rights Watch
IASC	Inter-Agency Standing Committee
ICRC	International Committee of the Red Cross
IDP(s)	Internally Displaced Person(s)
IO(s)	International Organization(s)
IOM	International Organization for Migration
OCHA	United Nations Office for the Coordination of Humanitarian Affairs
PoC	United Nations House Protection of Civilians
PRIMES	Population Registration and Identity Management Eco-System
UISP	Unique Identity Service Platform
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNHCR	United Nations High Commissioner for Refugees
UNMISS	United Nations Mission in South Sudan
UNSC	United Nations Security Council
WFP	World Food Programme
WHO	World Health Organization

Executive summary and key recommendations

Given the growing number of humanitarian crises, international organizations (IOs) started to get interested in leveraging technologies such as artificial intelligence (AI) to improve their work. However, there are risks and concerns associated with using these technologies in fragile contexts. In such cases, IOs have put in place guidelines to account for people in vulnerable conditions, like the accountability to affected populations (AAP) approach, which is “an active commitment by humanitarian actors to use power responsibly by taking account of, giving account of, and being held to account by the people they seek to assist” (IOM, 2020: 2). In this regard, this research paper seeks to determine how the power of AI can be harnessed to ensure its ethical and responsible use in accordance with the AAP approach as well as data responsibility.

This research paper is the final output of an Applied Research Project conducted by students of the Geneva Graduate Institute in partnership with the International Organization for Migration (IOM). It consists of a literature review, two case studies, and interviews carried out with humanitarians. The literature review delves into data protection and data responsibility guidelines, legal frameworks in humanitarian action, the concepts of AAP, AI, and biometrics, as well as their ethical frameworks in fragile contexts. The main observation found is that even though there is a common interest in the use of biometrics, there is a lack of consensus on the responsible use of this technology in humanitarian action.

The case studies focus on the interplay of AI, AAP, and biometrics in the protracted migration flows in South Sudan and regarding the Rohingya people in Bangladesh. Finally, interviews with four experts working with IOM were conducted to fill in the gaps in the knowledge detected previously, as well as to identify good practices and areas of potential improvement in the use of AI and biometrics in the context of AAP.

From the research, it is derived that IOs involved in humanitarian work are increasingly concerned with data responsibility and data protection, as is reflected in their policies and guidelines, which emphasize similar principles like accountability, security, and transparency when handling personal data. However, there are significant gaps in implementation. While legal frameworks can help improve policies, there is a lack of specific regulations on AI in humanitarian contexts.

Ultimately, IOs are placing more emphasis on involving affected populations in decision making, highlighting the need for a human-centered approach to AI use in humanitarian assistance, especially in its intersection with biometric data management. The case studies

highlight the importance of responsible data-sharing of IOs with third partners, as well as maintaining the AAP approach throughout all phases of data management and humanitarian assistance provision.

The interviews revealed that IOM is not currently using AI in the field, and interviewees expressed mixed opinions on its potential for good in humanitarian assistance. Regarding a legally binding framework for AI use in humanitarian work, opinions ranged from organizational self-governance under inter-agency guidelines to the creation of a monitoring body, with concerns raised about achieving consensus for such a framework. Interviewees highlighted potential biases in the use of biometric data and the potential introduction of AI. Principles like data security, privacy, purpose, and necessity were stressed for its safe management. Finally, the importance of data-sharing agreements with partners before sharing sensitive information was raised.

To ensure that IOM and other humanitarian IOs in the United Nations (UN) system considering the use of AI and biometrics enhance the AAP approach, instead of putting vulnerable populations further at risk, this research paper has come up with six key recommendations:

Necessary ethical considerations for biometric data management and use of AI:

- **Placing humanitarian principles at the forefront.** As the most important principles of humanitarian action, “Do No Harm”, purpose and necessity, and people-centered approach should be the guiding ethical aspects when evaluating the possibility of using biometrics and AI in humanitarian action. They are essential considerations for ensuring AAP: this activity should not cause or exacerbate risks for affected populations to whom the collection of biometric data puts them in a more vulnerable position, whether by action or inaction.

- **Providing alternatives for data subjects.** IOs should come up with alternatives for beneficiaries who do not feel comfortable with giving their biometric data when receiving humanitarian assistance, especially if they fear persecution if doing so. Biometric data must not be a requisite for affected populations to access critical services in fragile contexts; doing so can lead to discrimination and endangerment of people already in vulnerable conditions. In this context, IOs should propose several alternatives to biometrics deployed, including when there is potential for integration with AI.

Data protection policies and data responsibility:

- **Strengthening data protection policies and integrating data responsibility.** To make sure that AAP is implemented through the use of biometrics - and its potential integration with AI, IOs must periodically update their data protection policies to reflect how this technology has impacted the way assistance is provided in humanitarian contexts and include a lessons-learned assessment of past experiences with deploying these technologies.

  A suggestion in this sense could be evaluating the implementation of a policy specific to the use of biometrics for delivering humanitarian assistance as done by other humanitarian organizations. Also, IOs must integrate the principles and guidelines mentioned in the Inter-Agency Standing Committee (IASC)'s Operational Guidance into their data protection policies, to guarantee effective AAP and have a strong framework for when the use of AI for managing biometric data is considered.

Ensuring accountability on all organizational levels:

- **Establishing mechanisms to exercise claim-rights and provide feedback.** Mechanisms and channels such as standardized forms should be provided to affected populations to ensure they can exercise the rights recognized in data protection policies. Instruments to provide feedback on the collection and usage processes of their data should also be put in place. Ideally, these instruments should have a closed form (e.g. surveys and/or structured interviews), to avoid overloading the feedback channel and to ensure expectations on the outcome of the complaints process are realistic.

- **Establishing clear boundaries on data-sharing agreements.** Data-sharing agreements should be unique to each set of data potentially being shared, and drafted after a data impact assessment has been carried out. Said assessments should focus both on the sensitivity of the data and the possibility of it being leaked, and on the partner organization's (other IOs, private partners, or governments) potential use of it. Each agreement should consider the overarching principles outlined earlier, and IOs should commit not to enter into them if there is uncertainty about affected populations' rights being respected. Finally, partners should subscribe to IOs' data protection policies as part of the data-sharing agreement.

How and when to use AI tools in humanitarian work:

- **Contextualizing the use of technology.** Within the AAP approach, AI should not be thought of as a solution, but rather a tool to enhance previously made commitments. IOs considering using AI in the humanitarian field should bear in mind that its use may not be suitable in all situations. If the use of AI does not provide any sort of added value to the work carried out, the AAP approach, and/or the rights of affected populations, it should not be applied. In other words, IOs' AI policy cannot consider using it by default.

1. Introduction

Whether due to extreme weather phenomena caused by climate change, or conflicts, such as interstate and intrastate wars, the need for humanitarian assistance has reached unprecedented levels. This sudden increase in humanitarian needs pushed the UN Secretary-General to organize a World Humanitarian Summit in 2016 to find a new approach to act in a unified and effective manner towards mounting humanitarian challenges (Heintze and Thielbörger, 2018). According to the Secretary-General, 125 million people needed humanitarian assistance in 2015, including 80% caused by armed conflicts. A further 60 million were forced to leave their homes (United Nations General Assembly, 2016).

As technological innovations have rapidly evolved recently, humanitarian IOs become increasingly interested in leveraging emerging technologies to collect and process large amounts of data related to their activities. However, with these innovations also comes the concern for data protection, especially regarding the personal data of the people they seek to help. In this regard, IOs have created data protection policies to guide humanitarians in handling the personal data of affected populations.

Through the analysis of the policies that IOs such as IOM have adopted for these matters and considering their legal implications, this project fills gaps created by the increasing use of AI and biometrics and determines how these technologies should be harnessed to ensure their responsible and ethical use in the humanitarian sector while strengthening AAP in IOM.

Therefore, this paper attempts to answer two research questions:

1. How can the power of AI be harnessed to ensure its ethical and responsible use for AAP and data responsibility in the humanitarian sector?

2. Focusing on biometric data, how can AI help enhance accountability to affected populations, while ensuring data responsibility in protracted migration flows such as the Rohingya people in Bangladesh and the refugee crisis in South Sudan?

By answering these questions, this research project seeks to produce results that could be used to further develop IOM policy in the responsible use of data collected through biometrics and processed by AI, and how this should be articulated within the AAP framework.

2. Methodology

Following a literature review on the ethical and humanitarian use of AI for AAP and data responsibility, this qualitative research takes a two-pronged approach consisting of a desk review and semi-structured interviews conducted with humanitarian professionals.

The literature review was carried out using relevant peer-reviewed articles and gray literature centering on AAP frameworks and guidelines, responsible AI use data responsibility law and policy, responsible biometric data collection, usage, and storage, as well as other relevant documents linking these key concepts with humanitarian settings.

To generate primary data, two case studies were selected in which the AAP approach intersects with AI and biometrics. The first case study is the Rohingya people in Bangladesh, the country in which most Rohingya refugees now live in camps after fleeing brutal persecution in neighboring Myanmar. The United Nations High Commissioner for Refugees (UNHCR) administers these camps together with the Bangladeshi government, where biometric data of refugees is collected to guarantee their access to assistance. Specifically, fingerprints and photographs are collected (Thomas, 2018), as part of the UNHCR's Biometric Identity Management System (BIMS), which allows the agency to verify who has and has not been a beneficiary (UNHCR, 2017).

The second case study is the refugee crisis in South Sudan. In 2014, IOM proposed the use of biometric registration to obtain information on the number of people living in the UN House Protection of Civilians (PoC) and to control migratory flows (IOM, 2016). Over the years, and with the protraction of the conflict, the use of biometrics has been extended to broader uses than just refugee camps. The technology is now used by several organizations in and outside PoC camps to verify the identity of South Sudanese people to provide them with food, health, and financial assistance (Freeman, 2023). More than six million people are registered on the database. However, concerns have been raised about the exchange of such sensitive information between different organizations, given that not all of them use data for the same purposes.

In both cases, the time frame selected for their study ranges from the first indications of biometric data collection by humanitarian organizations (2014 in South Sudan and 2016 in the Rohingya case) until today.

In addition, four interviews with IOM experts familiar with the cases and the overall research topic were conducted with the primary objective to fill in the gaps in the knowledge detected through the desk reviews, as well as to identify good practices and areas of potential

improvement in the use of AI and biometrics in the context of AAP. Two interviewees work daily on the Displacement Tracking Matrix (DTM), one person works on the information, management, and digitalization of registration data, and another person works on the registration of internally displaced persons (IDPs). The interviews, conducted on April 30th and May 1st, 2024, lasted between 40 and 65 minutes. Ten questions regarding AI and biometrics data were asked[1]. The interviews were semi-structured, meaning that questions were prepared in advance but remained open to discussion if the interviewee wished to develop specific points. The interviewees' responses were then operationalized into relevant concepts and added to a spreadsheet to facilitate their analysis[2].

The conclusions and recommendations were derived from analyzing the information and data generated through the literature review, case studies, and interviews conducted. The final objective is to highlight how AI tools can be used to enhance AAP and what are the risks, ethical challenges, and policy implications, as well as possible ways to mitigate them. The integrality of the study follows the Geneva Graduate Institute Research Ethics Guidelines[3].

3. Literature review

3.1. Data protection and data responsibility in humanitarian action

3.1.1. Policies on data protection from IOM and other international organizations

This literature review section looks at IOM's and UNHCR's data protection policies. Considering that these organizations are part of the UN System, it is important to look at the general guidelines provided by the UN on this matter. The UN High-Level Committee on Management (HLCM) launched the UN Personal Data Protection and Privacy Principles, often referred to as "the UN Principles", in 2018, which provide a framework for processing personal data in the context of the mandates of these organizations and harmonizing data protection standards across the UN System (HLCM, 2018).[4]

[1] The complete questionnaire used to conduct the semi-structured interviews, as well as an explanation of the question development process, can be found in Annex II.
[2] A more detailed explanation of the primary data analysis, as well as the mentioned spreadsheet, can be found on Annex III.
[3] Available at https://www.graduateinstitute.ch/research-support/research-ethics.
[4] For a detailed description of these principles, see Annex I.

