DIIS POLICY BRIEF AUGUST 2021

Avoiding harm, delivering impact

RISKS OF TECHNOLOGY USE IN HUMANITARIAN SETTINGS

The use of emerging technology in humanitarian settings carries significant risks. The complexity of these risks entails a need to understand and imagine risks beyond those commonly associated with a particular technology, field, or implementing organization.

In June 2021, Human Rights Watch accused the UN Refugee Agency UNHCR of having committed serious data management breaches. Sensitive biometric data captured by the agency among Rohingya refugees seemed to have been shared with the Bangladeshi government, which had then shared it with the

RECOMMENDATIONS

- Apply an extensive interpretation of what risks may look like, where, when, for whom, and how they might occur.
- The indiscernible nature of risks related to technology use means identifying or imagining these moves beyond existing organizational experiences.
- Recognize that technology-related risks can emerge across the data chain and are not only relevant for engineering or operational staff.

Burmese government at a time when the Rohingya minority was still being hunted and persecuted in Myanmar.

This and many cases like it illustrate the complexity of the risks associated with technology-use in humanitarian settings. These perils are at the same time abstract and delocalized when they are imagined, but prove extremely local and intimate when they occur, with real consequences for real people. Use of data may help delivering aid more effectively, but it also exposes vulnerable groups to risks that may be difficult to imagine or identify beforehand. This indiscernible nature of many risks makes it exceedingly important for humanitarian actors to try and understand and imagine them beyond their own previous experiences. Here, we briefly assess the extent of the potential risks that humanitarian actors must take into account when pursuing technological solutions in humanitarian settings characterized by vulnerability