The UN Principles apply only to personal data, defined as “information relating to an identified or identifiable natural person” (HLCM, 2018: 1). However, they can be assessed when processing non-personal data in sensitive contexts that may put vulnerable populations at risk of harm. The UN Principles also encourage the UN System to adhere to them and establish its policies accordingly. Implementing the Principles does not affect the immunities and privileges of the organization in the UN System.

Regarding IOM’s data protection policy, it is worth noting that it was adopted before the UN Principles, having entered into effect in 2010, However, it has elements in common with the Principles. This policy is underlined in the IOM Data Protection Manual, which states that:

> “*IOM shall take all reasonable and necessary precautions to preserve the confidentiality of personal data and the anonymity of data subjects. All personal data shall be collected, used, transferred and stored securely in accordance with the IOM data protection principles.*” (IOM, 2010: 9)

The IOM Manual establishes that this policy only applies to personal data, which is defined as “all information that could be used to identify or harm data subjects” (IOM, 2010: 14). Among the types of personal data, the Manual lists the following: biographical data (name, date of birth, sex, gender, sexual orientation, race, and nationality); biometric and genetic data (fingerprints, iris scans, facial image, and voice recognition); background data (family and household history); images and recordings (photographs, videos, voice and digital recordings); personal documents (health, financial, and criminal records); and verification documents (passports, identity cards, social security cards, birth certificates, temporary permits, and visas).

The Manual also defines data protection as “[...] the systematic application of a set of institutional, technical and physical safeguards that preserve the right to privacy with respect to the collection, storage, use and disclosure of personal data” (IOM, 2010: 13). To effectively enhance data protection, the Manual outlines 13 principles for data processing[5]. As mentioned above, despite the IOM Manual having preceded the UN Principles, it already envisioned most of them.

Finally, the IOM Manual highlights the immunities and privileges the organization has as part of the UN System. In this sense, IOM can decide whether to comply or not with domestic data protection regulations, depending on the circumstances of the assistance it provides in a particular country and if such regulations are consistent with its policy. Nevertheless,

[5] For a detailed description of these principles, see Annex I.

compliance with such legislation does not affect IOM's immunity status, meaning that its main source for the lawful and fair collection of personal data is the principles set out in the policy (IOM, 2010).

Regarding UNHCR, this agency has the Policy on the Protection of Personal Data of Persons of Concern, which lays down the principles guiding the processing of personal data of these individuals[6]: "Given the particularly vulnerable position of persons of concern to UNHCR, the nature of their personal data is generally sensitive and, therefore, requires careful handling [...]" (UNHCR, 2015: 7). The Policy, in line with the UN Principles and the IOM's Manual, pertains only to the personal data of these subjects, and other types such as anonymized or aggregate data do not fall within its scope.

The UNHCR Policy on the Protection of Personal Data of Persons of Concern defines personal data as "[a]ny data related to an individual who can be identified from that data; from that data and other information; or by means reasonably likely to be used related to that data" (UNHCR, 2015: 11). The Policy provides a similar classification of types of personal data to the one in the IOM Manual: biographical data (name, sex, country of origin, country of asylum, and religion and ethnicity); biometric data (a photograph, fingerprint, facial, or iris image); and any expression of opinion about the individual (specific needs). It also outlines eight principles for data processing[7].

The Policy also gives a more comprehensive look at the rights of data subjects.[8] These mean that data subjects have the right to know about the specific purposes for which their data is collected; if it is transferred to third parties; the possible consequences of refusing to provide personal data; the right to ask for their data to be corrected or deleted; and objecting to its collection. Lastly, this policy mentions the privileges and immunities UNHCR has, specifically regarding data transfer, and it says that this status exists regardless of cooperation agreements with governments (UNHCR, 2015).

It is worth mentioning that, in 2022, UNHCR published another data policy, known as the General Policy on Data Protection and Privacy (often referred to as "UNHCR General Policy"). This policy provides a framework on a general level, going beyond persons of concern and outlining particular standards, responsibilities of UNHCR staff, and mechanisms for data subjects to exercise their rights regarding personal data protection.

---

[6] According to UNHCR, a person of concern is "[A] person whose protection and assistance needs are of interest to UNHCR. This includes refugees, asylum-seekers, stateless persons, internally displaced persons and returnees." (UNHCR, 2015: 11).

[7] For a detailed description of these principles, see Annex I.

[8] These rights are: 1) Information; 2) Access; 3) Correction and deletion; 4) Objection; 5) Modalities of requests; 6) Recording and response by UNHCR.

This framework is consistent with the UN Principles, considering that the UNHCR Policy on Persons of Concern entered into effect before these. This policy draws from the main aspects of the Policy on Persons of Concern, especially on the data processing principles. It states that it will not replace it; rather, provisions contained in the General Policy should be applied according to the Policy on Persons of Concern when the data in question is the personal data of these people (UNHCR, 2022).

One new aspect that the UNHCR General Policy introduces is a specific provision on emerging technologies like automated decision-making.[9] It says that "UNHCR shall not subject data subjects to automated decision-making where a decision produces adverse legal effects or other significant adverse effects on the interests of the data subject [...]" (UNHCR, 2022: 8). There are three exceptions to this rule: a) when the data subject gives their consent; b) when the automated decision-making is necessary for entering into or performing a contract between UNHCR and the data subject; c) when the automated decision-making is authorized explicitly by a resolution of the General Assembly or other organs in the UN System.

3.1.2. A step further: data responsibility

In recent years, organizations have looked to provide more comprehensive guidelines that unify the existing policies and recommendations on data protection in humanitarian action. One of them is the IASC, created by the UN General Assembly in 1991 and considered the longest-standing and highest-level humanitarian coordination forum of the UN System. It has become a leading player in the humanitarian sector towards AAP and the protection of vulnerable populations from other issues such as sexual exploitation and abuse. The IASC's mission is to establish strategic plans to respond uniquely to humanitarian crises by putting crisis-affected communities at the center of their priorities.

In 2021, IASC published its Operational Guidance on Data Responsibility in Humanitarian Action, revised in 2023. The Operational Guidance establishes that, while each organization doing humanitarian work is responsible for its data, they need common guidance to inform their actions and to uphold a high standard for data responsibility in all response contexts. Therefore, the Guidance gathers and complements existing guidelines and policies from these organizations on data responsibility (IASC, 2023).

[9] According to the European Commission's Directorate for Communications Networks, Content and Technology, automated decision-making is "[a] software system – including its testing, training and input data, as well as associated governance processes – that, autonomously or with human involvement, takes decisions or applies measures relating to social or physical systems on the basis of personal or non-personal data, with impacts either at the individual or collective level" (European Commission's Directorate-General for Communications Networks, Content and Technology, 2018: 5).

As mentioned above, the Operational Guidance refers to data responsibility instead of data protection and understands it as a more comprehensive concept in humanitarian activities: “data responsibility in humanitarian action is the safe, ethical and effective management of personal and non-personal data for operational response, in accordance with established frameworks for personal data protection” (IASC, 2023: 9).

This definition offers a differentiation between data protection and data security as related concepts contained within data responsibility. On one hand, data protection is “the systematic application of a set of institutional, technical and physical safeguards that preserve the right to privacy with respect to the processing of personal data and uphold the rights of data subjects” (IASC, 2023: 9).

On the other hand, data security is “applicable to both personal and non-personal data, [and] refers to physical, technical and procedural measures that aim to safeguard the confidentiality, availability, and integrity of data” (IASC, 2023: 9). These two aspects of operational data management[10] are integral to data responsibility and should be understood as working simultaneously. It is worth noting that this definition of data protection draws from the one in the IOM Manual.

The Guidance also provides more comprehensive definitions of the concepts mentioned in the policies above. For example, unlike these, it defines non-personal data as:

> “*Any information that does not relate to a data subject. Non-personal data can be categorized in terms of its original nature: data that has never related to a data subject [...] or data that was initially personal data but later rendered anonymous [...]*” (IASC, 2023: 10).

The IASC Operational Guidance states that both personal and non-personal data can be sensitive, the level of sensitivity depends on the context of the humanitarian action being carried out, and it may change over time. Sensitive data is data that, if accessed or disclosed without proper authorization, may cause harm to an individual or impact a humanitarian organization’s capacity to carry out its activities or its public perception (IASC, 2023).

The Operational Guidance provides 12 principles for data responsibility in humanitarian action.[11] These principles gather the ones in the policies mentioned above and outline a

[10] According to the IASC Operational Guidance, operational data management refers to “the ensemble of data management activities for operational response, including the design of activities and their subsequent execution, including the collection or receipt, storage, quality assurance, analysis, sharing, use, retention and destruction of data and information by humanitarian actors.” (IASC, 2023: 10).

[11] For a detailed description of these principles, see Annex I.

more integral framework that considers the commitment of “Do No Harm”[12] and puts affected populations at the center of data management in humanitarian action (IASC, 2023). The Guidance also says that IOs with privileges and immunities not obliged to comply with domestic data protection legislation should follow their policies. In the case of the UN System, it mentions the UN Principles as a foundational framework for these organizations.

The IASC Operational Guidance also references the rights of data subjects recognized in the UNHCR Policy on Persons of Concern:

> “*Humanitarian organizations should uphold data subjects’ rights to be informed, in an easily accessible and appropriate manner, about the processing of their personal data, to be able to request to access, correct, delete, object to or request information about the processing of their personal data, and to not be subject to automated decision-making except under the specific conditions set out in the legal frameworks applicable to an organization.*” (IASC, 2023: 18)

3.1.3. Applicability of domestic legal frameworks on data protection to international organizations

The previous analysis shows that one aspect in common among IOs is the recognition of the privileges and immunities they have when articulating their data protection frameworks to those of the countries where they operate. This status originates from the 1946 Convention on the Privileges and Immunities of the United Nations - hereby referred to as the 1946 Convention -, which means they are not obliged to comply with domestic legislation and cannot be subjected to its jurisdiction (United Nations General Assembly, 1946). The status of IOs regarding data protection has been debated over recent years, especially after the emergence of different national and regional legislation on data protection.

The data protection policies of IOs state that the reason for these privileges and immunities is to guarantee that they can fulfill their mandate independently and without interference from state interests. This is especially relevant in the case of IOs’ immunity from jurisdiction, which seeks to prevent them from being subjected to external pressures by states through their judiciary bodies. Hence, domestic data protection laws are incompatible with this immunity.

[12] According to the IASC, “Do No Harm” in the context of the Operational Guidance must be understood as follows: “Data management in humanitarian response should not cause or exacerbate risk for affected people and communities, host communities, humanitarian personnel or other stakeholders, neither through actions nor omissions.” (IASC, 2023: 16).

Some experts in the field, like Marelli (2023), have argued in favor of this view, mentioning three reasons IOs should have such privileges and immunities. First, because of their mandate's nature under public international law, IOs operate in many states, making it burdensome for them to apply the data protection legislation of each one. This is highlighted by the fact that legal structures and cultures vary globally and may be conflicting between them.

Second, IOs must maintain independence for data flows to operate efficiently across borders to guarantee a single regulatory framework overseeing data protection. Third, domestic legal frameworks are designed to be enforced by local judicial authorities with the power to investigate and impose sanctions that, if applied to an IO, would interfere with the independence its privileges and immunities provide.

Other experts, like Kuner (2019), have argued that there may be instances where IOs are bound by domestic law. For example, in the case of the European Union (EU), they note that there are no international agreements dealing with these privileges and immunities under EU law, and the general rule for this relationship is framed under host agreements between a Member State and an IO, such as the headquarters agreement between the Netherlands and the International Criminal Court and the International Court of Justice. These agreements usually mention that, without prejudice to privileges and immunities, all persons within them must respect the host state's laws. Furthermore, the EU is not a party to the 1946 Convention, and this relationship has been rather informal and not mentioned in formal agreements or treaties.

Here, the EU's General Data Protection Regulation (GDPR), which entered into effect in 2018, is worthy of note. The GDPR recognizes certain instances for allowing free international data transfers from IOs in humanitarian situations. Persons and organizations collecting personal data in the EU must have a lawful basis for processing it, including consent from data subjects (which should be free, specific, unambiguous, and informed), legal obligations, vital interests, the achievement of a mission of public interest, and when exercising public authority.

In this regard, Recital 46 establishes that humanitarian actions carried out by organizations fall under the requirement of achieving a mission of public interest. Furthermore, Recital 112 states that all personal data transfers from individuals who are physically or legally incapable of providing consent to IOs performing humanitarian activities to achieve a task incumbent under the Geneva Conventions or other regulations of international humanitarian law also fall under this case (European Union, 2018).

This is an ongoing debate that ought to be considered by IOs when it comes to applying their data protection policies in humanitarian activities, especially when emerging technologies are being implemented to enhance and facilitate data management.

3.2. Effects of artificial intelligence on accountability to affected populations

3.2.1. What is accountability to affected populations?

IOM describes AAP as “an active commitment by humanitarian actors to use power responsibly by taking account of, giving account to, and being held to account by the people they seek to assist” (IOM, 2020: 2). Other IOs, such as the UNHCR or the UN Office for the Coordination of Humanitarian Affairs (OCHA), have similarly defined this concept. However, AAP should not be seen only as a concept, but rather as an approach in humanitarian work, characterized by the willingness to be inclusive and to put the individual concerned at the center of the design process of humanitarian development projects. In other words, it promotes an affected-population-centric vision.

In this regard, the International Committee of the Red Cross (ICRC) states that “accountability to affected people is an approach that reduces the opportunities for this power asymmetry to be exploited and ensures humanitarian programs are relevant, inclusive, and accessible to those most marginalized” (ICRC, 2018). By being affected-population-centered, this approach underlines two elements. First, it implies that humanitarian project goals are to target and respond precisely to the needs of affected populations while preserving their rights and dignity. Second, it calls for the necessity of empowering affected populations through their participation in the decision-making process. Furthermore, it distinguishes two forms of agency: the affected populations and people willing to help (Al-Sharif, 2020).

Having begun to emerge in the 1990s, this is a somewhat recent concept. The adoption of the Code of Conduct for Humanitarian Agencies in 1994 (Hilhorst et al., 2021) is notable. Furthermore, from the 2000s onwards, many initiatives have appeared dealing with AAP and its ethical considerations. This notion became a dominant approach in 2014 with the publication of the Core Humanitarian Standard on Quality and Accountability report, in which more than 200 humanitarian actors (academia, governments, non-governmental organizations, United Nations officials, stakeholders, and so on) affirmed, through nine commitments, the use of an accountable approach based on “high-quality humanitarian

action that places respect for the fundamental rights of affected populations at the center" (Heintze and Thielbörger, 2018: 410).

To ensure that the AAP approach is embedded in each humanitarian project, several frameworks have been proposed to assess whether a project truly meets the needs of the populations while respecting their rights and dignity, as well as including them in the process. IOM defines five key criteria to guarantee the AAP approach, namely: 1) Leadership; 2) Information-sharing and transparency; 3) Participation; 4) Complaints and feedback mechanism; and 5) Partner coordination.

Similarly, the IASC has also developed a framework composed of four key commitments. The AAP approach targets all types of populations considered affected, such as vulnerable or disabled people. It includes, among others, women, children, the elderly, ethnic and religious minorities, and those sexually exploited and abused.

3.2.2. Frameworks for the ethical use of artificial intelligence

As of the writing of this paper, there are no internationally legally binding instruments regulating good practices regarding AI, which is why this section will focus on the existing frameworks and recommendations for the ethical use of AI. However, it is worth noting that on March 13th, 2024, the European Parliament adopted the AI Act, which will enter into force 24 months after its adoption. Although it is on a regional scale, it is the first legally binding regulatory framework on AI and is based on the banning and permitting of certain uses of AI depending on previous risk assessments and conformity to other EU legislation (Madiega, 2023).

Regarding non-legally binding frameworks, the most relevant one currently in place is the United Nations Educational, Scientific, and Cultural Organization's (UNESCO) 2021 "Recommendation on the Ethics of Artificial Intelligence". This is a recommendation addressed to the UNESCO Member States as actors and authorities responsible for developing and implementing legal and policy frameworks on the ethical use of AI and has been adopted by all 193 Member States, putting it at the forefront of ethical AI guidelines. Its objectives are to reduce the risks posed by the use of AI in a myriad of aspects, including data protection, while highlighting the positive opportunities it presents.

The text recommends guiding action through a set of values and principles, including the respect of human rights, fundamental freedoms and human dignity, proportionality, the right to privacy and data protection, human oversight and determination, adaptive governance, and awareness and literacy (UNESCO, 2022). Other IOs, such as the World Health

Organization (WHO), have proposed a similar set of principles to regulate the use of AI after having identified them as the most commonly used (WHO, 2021).

As stated above, the EU is currently at the forefront of developing legally binding instruments on the use of AI and has maintained a policy of encouraging its member states to use this technology (European Union, 2023). In parallel, various EU institutions have published ethical guidelines and frameworks on the use of AI. In a report by the European Commission, an independent group of experts recommended aiming policy toward "trustworthy AI", which means that its ethical purpose is not challenged by ensuring respect for fundamental rights and other applicable regulations, principles, and values; and maintaining its technical robustness and reliability to ensure no unintentional harm is caused.

The report found that AI should be human-centric, especially when vulnerable groups are concerned, continuously evaluating any possible effects on human beings and the common good. Also, AI should incorporate requirements such as accountability, data governance, design for all, human oversight, non-discrimination, respect for human autonomy, respect for privacy, robustness, safety, and transparency from the earliest design phase possible (European Commission, 2019).

The European Parliament has also produced a framework on the ethical aspects of AI, robotics, and related technologies. This framework stands out for its positive view of AI, encouraging a common approach amongst EU Member States on the topic of AI ethics as a way to promote job creation and economic opportunity. The main concern is what has been called the "soft nature of AI" (Evas, 2020: 20), referring to the difficulties in monitoring AI and the lack of enforceability in its guiding principles. For this reason, legislation at the EU level to establish a common ground for all Member States is encouraged. The importance of the existence of a body that can protect the public interest and promote social responsibility by private corporations is also highlighted.

Beyond IOs, the ethical considerations of AI and its relation to data collection and processing have been widely discussed by research centers on all kinds of specialized topics, from healthcare to agriculture (Noor and Manantan, 2022). These reports tend to also focus more on the risks posed by AI than on the possibilities the use of this technology opens, and propose a set of principles and values to reduce said risks. These principles and values, similar to those found in the frameworks produced by IOs, revolve around concepts of fundamental freedoms, human dignity, equality, and personal data protection (Cataleta, 2020).

Although all the studied frameworks on the ethical use of AI have commonalities in the sets of principles and values they propose to minimize risks, they all have an important setback: the lack of assessment and enforceability mechanisms that ensure the responsible and ethical use of AI.

3.2.3. Artificial intelligence applied to the humanitarian field

The term “AI” has many definitions, mostly depending on the sector in which it aims to be used. The notion of AI, as it is known today, was born in the 1950s, following several conference cycles focusing on the topic of computational science. At the time, AI was considered a simple theory according to which human intelligence could be described so precisely that a machine could reproduce it (Helm et al., 2020). In the following decades, some predicted that, in the 21st century, AI would replace scientists like physicians (Maxmen, 1977).

Although alarmist, this prediction is an example of the two opposing visions of AI. On the one hand, people like Maxmen (1977) offer a rather pessimistic view of this technology as a synonym for dystopia and go as far as saying that it is an existential threat to humanity. On the other hand, some look at this technology from an optimistic angle, believing that it can bring new professions and economic growth based on rational and intelligent choices (Bini, 2018).

Concerning migration, IOM takes a more balanced view of the technology. It presents AI and other similar technologies as tools with real leverage to “revolutionize” the migration process in a positive way. For example, it can help in administrative and decision-making processes, such as speeding up visa and asylum requests or identifying and tracking migration flows to facilitate the provision of humanitarian assistance (Pizzi, 2020).

However, the organization also warns that this technology is not neutral and can cause substantial harm if misused or not properly controlled (IOM, 2022). AI has increasingly been presented as a potential threat since revelations indicate that certain states may have used this digital tool for surveillance purposes, and concerns have arisen about the right to privacy of migrants, as well as how sensitive personal information is stored, accessed, and shared (IOM, 2022).

It is therefore crucial to be aware of who is using these technologies and for what purposes. IOM maintains that the “Do No Harm” principle, explained above, must be respected at all times throughout the migration process when using AI (IOM, 2022). Following this neutral approach, the definition retained for this paper is the broad one established in the latest

World Migration Report: “the programming of computers to do tasks that would normally require human intelligence” (IOM, 2022: 282).

Recently, many IOs, including IOM, have started to explore AAP and data responsibility as ways to improve their humanitarian response concerning AI. For example, in its latest World Migration Report, IOM presents AI as a source of discrimination and exclusion through the amplification and institutionalization of human biases. Serious concerns are therefore raised regarding the sensitivity of affected populations' data.

However, the report mentions that AI should not be perceived only as dangerous and unsafe, highlighting the valuable assistance it could bring, provided that it meets a certain number of criteria, in particular those defined in the AAP approach (IOM, 2022). In this regard, studies have shown that the use of AI in the collection of large amounts of data can significantly help disaster risk management (Soden et al., 2021).

3.3. Artificial intelligence and accountability to affected populations: the case of biometric data

3.3.1. Biometric data for delivering humanitarian assistance

Developments in humanitarian action have been closely linked to those in migration management. Efforts such as resettlement schemes and humanitarian visas are examples of this relationship and how it opens a space for data flows between these two sectors (Tsui et al., 2023). As humanitarian emergencies have risen, the need to establish a safe and efficient way to collect beneficiary data has also increased. Amidst new and emerging technologies, biometrics have surged as a widely used tool for identifying and verifying beneficiaries and ensuring that aid reaches those who need it most.

Biometric data can be defined as the “personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data” (European Commission, 2016). IOM defines a biometric characteristic as “a biological and behavioral characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition” (IOM, 2018a: 2). The purpose of the collection of biometric data is usually to ensure the correct identification or authentication of a physical person (Innovatrics, 2024).

On identification, biometrics offer a one-to-many authentication, meaning that, in a presented sample, there is a search and contrast exercise with several biometric profiles stored in a centralized database. As for verification, biometrics offer a one-to-one authentication, which means using the presented sample to check whether it is identical to the stored template. These functionalities allow humanitarian organizations to perform many activities, like registration for services provision, repatriation, and food distribution. Hence, “with biometrics, [humanitarian organizations] can not only run [a] deduplication to eliminate redundant data and identify targeted beneficiaries, but they can also verify whether beneficiaries are entitled to claim several types of assistance” (Açıkyıldız, 2023, para. 7).

IOs that are part of the UN System, like IOM, UNHCR, and the World Food Programme (WFP) have also argued that biometrics have helped deploy digital identities for affected populations who have been historically marginalized. For them, digital identity plays an important role in achieving legal identity, as set out in the Sustainable Development Goals. For this, IOs have partnered with private companies, which have increasingly aligned with the humanitarian sector in the past decade (Tsui et al., 2023).

These partnerships bring a relevant matter to light: data sharing. Beneficiary data collected by these organizations can also be processed by service providers, partner organizations, and government agencies when they lack the institutional capacity to perform these tasks by themselves. IOs argue that data sharing can help guarantee operational continuity where provision and access to assistance are difficult to achieve. This process can be done by performing data transfers (a copy of a dataset is sent to the partner) or granting direct third-party access to a database (Açıkyıldız, 2023).

In this area, WFP is playing a key role. To collect beneficiary data and guarantee access to supplies in areas affected by humanitarian crises producing famine and food shortages, WPF uses SCOPE, a digital beneficiary and transfer management system compatible with iris scans, fingerprints, and photographs. SCOPE stores these data in a centralized database, allowing for the expedition of ration cards with unique identity numbers for each beneficiary. SCOPE is considered the largest database of humanitarian assistance, with almost 63.8 million identities registered by the end of 2020 (Tsui et al., 2023), which is why many other IOs doing humanitarian work seek to partner with it.

For example, WFP and UNHCR signed, in 2018, an Addendum on Data Sharing to their 2011 Memorandum of Understanding, where they established the interoperability of SCOPE and UNHCR’s BIMS (UNHCR and WFP, 2018). Through this partnership, WFP’s e-voucher program is integrated with BIMS to keep an up-to-date account of beneficiary data. WFP

also signed an agreement with IOM in 2018 to exchange biometric data for humanitarian assistance, allowing for interoperability between SCOPE and the IOM's Biometrics Registration and Verification System (BRaVE) (IOM, 2018b).

Biometrics in the humanitarian sector have also expanded to organizations outside the UN System. The ICRC stands out as one of the largest humanitarian organizations with a policy specific to regulating biometrics in its operations. In its Policy on the Processing of Biometric Data (referred to as "the Policy" from now on), the ICRC restricts one-to-many authentication processes, like storing centralized databases of living people. Instead, the Policy highlights using token-based verification as the most appropriate way to provide humanitarian assistance.

The Policy also allows partners and service providers to collect biometric data on behalf of the ICRC as long as they abide by its standards. Among the conditions necessary for this data sharing, the Policy mentions the fulfillment of a humanitarian obligation, the execution of a Data Protection Impact Assessment (DPIA), the vital interest of the data subject, a written commitment from the recipient to use the data for humanitarian purposes, and the informed consent of the data subject. Finally, the Policy has several data protection measures, like data minimization, encryption, audit trails, and the encoding of biometric images. In this sense, data subjects have a right to access their data and request its correction or deletion (ICRC, 2019a).

3.3.2. Interplay with artificial intelligence

The growing use of biometrics in humanitarian assistance has opened up the space for its integration with other new and emerging technologies. In this sense, AI has been garnering attention in recent years for its possibility to create interoperability between biometric technologies and AI-based analysis for operationalizing the collection and processing of biometric data, especially from affected populations whose data is difficult to collect because of inherent vulnerabilities. For example, AI could be useful for analyzing physiological biometrics, like patterns in earlobes, and behavioral biometrics, like speech patterns (Bither and Ziebarth, 2020).

The deployment of AI by IOs conducting humanitarian work is still nascent, but some have started to use it for processing biometric data. In this regard, partnerships with private companies have been crucial. For example, UNHCR partnered with Accenture to develop its identity management system (Accenture, 2015). UNHCR registration tools are housed under the Population Registration and Identity Management Eco-System (PRIMES), which

includes different repositories of biometric data for identity management, documentation provision, and humanitarian assistance (UNHCR, 2018a).

As part of PRIMES, BIMS has interoperability with Accenture's Unique Identity Service Platform (UISP), which works by analyzing an individual's ten fingerprints and two irises and builds a biometric record available for storing in BIMS. Part of UISP works with the Biometric Matching Engine, a software that uses AI to compare these biometric identifiers and creates a unique identification process that makes faster and more accurate the matching of existing records in databases.

This process allows BIMS to pair the biometric data with other records like address and profession and stores these combined data in a centralized database (Nalbandian, 2022). After this verification, UNHCR issues an identity card compatible with local identification systems, allowing beneficiaries to access services like cash-based transfers and apply for protection or resettlement. Here, BIMS allows one-to-one and one-to-many authentication. UNHCR also collaborates with third parties when collecting and sharing these data (Açıkyıldız, 2023).

Another example is ICRC, which has the Restoring Family Links Programme. Here, affected populations looking for missing relatives provide the ICRC with their photographs, which are run through a database. Then, an AI-based algorithm completes the search using facial recognition and performs automatic searches and matches. The database can be accessed through a website called Trace the Face (ICRC, 2019b). This program is the only exception the ICRC has on the restriction of using biometric data for a one-to-many authentication. It is worth noting that the ICRC implements this technology autonomously, as it does not rely on partnerships for performing facial recognition (Açıkyıldız, 2023).

Finally, regarding IOM, there is no evidence found that it is implementing AI for enhancing biometric data collection and processing in humanitarian settings. Nevertheless, it is worth noting that the Organization is interested in this interplay. For example, IOM launched the Data Innovation Directory in 2020, a platform within its Migration Data Portal containing information on initiatives seeking to better understand and educate on migration in emergency contexts using different technologies, like AI, satellite imagery, and machine learning (Bither and Ziebarth, 2020).

To ensure the safe use of AI, IOs and academics have tried to elaborate on frameworks and recommendations. For example, the approach of participatory AI "refers to the involvement of a wider range of stakeholders than just technology developers in the creation of an AI

system, model, tool, or application. As a field, it sits within the broader category of participatory design of technology" (Berditchevskaia et al., 2021). Although there are still few examples using this approach to assess its effectiveness, the first results have shown that it could be a promising approach for the humanitarian sector.

3.3.3. Risks and concerns

Humanitarian organizations recognize that, just as biometrics can provide many advantages in making humanitarian assistance more effective, they can pose some risks. According to a report by the non-profit organization The Engine Room on the use of biometrics in humanitarian action:

> "*The growing overlap between the two parallel sectors renders the biometric data of people on the move even more sensitive than before, and adds a layer of complexity for humanitarian organisations engaged in data exchanges with national authorities who enforce asylum and migration systems.*" (Tsui et al., 2023)

Another concern revolves around one-to-many authentication and the centralization of biometric data, especially regarding data security. The possibility of discrimination against vulnerable populations is also of concern, as matching algorithms - like those built through machine learning - tend to underperform when collecting biometric data from marginalized groups due to inherent human biases (Açıkyıldız, 2023). Furthermore, this centralization for data sharing can lead to the exclusion of local and grassroots organizations in humanitarian efforts. This situation, in which larger organizations collect biometric data and smaller ones deliver services, poses difficulties in ensuring AAP (Tsui et al., 2023).

It has also been pointed out that since biometric data is unique to each individual and cannot be changed, it is increasingly being used for surveillance and monitoring purposes, which can put vulnerable populations like migrants and refugees at greater risk, especially if their data is shared with government authorities. In this sense, partnerships with private companies for processing and storing biometric data are of particular concern since the data privacy of affected populations may not be one of their priorities. A lack of communication between a humanitarian organization and a private company on this aspect can lead to the endangerment of beneficiaries. In the case of migrants and refugees, it can lead to discrimination, involuntary resettlement or repatriation, and persecution (Holloway et al., 2021).

Lastly, another issue is that there does not seem to be an agreement between IOs on the risks of biometrics. These organizations seem to be on the same page about the desire to

use biometrics - and new and emerging technologies in general - to enhance humanitarian action. Nevertheless, there are differences in understanding the risks biometrics can pose and how they should be regulated. This lack of consensus on the responsible use of biometric technologies can lead to inefficient implementation (Tsui et al., 2023).

3.4. Key takeaways

From this literature review it can be concluded that data responsibility and data protection are of concern for IOs working in humanitarian action, which can be seen in their data policies and guidelines. All of these provisions are guided by similar principles, especially regarding accountability to the data subjects, data security, transparency, confidentiality, necessity and proportionality, data minimization, and the lawfulness and fairness of the collection of personal data.

Most of them also recognize the rights of data subjects regarding processing of their data, and some acknowledge the role new and emerging technologies play in changing the landscape. Some of these policies also mention the importance of guaranteeing that automated decision-making does not negatively impact data subjects. Therefore, the use of AI in humanitarian action must consider these principles and guidelines at the core of its design and implementation.

However, there are gaps in the application of data responsibility and data protection. One of them is the lack of consensus among IOs on understanding if they should refer to one concept or the other. While the policies and guidelines mentioned above establish personal data protection as the goal to achieve in data management, the IASC Operational Guidance establishes it as an important element for achieving the goal of data management in humanitarian action, which is data responsibility.

Also, there are differing views on what data falls under these practices. On one hand, the IOs talking about data protection do not consider that non-personal data should fall under their policies because it is not subject to being sensitive. On the other hand, the IASC Operational Guidance recognizes that non-personal data can become sensitive in specific emergencies and fragile situations.

On the privileges and immunities of IOs, they will likely continue to argue for them, especially if they are carrying out humanitarian activities. Nevertheless, IOs can look at legislation such as the GDPR to enhance their policies and design and implement them in a way that harmonizes the provisions set out in this type of legal framework. Furthermore, there is no current legal framework focusing on the use of AI and its relationship with AAP. However,

this should be a crucial aspect of any data responsibility to be adopted by humanitarian IOs working directly with affected populations.

On the use of biometric data, data-sharing practices between IOs and private companies significantly ease the management of this data. However, they also pose risks due to its sensitivity. A wider circulation of biometric data increases the chances of it being treated by actors whose primary concern is not the privacy of affected populations, and of it being used for monitoring and surveillance purposes instead of delivering humanitarian assistance.

Finally, another point to be highlighted is the increasing importance that IOs have placed on putting affected populations at the center of any humanitarian project to ensure their needs are met. In this regard, several IOs such as IOM have publicly shared approaches and frameworks allowing any humanitarian organization to rely on them to assess whether their activities meet the needs of populations affected with effectiveness while ensuring their rights, protection, and dignity.

Although there are several existing frameworks and recommendations on the safe and ethical use of AI, they are not overly concerned with its use in the humanitarian field and its intersection with the management of biometric data. However, it is worth noting that the consensus seems to point once more to a human-centric approach.

4. Case studies

4.1. Biometrics in protracted migration movements: the case of the Rohingya people in Bangladesh

4.1.1. Origin of the refugee crisis and current humanitarian situation

The Rohingya people are a Muslim ethnic minority group who have for centuries resided in predominantly Buddhist Myanmar. Over a million Rohingya people are estimated to have fled since the 1990s to neighboring Bangladesh after different waves of violence faced in their home country (UNHCR, 2023). The latest wave of violence began in August 2017, when the Myanmar armed forces perpetrated several violent attacks against the Rohingya people, amounting to what some specialized organizations, including Human Rights Watch (HRW), have qualified as genocide. The UN has described the Rohingya people as the most discriminated against minority on the planet due to, amongst other reasons, being denied Myanmar citizenship under the country's law (HRW, 2022).

Being rendered stateless has left the Rohingya population in a specially vulnerable position. The majority of refugees, over 50% of whom are women and children, now live in camps in Cox Bazar, Bangladesh, which are administered jointly by UNHCR and the Bangladeshi government. Rohingya refugees make up a third of the population in this Bangladeshi region, making cooperation with the local population essential to ensure a satisfactory quality of life. Refugees in this area are also especially vulnerable to natural circumstances such as the monsoon season, because their dwellings are not sufficiently prepared for harsh conditions (UNHCR, 2023b).

Life in refugee camps in Bangladesh has not amounted to a significant amelioration of the Rohingya people's quality of life. The Bangladeshi government has set restrictions on their livelihoods, education, and mobility, among other aspects, thus perpetuating their vulnerability. Furthermore, Bangladesh has attempted repatriation of refugees to Myanmar on several occasions, even though return conditions have been deemed unacceptable by the UN High Commissioner for Human Rights. Lack of funding remains a crucial issue: while several Joint Response Plans have been agreed upon by humanitarian agencies and other partners, their target funding has never been reached (HRW, 2022).

The international community's response to the ongoing crisis has been varied. Experts consider that a United Nations Security Council (UNSC) resolution establishing an arms embargo on Myanmar would be effective; however, the prediction of a Russian and/or Chinese veto has rendered the UNSC inactive. Meanwhile, the targeting of civilians by the Myanmar junta continues to this day (HRW, 2022).

4.1.2. Use of biometric data and AI in Rohingya refugee camps

Collection of biometric data in Rohingya refugee camps has been carried out by UNHCR and Bangladeshi authorities to facilitate the distribution of humanitarian assistance. The data collected is used to create personalized cards, which, for many of these stateless people, represented receiving an ID card for the first time in their lives. Said cards state that Myanmar is the country of origin of the refugees.

To collect data, UNHCR's BIMS was used, recording fingerprints, iris scans, and other relevant personal information such as family relations. When using ID cards to access humanitarian assistance, verification of the collected data is done through the Global

Distribution Tool (GDT)[13], used mainly to speed up distributions and avoid fraud (UNHCR, 2019).

The collection and use of biometric data by UNHCR in partnership with the Bangladeshi government has been widely criticized. In some cases, the GDT failed to recognize fingerprints, leaving some refugees without access to food (Amnesty International, 2020). Most importantly, UNHCR did not carry out a data impact assessment before the collection and handling of biometric data, allowing the Bangladeshi government to send the information collected in ID cards to the Myanmar government for repatriation purposes, even though repatriation is not a safe option for Rohingya refugees (Hersey, 2021).

Consent in data collection has also been pointed out as an area for improvement. A study reported that most refugees interviewed were told by UNHCR workers that providing data was obligatory to access aid. Only a very small percentage were told afterward that their data might be used for repatriation purposes, and some reported seeing the box that signals consent for this specific use ticked on the printed receipt they were given, even if they had not been explicitly asked before.

Furthermore, language barriers were an issue, as printed receipts were in English and the vast majority of Rohingya refugees do not speak this language. 21 people reported having gone into hiding after learning their names had been added to repatriation lists, with over half of them having been added to these lists based on data collected in refugee camps (Hersey, 2021).

4.2. Biometrics in protracted migration movements: the case of South Sudan

4.2.1. Origin of the refugee crisis and current humanitarian situation

The origin of the South Sudan humanitarian crisis dates back to the colonial presence of the British empire and Egypt in Sudan since 1899. The imposition of an Islamic cultural model in the north, due to its proximity to Egypt, and a Christian one in the south, which was under English supervision (Rodríguez Gómez, 2023) leading to ethnic and religious disputes resulting in the first civil war (1955-1972) after Sudan's independence in 1956. These led to the 1972 Addis Ababa Accords recognizing the Southern Sudan Autonomous Region.

[13] The GDT is one of UNHCR's PRIMES tools, used at points of distribution with the purpose of identity management and assistance tracking. It draws data directly from the UNHCR's PRIMES biometrics portfolio (UNHCR, 2018b), and matches it to the data of the refugee population present at the distribution site.

However, the imposition of several islamic laws, such as the extension of Muslim law to criminal law (Bleuchot, 1990) went against the greater autonomy given to the southern region and resulted in a second civil war (1983-2005). The latter led to a referendum recognizing South Sudan as an independent republic in 2011. Yet, this historic act has brought, to date, neither peace nor political stability, causing the population to suffer the full brunt of the repercussions. The multiple internal conflicts created 1.5 million IDPs (ICRC, 2021). Given the growing demand for emergency assistance, many international actors have mobilized in what is called a humanitarian crisis.

For example, OCHA has developed a response plan to humanitarian needs, with the objective to help six million vulnerable people (women, children, elderly, disabled) among the nine million people in need. The main needs are food security and livelihoods; health; water, sanitation, and hygiene (OCHA, 2023). In addition to these vital needs, climate risks must be taken into account in humanitarian intervention plans, as South Sudan is considered the second most vulnerable country to natural hazards (European Commission, 2024).

OCHA indicates that its response plan is based on the AAP approach, considering that the opinion of affected people is paramount in the decision-making processes. In addition, OCHA supervises the South Sudan Humanitarian Fund (OCHA, 2024), made available to allow international actors to finance humanitarian assistance. Ultimately, the majority of cooperation between stakeholders occurs in PoC sites, built by the UN and protected by soldiers of the UN Mission in South Sudan (UNMISS). Among the actors involved, IOM is in charge of registering IDPs who wish to enter the PoC. Given the increasing number of registration requests, the organization has resorted to the use of biometrics to be able to process the massive amounts of data.

4.2.2. Use of biometric data and AI in South Sudan

IOM has developed the DTM, a platform bringing together various up-to-date information (ad-hoc surveys, headcounts, mapping exercises, etc.) in order to improve each phase of the assistance (preparation, intervention, and recovery) (IOM, 2023b). Moreover, IOM explicitly mentions that registration procedures are developed in close cooperation with IDPs in PoCs, to ensure community inclusion and awareness of data collection. In other words, the AAP approach is integrated into the use of DTM.

DTM uses BRaVE in its methodology for the registration process of new arrivals in refugee sites to accurately identify the number and type of people present in these sites. Through the collection of the name, birthdate, or gender, and its beneficiary data management, BRaVE

contributes to the effectiveness of humanitarian response by more easily targeting the required needs of refugees. Following the organization's data protection principles (IOM, 2009), the UN house sites in South Sudan were the first pilot case for the use of BRaVE in the registration process in 2014.

As part of the constant evaluation of DTM, reports and satisfaction surveys are produced regularly on UN sites. For example, a report on the concrete use of biometric registration in the Malakal PoC site published in December 2021 shares statistics from the data collected, such as the number of men and women, adults and minors, with family or alone (IOM, 2021). In addition to creating a profile and issuing a personal plastic card to new arrivals, biometric data also makes it possible to verify the information of a person who has lost their card to give them a new one, which acts as an ID document (IOM, 2023a).

Overall, the use of biometric data by IOM in South Sudan brought positive results such as valuable benefits of speeding the process, and helping IOs deliver better and more effective assistance (Jacobsen, 2017). Moreover, the vast majority of people directly confronting biometric registration seem satisfied with the way the data is managed (91.2%), according to the Biometric Registration Services Beneficiary Satisfaction Survey. Only a few isolated incidents occurred during aid distributions due to lost or discarded cards (2% of the people surveyed).

Another criticism reported by a minority of affected people is the need for more information about the registration process such as the purpose of recording and data security (IOM 2021b). Otherwise, the only remarks observed are warnings on the ethical, clear, and secure processing of data, following the various frameworks and principles defined by the organization (Freeman, 2023). However, although reports published online describe how DTM uses biometric technology, no information can be found publicly on the use of AI in South Sudan.

5. Interview analysis

All interviewees mentioned that IOM does not have a specific data responsibility policy, using instead that of the IASC, though it is working on an updated data protection policy. They also pointed out that the organization does not currently use AI in its field operations. Skepticism on the potential use of this technology in the humanitarian work carried out by IOM varied, although interviewees generally recognized its potential for good under properly supervised use. Furthermore, all interviewees agreed on the importance of data security and privacy, as well as acting under principles such as purpose and necessity. They also highlighted the

necessity of carrying out risk assessments before using biometric data to minimize risks of it ending up being used for harmful purposes.

When asked about the potential importance of having a legally binding framework for the use of AI in humanitarian work, interviewees' responses varied greatly. Some believe that binding instruments are not suitable in the context of IOs, and therefore each organization should practice self-governance, relying on inter-agency guidelines when needed. Others expressed optimism at the prospect of there being a binding framework, highlighting the need for increased accountability concerning IOs' work and proposing the creation of a supra-organizational monitoring body to ensure it. Lastly, while still giving a general positive answer to the question, others pointed out that achieving consensus amongst IOs and other economic stakeholders to create said binding agreement would be extremely difficult, and therefore not a very feasible option.

On the use of technology to improve and ensure the AAP approach is respected, interviewees highlighted the importance of focusing on the intersection between the use of technology and the AAP process itself, rather than falling into the erroneous idea that technology can be used as a one-size-fits-all solution. They also recognized that technological biases are present in the use of biometric data, and pose a significant risk to the ethical use of new technologies. Therefore, they highlighted the need to have a cautious approach to their use and to ensure that biases are minimized.

On the responsible use of biometric data, they pointed to the need for data deletion once it has been used for its well-defined purpose. The relevance of ensuring informed consent is received from the affected populations was also brought up, as was the necessity of facilitating the communication of feedback and complaints. Other principles of data protection and responsibility, such as confidentiality, security, and inclusivity, were also repeatedly mentioned.

Finally, one aspect that appeared in the interviews that had yet to be previously addressed in the research was the importance of having data-sharing agreements between IOs and other partners, be it private companies or governments. The importance of achieving said agreements before sharing sensitive information and assessing the risk of doing so was another point raised.

6. Conclusions

The objective of this research paper was to determine how the power of AI can be harnessed to ensure its ethical and responsible use within the AAP approach and data responsibility in the humanitarian sector, with a special focus on the use of biometric data by IOM and other IOs. With this in mind, this research paper has come up with a series of recommendations, which can be found in the executive summary, to ensure that it can help enhance AAP, instead of putting vulnerable populations further at risk.

As has been established, the use of biometrics in the delivery of humanitarian aid is not new, but its success has been varied. The lessons to be learned from the use of biometrics in the two selected case studies are intrinsically linked to questions of privacy, data protection, and ethical commitments of IOs. Given the personal nature of this data, what can be used to enhance effectiveness and accuracy in delivering assistance can pose serious threats to vulnerable populations if mishandled, including discrimination, involuntary resettlement, and persecution. The sharing of biometric data with governments and/or private actors not bound by the same ethical commitments as IOs is especially worrying, as ensuring its safe use and holding these actors accountable is often extremely difficult.

Maintaining the AAP approach is especially important when dealing with biometric data. In this regard, ensuring that affected populations retain their rights on all aspects of security, confidentiality, and consent, as well as holding IOs to their obligations to transparency, is essential. The introduction of AI in the humanitarian field has made these commitments even more important, as it is a very new and unregulated technology capable of reproducing harmful biases if not properly supervised. However, AI can also be a tool for good. Among others, its potential to make humanitarian action more efficient and reliable is remarkable.

Maximizing preparedness and capacity of ground teams working directly with affected populations and collecting their biometric data, especially in emergency situations, is essential to ensure good practices are respected. In this regard, capacity-building areas include awareness of all ethical and informed consent considerations at play when carrying out humanitarian work, and optimization of team organization to avoid delaying the deployment of humanitarian assistance due to bureaucratic processes.

7. Limitations and further research

The research carried out in this paper has potential limitations. Without being able to carry out research directly in the field, the data collection on the two case studies relied on other publications and studies, potentially being subject to reproducing biases contained in said publications. Also, having focused on two specific case studies could have made the conclusions and recommendations from the research context-specific. Moreover, all interviewees were professionals working with the same IO. Hence, further research could benefit from having a broader methodological scope and, if possible, including data collected first-hand through a field study.

An area that this study did not go into detail on, and could also be a focal point of further research, are the inherent biases present in AI tools, such as racial biases, which could pose a major risk in its use by humanitarian organizations. Other lines of research could focus on how to detect, overcome, and correct these biases when providing humanitarian action.

Finally, the fast-paced nature of the current technological landscape is a concern to humanitarian IOs. While this research paper has attempted to show how to adapt to it, further research could study how IOs can keep up with technological changes and bear responsibility for future regulations of new developments on biometrics and AI.

References

Accenture. (2015). *United Nations High Commissioner for Refugees and Accenture Deliver Global Biometric Identity Management System to Aid Displaced Persons*. Retrieved from https://newsroom.accenture.com/news/2015/united-nations-high-commissioner-for-refugees-and-accenture-deliver-global-biometric-identity-management-system-to-aid-displaced-persons [last accessed on 04/03/2024].

Açıkyıldız, Ç. (2023) 'I know you like the back of my hand': biometric practices of humanitarian organizations in international aid. *Disasters*, 48(2). Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1111/disa.12612 [last accessed on 07/05/2024].

Al-Sharif, B. F. Z. (2020). *The accountability to affected people practiced by the humanitarian actors while supporting the resilience of the residents of Masafer Yatta from the residents' perspective*. Jerusalem: Al-Quds University. Retrieved from https://dspace.alquds.edu/server/api/core/bitstreams/778b3e07-9348-42ef-93f0-bebc8af7ea43/content [last accessed on 05/12/2023].

Amnesty International. (2020). *Race, borders, and digital Technologies. Submission to the UN Special Rapporteur on contemporary forms of racism, xenophobia and related intolerance.* Retrieved from https://www.ohchr.org/sites/default/files/Documents/Issues/Racism/SR/RaceBordersDigitalTechnologies/Amnesty_International.pdf [last accessed on 14/05/2024].

Berditchevskaia, A. et al. (2021). *Participatory AI for humanitarian innovation: a briefing paper.* London: Nesta. Retrieved from https://media.nesta.org.uk/documents/Nesta_Participatory_AI_for_humanitarian_innovation_Final.pdf [last accessed on 05/12/2023].

Bini, S. A. (2018). Artificial Intelligence, Machine Learning, Deep Learning, and Cognitive Computing: What Do These Terms Mean and How Will They Impact Health Care?. *The Journal of Arthroplasty*, *33*(8), pp. 2358–2361. Retrieved from https://doi.org/10.1016/j.arth.2018.02.067

Bither, J and Ziebarth, A. (2020). *Migration Strategy Group on International Cooperation and Development. AI, digital identities, biometrics, blockchain: A primer on the use of technology in migration management*. Retrieved from https://www.iom.int/resources/ai-digital-identities-biometrics-blockchain-primer-use-technology-migration-management [last accessed on 08/05/2024].

Bleuchot, H. (1990). L'étude du droit musulman: Jalons pour une convergence (entre l'islamologie juridique et l'anthropologie juridique). *Droit et société*, *15*(1), 175–187. https://doi.org/10.3406/dreso.1990.1075

Cataleta, M. S. (2020). *Humane Artificial Intelligence: The Fragility of Human Rights Facing AI*. East-West Center. Retrieved from http://www.jstor.org/stable/resrep25514 [last accessed on 05/12/2023].

European Commission (2016). *Migration and Home Affairs. Glossary: Biometric Data*. Retrieved from https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/biometric-data_en [last accessed on 14/12/2024].

European Commission. (2019). *Independent High-Level Expert Group on Artificial Intelligence. Ethics Guidelines for Trustworthy AI*. Retrieved from https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html [last accessed on 05/12/2023].

European Commission. (2024). *DRMKC - INFORM. Country Risk Profile*. Retrieved from https://drmkc.jrc.ec.europa.eu/inform-index/INFORM-Risk/Country-Risk-Profile [last accessed on 12/05/2024].

European Commission's Directorate-General for Communications Networks, Content and Technology. (2018). *algo:aware. Raising awareness on algorithms*. Retrieved from https://actuary.eu/wp-content/uploads/2019/02/AlgoAware-State-of-the-Art-Report.pdf [last accessed on 12/06/2024].

European Union. (2018). *General Data Protection Regulation*. Regulation (EU) 2016/679. Retrieved from https://gdpr-info.eu/ [last accessed on 05/11/2023].

European Union (2023). Open data and AI: A symbiotic relationship for progress. *European Data*. Retrieved from https://data.europa.eu/en/publications/datastories/open-data-and-ai-symbiotic-relationship-progress [last accessed on 05/12/2023].

Evas, T. (2020). *European framework on ethical aspects of artificial intelligence, robotics and related technologies*. European Parliamentary Research Service. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654179/EPRS_STU(2020)654179_EN.pdf [last accessed on 05/12/2023].

Freeman, S. E. (2023). CSRF Analysis: Biometric Registration and Conflict Sensitivity: Potential Risks and Opportunities for Aid Actors in South Sudan. *CSRF Conflict Sensitivity Resource Facility in South Sudan*. Retrieved from https://www.csrf-southsudan.org/repository/csrf-analysis-biometric-registration-and-conflict-sensitivity-potential-risks-and-opportunities-for-aid-actors-in-south-sudan/ [last accessed on 14/02/2024].

High-Level Committee on Management. (2018). *Personal data protection and privacy principles*. Retrieved from https://archives.un.org/sites/archives.un.org/files/_un-principles-on-personal-data-protection-privacy-hlcm-2018.pdf [last accessed on 12/02/2024].

Hilhorst, D., et al. (2021). Accountability in Humanitarian Action. *Refugee Survey Quarterly*, *40*(4), 363–389. Retrieved from https://doi.org/10.1093/rsq/hdab015 [last accessed on 05/12/2023].

Heintze, H. J., and Thielbörger, P. (2018). *International Humanitarian Action*. Springer International Publishing. Retrieved from https://doi.org/10.1007/978-3-319-14454-2 [last accessed on 05/12/2023].

Helm, J. M., et al. (2020). Machine Learning and Artificial Intelligence: Definitions, Applications, and Future Directions. *Current Reviews in Musculoskeletal Medicine*, *13*(1), 69–76. Retrieved from https://doi.org/10.1007/s12178-020-09600-8 [last accessed on 05/12/2023].

Hersey, F. (2021). UNHCR shared Rohingya biometric data 'without consent'. *Biometric Update*. Retrieved from https://www.biometricupdate.com/202106/unhcr-shared-rohingya-biometric-data-without-consent [last accessed on 14/05/2024].

Holloway, K., et al. (2021). *HPG working paper. Digital identity, biometrics and inclusion in humanitarian responses to refugee crises*. Retrieved from https://odi.org/en/publications/digital-identity-biometrics-and-inclusion-in-humanitarian-responses-to-refugee-crises/ [last accessed on 06/05/2024].

Human Rights Watch. (2022). *Myanmar: No Justice, No Freedom for Rohingya 5 Years On.* Retrieved from https://www.hrw.org/news/2022/08/24/myanmar-no-justice-no-freedom-rohingya-5-years [last accessed on 14/05/2024].

Innovatrics. (2024). *Biometric Data.* Retrieved from https://www.innovatrics.com/glossary/biometric-data/ [last accessed on 14/02/2024].

Inter-Agency Standing Committee. (2023). *Operational Guidance on Data Responsibility in Humanitarian Action*.
Retrieved from https://interagencystandingcommittee.org/sites/default/files/migrated/2023-04/IASC%20Operational%20Guidance%20on%20Data%20Responsibility%20in%20Humanitarian%20Action%2C%202023.pdf [last accessed on 07/11/2023].

International Committee of the Red Cross. (2018). *Accountability to Affected Populations.* Retrieved from https://www.icrc.org/en/accountability-affected-people [last accessed on 29/11/2023].

International Committee of the Red Cross. (2019a). *Policy on the Processing of Biometric Data by the ICRC*. Retrieved from https://www.icrc.org/en/document/icrc-biometrics-policy [last accessed on 13/05/2024].

International Committee of the Red Cross. (2019b). *Bringing families together, with a new interface*. Retrieved from https://blogs.icrc.org/inspired/2019/06/27/families-together-trace-face-corners/ [last accessed on 13/05/2024].

International Committee of the Red Cross. (2021). *Les déplacés au Soudan du Sud*. Retrieved from https://www.icrc.org/fr/deplaces-sud-soudan [last accessed on 03/03/2024].

International Organization for Migration. (2009). *Data Protection Principles*. Retrieved from https://www.iom.int/sites/g/files/tmzbdl486/files/documents/2023-08/iom-dp-principles-en.pdf [last accessed on 21/04/2024].

International Organization for Migration. (2010). *IOM Data Protection Manual*. Retrieved from https://publications.iom.int/books/iom-data-protection-manual [last accessed on 06/12/2023].

International Organization for Migration. (2016). *IOM South Sudan, Partners Start Biometric Registration in Juba IDP Site*. Retrieved from https://www.iom.int/news/iom-south-sudan-partners-start-biometric-registration-juba-idp-site [last accessed on 14/02/2024].

International Organization for Migration. (2018a). *IOM and biometrics*. Retrieved from https://www.iom.int/sites/g/files/tmzbdl486/files/our_work/DMM/IBM/iom_and_biometrics_external_info_sheet_november_2018.pdf [last accessed on 14/02/2024].

International Organization for Migration. (2018b). *IOM, WFP Conduct First Beneficiary Data Exchange in South Sudan*. Retrieved from https://www.iom.int/news/iom-wfp-conduct-first-beneficiary-data-exchange-south-sudan [last accessed on 10/05/2024].

International Organization for Migration. (2020). *Accountability to Affected Populations (AAP) Framework.* Retrieved from https://www.iom.int/resources/iom-aap-framework [last accessed on 05/11/2023].

International Organization for Migration. (2021). *South Sudan — Biometric registration update: Malakal PoC Site*. Retrieved from https://dtm.iom.int/reports/south-sudan-biometric-registration-update-malakal-poc-site-december-2021 [last accessed on 21/04/2024].

International Organization for Migration. (2022). *World Migration Report 2022*. Geneva: IOM. Retrieved from https://publications.iom.int/books/world-migration-report-2022 [last accessed on 05/12/2023].

International Organization for Migration. (2023a). *Positioning innovative data solutions at the core of effective humanitarian response in South Sudan.* Retrieved from https://southsudan.iom.int/stories/positioning-innovative-data-solutions-core-effective-humanitarian-response-south-sudan [last accessed on 21/04/2024].

International Organization for Migration. (2023b). *South Sudan. Displacement Tracking Matrix.* Retrieved from https://dtm.iom.int/south-sudan [last accessed on 13/05/2024].

Jacobsen, K. L. (2017). On Humanitarian Refugee Biometrics and New Forms of Intervention. *Journal of Intervention and Statebuilding*, 11(4), pp. 529–551.

Kuner, C. (2019). University of Cambridge Faculty of Law Research Paper No. 20/2018: International Organizations and EU General Data Protection Regulation. *International Organizations Law Review*, 16, pp. 158-191.

Madiega, T. (2023). *Briefing: European Legislation in Progress. Artificial Intelligence Act*. European Parliamentary Research Service. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf [last accessed on 05/12/2023].

Marelli, M. (2023). The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders. *Computer Law & Security Review*, 50, pp. 1-17. Retrieved from https://www.sciencedirect.com/science/article/pii/S0267364923000596 [last accessed on 12/02/2024].

Maxmen, J. S. (1977). The post-physician era: medicine in the twenty-first century. *Journal of the American Medical Association*, 237(21), pp. 2336-2337. Retrieved from https://jamanetwork.com/journals/jama/article-abstract/353321 [last accessed on 05/12/2023].

Nalbandian, L. (2022). An eye for an 'I:' a critical assessment of artificial intelligence tools in migration and asylum management. *Comparative Migration Studies*, 10(32). Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9361936/ [last accessed on 04/03/2024].

Noor, E. and Manantan, M. B. (2022). "Artificial Intelligence". In *Raising Standards: Data and Artificial Intelligence in Southeast Asia* (p. 87-136). Retrieved from https://www.jstor.org/stable/resrep48536.10 [last accessed on 05/12/2023].

Pizzi, M., et al. (2020). AI for humanitarian action: Human rights and ethics. *International Review of the Red Cross*, *102*(913), 145–180. Retrieved from https://doi.org/10.1017/S1816383121000011 [last accessed on 05/12/2023].

Rodríguez Gómez, A. A. (2023). Soudan et Soudan du Sud : contexte historique des conflits actuels. *The Conversation*. Retrieved from https://theconversation.com/soudan-et-soudan-du-sud-contexte-historique-des-conflits-actuels-219048 [last accessed on 08/05/2024].

Soden, R., et al. (2021). *Responsible AI For Disaster Risk Management, Working Group Summary*. Geneva: World Bank. Retrieved from https://reliefweb.int/report/world/responsible-ai-disaster-risk-management-working-group-summary [last accessed on 05/12/2023].

Thomas, E. (2018). Tagged, tracked and in danger: how the Rohingya got caught in the UN's risky biometric database. *Wired*. Retrieved from https://www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh [last accessed on 14/02/2024].

Tsui, Q., Perosa, T., and Singler, S. (2023). Biometrics in the Humanitarian Sector: A current look at risks, benefits and organizational policies. *The Engine Room*. Retrieved from https://www.theengineroom.org/wp-content/uploads/2023/07/TER-Biometrics-Humanitarian-Sector.pdf [last accessed on 16/04/2024].

United Nations Educational, Scientific and Cultural Organization. (2022). *Recommendations on the Ethics of Artificial Intelligence.* Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000381137 [last accessed on 05/12/2023].

United Nations General Assembly. (1946). *Convention on the Privileges and Immunities of the United Nations*. Retrieved from https://www.un.org/en/ethics/assets/pdfs/Convention%20of%20Privileges-Immunities%20of%20the%20UN.pdf [last accessed on 12/02/2024].

United Nations General Assembly. (2016). *Report of the Secretary-General for the World Humanitarian Summit (A/70/709)*. Retrieved from https://reliefweb.int/report/world/one-humanity-shared-responsibility-report-secretary-general-world-humanitarian-summit [last accessed on 27/11/2023].

United Nations High Commissioner for Refugees. (2015). *Policy on the Protection of Personal Data of Persons of Concern to UNHCR*. Retrieved from https://www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=55643c1d4 [last accessed on 06/12/2023].

United Nations High Commissioner for Refugees. (2017). *Biometric Identity Management System. Enhancing Registration and Data Management*. Retrieved from https://www.unhcr.org/uk/media/biometric-identity-management-system [last accessed on 14/02/2024].

United Nations High Commissioner for Refugees. (2018a) *Guidance on Registration and Identity Management*. Retrieved from https://www.unhcr.org/registration-guidance/ [last accessed on 04/03/2024].

United Nations High Commissioner for Refugees. (2018b). *Guidance on Registration and Identity Management. 7.4: Registration and Assistance Management*. Retrieved from https://www.unhcr.org/registration-guidance/chapter7/registration-and-assistance-management/ [last accessed on 14/05/2024].

United Nations High Commissioner for Refugees. (2019). *Briefing Notes. More than half a million Rohingya refugees receive identity documents, most for the first time*. Retrieved from https://www.unhcr.org/news/briefing-notes/more-half-million-rohingya-refugees-receive-identity-documents-most-first-time [last accessed on 13/05/2024].

United Nations High Commissioner for Refugees. (2022). *General Policy on Personal Data Protection and Privacy.* Retrieved from https://www.refworld.org/policy/strategy/unhcr/2022/en/124207 [last accessed on 12/02/2024].

United Nations High Commissioner for Refugees. (2023). *Rohingya Refugee Crisis Explained*. Retrieved from https://www.unrefugees.org/news/rohingya-refugee-crisis-explained/ [last accessed on 14/05/2024].

United Nations High Commissioner for Refugees and World Food Programme. (2018). *Addendum on Data Sharing to the January 2011 Memorandum of Understanding Between the Office of the United Nations High Commissioner for Refugees (UNHCR) and the World Food Programme (WFP)*. Retrieved from https://emergency.unhcr.org/sites/default/files/WFP%20Addendum%20on%20data%20sharing%20%282018%29.pdf [last accessed on 10/05/2024].

United Nations Office for the Coordination of Humanitarian Affairs. (2023). *South Sudan: Humanitarian Needs and Response Plan 2024*. Retrieved from https://www.unocha.org/publications/report/south-sudan/south-sudan-humanitarian-needs-and-response-plan-2024-issued-november-2023 [last accessed on 08/05/2024].

United Nations Office for The Coordination of Humanitarian Affairs. (2024). *About the South Sudan Humanitarian Fund*. Retrieved from https://www.unocha.org/south-sudan/about-south-sudan-humanitarian-fund [last accessed on 12/05/2024].

World Health Organization. (2021). Ethical use of artificial intelligence: principles, guidelines, frameworks and human rights standards. In *WHO Consultation Towards the Development of guidance on ethics and governance of artificial intelligence for health: Meeting report Geneva, Switzerland, 2–4 October 2019* (pp. 8–11). World Health Organization. Retrieved from http://www.jstor.org/stable/resrep35680.8 [last accessed on 05/12/2023].

Annex I: Principles for data protection and data responsibility

UN PERSONAL DATA PROTECTION AND PRIVACY PRINCIPLES

1. **Fair and Legitimate Processing:** The United Nations System Organizations should process personal data in a fair manner, in accordance with their mandates and governing instruments and on the basis of any of the following: (i) the consent of the data subject; (ii) the best interests of the data subject, consistent with the mandates of the United Nations System Organization concerned; (iii) the mandates and governing instruments of the United Nations System Organization concerned; or (iv) any other legal basis specifically identified by the United Nations System Organization concerned.
2. **Purpose Specification:** Personal data should be processed for specified purposes, which are consistent with the mandates of the United Nations System Organization concerned and take into account the balancing of relevant rights, freedoms and interests. Personal data should not be processed in ways that are incompatible with such purposes.
3. **Proportionality and Necessity:** The processing of personal data should be relevant, limited and adequate to what is necessary in relation to the specified purposes of personal data processing.
4. **Retention:** Personal data should only be retained for the time that is necessary for the specified purposes.
5. **Accuracy:** Personal data should be accurate and, where necessary, up to date to fulfill the specified purposes.
6. **Confidentiality:** Personal data should be processed with due regard to confidentiality.
7. **Security:** Appropriate organizational, administrative, physical and technical safeguards and procedures should be implemented to protect the security of personal data, including against or from unauthorized or accidental access, damage, loss or other risks presented by data processing.
8. **Transparency:** Processing of personal data should be carried out with transparency to the data subjects, as appropriate and whenever possible. This should include, for example, provision of information about the processing of their personal data as well as information on how to request access, verification, rectification, and/or deletion of that personal data, insofar as the specified purpose for which personal data is processed is not frustrated.

9. **Transfers:** In carrying out its mandated activities, a United Nations System Organization may transfer personal data to a third party, provided that, under the circumstances, the United Nations System Organization satisfies itself that the third party affords appropriate protection for the personal data.
10. **Accountability:** United Nations System Organizations should have adequate policies and mechanisms in place to adhere to these Principles.

IOM DATA PROTECTION MANUAL

1. **Lawful and Fair Collection:** Personal data must be obtained by lawful and fair means with the knowledge or consent of the data subject.
2. **Specified and Legitimate Purpose:** The purpose(s) for which personal data are collected and processed should be specified and legitimate, and should be known to the data subject at the time of collection. Personal data should only be used for the specified purpose(s), unless the data subject consents to further use or if such use is compatible with the original specified purpose(s).
3. **Data Quality:** Personal data sought and obtained should be adequate, relevant and not excessive in relation to the specified purpose(s) of data collection and data processing. Data controllers should take all reasonable steps to ensure that personal data are accurate and up to date.
4. **Consent:** Consent must be obtained at the time of collection or as soon as it is reasonably practical thereafter, and the condition and legal capacity of certain vulnerable groups and individuals should always be taken into account. If exceptional circumstances hinder the achievement of consent, the data controller should, at a minimum, ensure that the data subject has sufficient knowledge to understand and appreciate the specified purpose(s) for which personal data are collected and processed.
5. **Transfer to Third Parties:** Personal data should only be transferred to third parties with the explicit consent of the data subject, for a specified purpose, and under the guarantee of adequate safeguards to protect the confidentiality of personal data and to ensure that the rights and interests of the data subject are respected. These three conditions of transfer should be guaranteed in writing.
6. **Confidentiality:** Confidentiality of personal data must be respected and applied at all stages of data collection and data processing, and should be guaranteed in writing. All IOM staff and individuals representing third parties, who are authorized to access and process personal data, are bound by confidentiality.

7. **Access and Transparency:** Data subjects should be given an opportunity to verify their personal data, and should be provided with access insofar as it does not frustrate the specified purpose(s) for which personal data are collected and processed. Data controllers should ensure a general policy of openness towards the data subject about developments, practices and policies with respect to personal data.
8. **Data Security:** Personal data must be kept secure, both technically and organizationally, and should be protected by reasonable and appropriate measures against unauthorized modification, tampering, unlawful destruction, accidental loss, improper disclosure or undue transfer. The safeguard measures outlined in relevant IOM policies and guidelines shall apply to the collection and processing of personal data.
9. **Retention of Personal Data:** Personal data should be kept for as long as is necessary, and should be destroyed or rendered anonymous as soon as the specified purpose(s) of data collection and data processing have been fulfilled. It may however, be retained for an additional specified period, if required, for the benefit of the data subject.
10. **Application of the Principles:** These principles shall apply to both electronic and paper records of personal data, and may be supplemented by additional measures of protection, depending, inter alia, on the sensitivity of personal data. These principles shall not apply to non-personal data.
11. **Ownership of Personal Data:** IOM shall assume ownership of personal data collected directly from data subjects or collected on behalf of IOM, unless otherwise agreed, in writing, with a third party.
12. **Oversight, Compliance and Internal Remedies:** An independent body should be appointed to oversee the implementation of these principles and to investigate any complaints, and designated data protection focal points should assist with monitoring and training. Measures will be taken to remedy unlawful data collection and data processing, as well as breach of the rights and interests of the data subject.
13. **Exceptions:** Any intent to derogate from these principles should first be referred to the IOM Office of Legal Affairs for approval, as well as the relevant unit/department at IOM Headquarters.

POLICY ON THE PROTECTION OF PERSONAL DATA OF PERSONS OF CONCERN TO UNHCR

1. **Legitimate and Fair Processing:** Processing of personal data may only be carried out on a legitimate basis and in a fair and transparent manner. UNHCR may only process personal data based on one or more of the following legitimate bases: (i) with the consent of the data subject; (ii) in the vital or best interests of the data subject; (iii) to

enable UNHCR to carry out its mandate; or (iv) beyond UNHCR's mandate, to ensure the safety and security of persons of concern or other individuals

2. **Purpose Specification:** Personal 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).
3. **Necessity and Proportionality:** The processing of personal data should be necessary and proportionate to the purpose(s) for which it is being processed. Therefore, data that is processed should be adequate and relevant to the identified purpose, and not exceed that purpose.
4. **Accuracy:** Personal data should be recorded as accurately as possible and, where necessary, updated to ensure it fulfils the purpose(s) for which it is processed.
5. **Respect for the Rights of the Data Subject:** The data subject's rights are information, access, correction, deletion and objection.
6. **Confidentiality:** UNHCR personnel need to maintain the confidentiality of the personal data of persons of concern at all times, even after a data subject is no longer of concern to UNHCR.
7. **Security:** In order to ensure the confidentiality and integrity of personal data, appropriate technical and organizational data security measures need to be put in place.
8. **Accountability and Supervision:** In order to ensure accountability for the processing of personal data in line with this Policy, UNHCR will set up an accountability and supervision structure.

IASC OPERATIONAL GUIDANCE ON DATA RESPONSIBILITY IN HUMANITARIAN ACTION

1. **Accountability:** In accordance with relevant applicable rules, humanitarian organizations have an obligation to accept responsibility and be accountable for their data management activities. Humanitarian organizations are accountable to affected populations, to internal governance structures, and to national, regional and international actors and authorities, as applicable. Humanitarian organizations should put in place all measures required to achieve their accountability commitments in line with these Principles.
2. **Confidentiality:** Humanitarian organizations should implement appropriate organizational safeguards and procedures to keep sensitive data confidential at all times, including through clear and consistent access restrictions. Measures should be in line with applicable organizational policies and legal requirements, while taking into account the relevant data and information sensitivity classification system(s) in the response context.

3. **Coordination and Collaboration:** Coordinated and collaborative data management entails the meaningful inclusion of humanitarian partners, national and local authorities, people affected by crisis, and other stakeholders in data management activities, where appropriate and without compromising the humanitarian principles or this Operational Guidance. Humanitarian organizations should coordinate and collaborate to ensure that appropriate connections are established between humanitarian operational data management activities and longer-term development-oriented data processes and data investments. Local and national capacity should be strengthened wherever possible, and not be undermined.
4. **Data Security:** Humanitarian organizations should implement appropriate organizational and technical safeguards, procedures and systems to prevent, mitigate, report and respond to security breaches of both digital and non-digital data. These measures should be designed to protect against material external breaches as well as unauthorized or inappropriate internal access or manipulation, accidental disclosure, damage, alteration, loss, and other security risks related to data management. Measures should be based on the sensitivity of the data and updated as data security standards and best practice evolve.
5. **Defined Purpose, Necessity and Proportionality:** Humanitarian data management and its related activities should have a clearly defined purpose. The design of processes and systems for data management should contribute to improve humanitarian outcomes, be consistent with relevant mandates, respect and promote rights and freedoms, and carefully balance those where needed. In line with the concept of data minimization, the management of data in humanitarian response should be relevant, limited and proportionate to the specified purpose(s).
6. **Fairness and Legitimacy:** Humanitarian organizations should manage data in a fair and legitimate manner. Fair data management enables the delivery of humanitarian action in a neutral and impartial manner.
7. **Human Rights-Based Approach:** Data management should be designed and implemented in ways that respect, protect and promote the fulfillment of human rights, including fundamental freedoms and the principles of equality and non-discrimination as defined in human rights frameworks, as well as data-specific rights promulgated in applicable legislation.
8. **People-Centered and Inclusive:** Affected populations should be afforded an opportunity to participate and be included, represented, and empowered to exercise agency in all steps of data management for a given activity, whenever the operational context permits. The human autonomy of people affected by crisis should guide humanitarian data management. Special efforts should be made to support the

participation and engagement of people who are not well represented or may be marginalized in a given data management activity (e.g., due to age, gender and other diversity characteristics such as disability, ethnicity, religion or sexual orientation), or are otherwise 'invisible', consistent with commitments to leave no one behind. These should include fostering data literacy across and within communities.

9. **Personal Data Protection:** When managing personal data, humanitarian organizations have an obligation to adhere to (i) applicable national and regional data protection laws, or (ii) if they enjoy privileges and immunities such that national and regional laws do not apply to them, to their own data protection policies These laws and policies contain the principles for personal data protection, such as a list of equally valid legal bases for the processing of personal data, including but not limited to consent. Humanitarian organizations should take personal data protection into consideration when developing open data frameworks.
10. **Quality:** Data quality should be maintained such that the owners, users and other key stakeholders are able to trust data management activities and their resulting products. Data quality entails that data is relevant, accurate, timely, complete, standardized, interoperable, well-documented, up-to-date and interpretable, in line with the intended use and bearing in mind the given operational context.
11. **Retention and Destruction:** Organizations should establish a data retention and destruction schedule that indicates how long data will be retained and when data should be destroyed, as well as how to do so in a way that renders data retrieval impossible. Sensitive data should only be retained for as long as it is necessary to the specified purpose(s) for which it is managed or as required by applicable laws or audit regulations. When retaining sensitive data, organizations should specify and ensure its safe and secure storage to prevent misuse or exposure. Non-sensitive data may be retained indefinitely, in line with applicable laws, regulations and policies, and provided that access rights are established and the sensitivity of the data is reassessed on a regular basis.
12. **Transparency:** Organizations should manage data in ways that offer meaningful transparency toward humanitarian actors and stakeholders, particularly affected populations. This should include the provision of timely and accurate information about the data management activity such as its purpose(s), the intended use(s) of and approaches to sharing the data, as well as any associated limitations and risks.

Annex II: Semi-structured interviews

Question design

Table 1: Question design for the semi-structured interviews

Question	Type of question	Rationale
1. What is your relation to biometrics and/or artificial intelligence? 1.1. What is your vision of these technologies?	Open-ended	This question is aimed at getting to know the interviewees' opinions of these technologies and assess their level of familiarity about them. Understanding this is relevant so that the research team is aware if there is a need for further clarification of certain concepts related to them. It is also important to ensure pre-existing biases do not compromise the integrity of the research.
2. Could you explain how IOM uses artificial intelligence in humanitarian settings?	Open-ended	This question seeks to fill the gap identified in the literature and desk reviews about the lack of public information on how IOM uses AI in activities related to their humanitarian work.
3. What are the main aspects of data responsibility necessary to ensure the appropriate use of artificial intelligence in biometrics, according to you?	Open-ended	This question seeks to understand how data responsibility can be ensured when deploying AI in humanitarian settings. Hence, it is important to determine how, through the proposed focus on biometrics, the interviewees would approach data responsibility in this context.
4. What measures could be implemented to monitor the use of artificial intelligence in data management activities, while remaining accountable to affected populations in the handling of their data?	Open-ended	Another aspect this research seeks to understand is how AAP can be preserved when handling beneficiary data using AI and biometrics. This question allows for obtaining information for possible recommendations on the best strategies to enhance beneficiary data management while making sure the organizations are accountable to them.

5. If IOM was developing a new policy on data responsibility, what aspects do you think should be addressed/included in it?	Open-ended	This question aims to understand what should be the priorities when addressing data responsibility in future institutional assessments like updating existing policies or drafting new ones. This is important for the research team to get familiarized with what the interviewees believe data responsibility should look like within their organization.
6. From your experience, what ethical considerations do you think are necessary to ensure the appropriate use of biometric data in the delivery of aid? 6.1. How can relevant actors commit to them?	Open-ended	One of the goals of this research is to establish the ethical considerations necessary for ensuring data responsibility and AAP when using new and emerging technologies. Considering there is a focus on biometrics (see research question 2), this question helps narrow down the most important ethical aspects in this matter, according to the interviewees' experience.
7. Taking into account that there currently is no binding framework on the use of artificial intelligence in humanitarian action, do you consider there should be one? (Yes or No). 7.1. If yes, what form should it take?	Closed-ended (7) and open-ended (7.1.)	One aspect identified in the literature review is the lack of a binding framework for IOs regarding data protection, especially for those in the UN System, as they have privileges and immunities. Considering that regulation on AI is currently developing, this question is aimed at understanding the interviewees' perspective on this issue, from their stance as experts in the field of interest for this research working in an organization that is part of the UN System.
8. Do you consider using biometric data has the potential to improve accountability to affected people? (Yes or No). 8.1. Why or why not?	Closed-ended (8) and open-ended (8.1.)	The literature and desk reviews identified biometric data as a technology recurrent in the handling of humanitarian needs in protracted migration flows, and one that can be integrated with AI (some organizations are already doing that). Hence, this question is relevant for determining if this widespread use of biometrics is seen as a tool that can help achieve AAP.

9. Do you have any recommendations on how the integration of AAP principles can ensure the responsible use of biometric data?	Open-ended	This research intends to provide recommendations on how AAP can serve data responsibility when handling biometric data, whether this is envisioned to be done with the help of AI or not. In this sense, obtaining information from the interviewees in their capacity as experts in the field of interest can help draft realistic and concrete recommendations.
10. More broadly, is artificial intelligence the most effective tool to enhance humanitarian work in complex settings? (Yes or No) 10.1. What other tool/technology would also be relevant to study/test?	Closed-ended (10) and open-ended (10.1.)	The main purpose of this research is to determine whether AI can help organizations achieve their mandates when delivering humanitarian assistance in a way that guarantees data responsibility and AAP. Considering that the use of new and emerging technologies in humanitarian action is on the rise, this question intends to understand how the interviewees assess this situation and if other technologies should be considered too.

Annex III: Primary data analysis

The four semi-structured interviews with IOM professionals were conducted by the research team both online and in person in Geneva, Switzerland. The research team took notes and audio recordings of the interviews. Audio recordings were used only for transcription and verification purposes, and were deleted at the end of the research process. The main ideas and patterns identified in a primary analysis of each of the interviews were then operationalized into concepts and added to the table below using Airtable software[14].

For easier access and to conduct a comparative analysis, each row was dedicated to a question or sub-question of the questionnaire included in Annex II, with each column reflecting the interviewee's responses to the questions.

[14] The original spreadsheet created on Airtable can be found here: https://airtable.com/appuA6uEUeosagoWs/shrcVNyYfr5oUVY9b.

Table 2: Interviewees' responses

Interviewee	**1**	**2**	**3**	**4**
1. Relation to biometrics and/or AI	- Biometrics is a widely used tool in the sector. - IOM: Registration and creation of profiles to target needs. - Data identity. - Facial recognition in border management. - Few cases of direct application in humanitarian settings.	- Familiar with biometric data, but not much experience. - Some experience with risk assessment process using biometrics.	- Initial development of DTM. - No relationship with AI.	- Part of the Biometric Working Group of IOM. - Not directly involved with AI. - Knows about the relationship between AI and biometrics.
1.1. Vision of these technologies	- It needs a more nuanced approach. - Biometrics can be appropriate in one context and very inappropriate in another. - Biometrics as a "blanket" tool. - AI and biometrics: They provide technical solutions, but require an analysis approach first.	- Cautious approach to biometric data. - Complexities that surround AI can marginalize some groups. - AI is good for comparing situations and implementation for analysis. - Corporate interests that push AI can complicate its use.	- Biometrics are important for avoiding duplication of data. - AI should be a content-feeding system that operates under human intervention. - AI should be solution-solving and not problem-solving. - Biases are innate to AI. - AI should be embraced but it's also important to remember that it shouldn't be the center of IOs' work.	- AI could be useful for processing large amounts of information produced by other tools used in humanitarian contexts.

Table 2: Interviewees' responses (continued)

Interviewee	1	2	3	4
2. How IOM is using AI in humanitarian settings	- Technical procedures: Recruitment, data processing, and collection. - There's an interest in using AI sector-wide, but there are few cases. - AI won't be found in humanitarian settings because this work requires the intervention of donor and partner agreements. - Not sure if IOM will ever get to a point of actually implementing AI directly in humanitarian settings.	- Initial report writing. - Data visualizations. - Synthetic datasets. - Qualitative research. - AI is quite nascent in humanitarian settings.	- The IOM isn't using AI in field operations today.	- Mostly, AI is used for productivity tools in internal procedures.
3. Main aspects of data responsibility necessary to ensure the appropriate use of AI in biometrics	- Confidentiality - Defined Purpose - Necessity and Proportionality - People-Centered and Inclusive - Quality - Transparency	- Defined Purpose - Necessity and Proportionality - People-Centered and Inclusive - Personal Data Protection - Retention and Destruction - Transparency	- Data Security - People-Centered and Inclusive - Human Rights-Based Approach - Personal Data Protection - Quality	- Confidentiality - Data Security - People-Centered and Inclusive

Table 2: Interviewees' responses (continued)

Interviewee	1	2	3	4
4. Measures that could be implemented to monitor the use of AI in data management activities, while remaining AAP in the handling of their data	- Governance - Safeguards	- Needs assessment - Methodology - Monitoring framework - Periodic reviews	- Do No Harm - AAP Framework - Monitoring framework - Partner agreements - Governance	- Needs assessment - Monitoring framework - AI minimization - Guidelines on inclusivity - Governance
5. Aspects that should be addressed/included in a new policy	- Subsidiary use of IASC guidelines (DR) - Exploration of heavy AI tools - Update on DP policy	- Update on DP policy - Accountability - Timing of emergency response	- People-centered - Accountability - Do No Harm	- People-centered - Consent - Privacy and anonymity - Timing of emergency response - Transparency - Efficiency - Data sharing agreements - Partners subject to org's DP policy
6. Ethical considerations necessary to ensure the appropriate use of biometrics data in the delivery of aid	- Context - Added value - Relationships with external actors - Data retention	- Risk assessment - Do No Harm - Data retention	- Data storage and security - Capacity-building - Do No Harm	- Purpose - Minimalization - Data deletion
6.1. How can relevant actors commit to them	- Sensibilization campaigns on ethical data collection	- Guidelines on informed consent	- Data sharing agreements,Governance	- Alternatives to beneficiaries' data

Table 2: Interviewees' responses (continued)

Interviewee	1	2	3	4
7. Do you consider there should be a binding framework on the use of AI	- Yes - Pre-condition: accountability agency	- No - Organizational commitment - Inter-agency guidelines - Contextualization	- Yes	- Maybe - Pre-condition: identification of economic stakeholders
7.1. If yes, what form should it take	- Organizational self-governance - Monitoring body - Donor regulation	N/A	- Comprehensive guide on AI use - People-centered general guidelines - Global and adaptable perspective	- Purpose - Efficiency
8. Using biometric data has the potential to improve accountability to affected people	- No	- Yes - If not a one-off emergency - If no interference by local authorities	- Yes	- Yes
8.1. Why or why not	- Process improves AAP, not tech - Accountability is an inclusive process with dialogue - Biometrics isn't an inclusive tech	- Depending on the case - Useful in the South Sudan case - Consent and data management issues in Rohingya case	- Helps humanitarian workers to know what type of aid and how much is needed	- Biometrics helped solve technical challenges in humanitarian context - Needs to be constantly assessed and revised - Depends on the context - Needs to be assessed before implementation

Table 2: Interviewees' responses (continued)

Interviewee	1	2	3	4
9. Recommendations on how the integration of AAP principles can ensure the responsible use of biometric data	- Inform: explain why and how data is used, stored, shared - Communicate - Give data users rights: ensure AAP - Responsible implementation	- People-centered - Information-sharing - Support service - Managing complaints and feedback	- Do no harm - Responsible use of data	- Consulting the local community before engaging - Inform: explain AAP to affected people - Be aware and limit technological biases - Always act in favor of beneficiaries - Inform beneficiaries how they can access information on the use of data - Ensure feedback to improve data life cycle
10. Is AI the most effective tool to enhance humanitarian work in complex settings	- Yes - Many technologies in humanitarian context have or will have AI components	- No - No concrete evidences of it working in humanitarian context - Human capital is more relevant	- Yes - Yes but need more information on how effective it can be - Needs to be ground proven	- Yes - But needs to assess the efficiency - Should be based on the need
10.1. Other tool/technology relevant to study/test	- Climate technologies - Space technology - Satellite imagery	- Satellite imagery in specific cases	- Machine learning - Satellite imagery - Data records	- Technology isn't bad but it shouldn't be a blanket solution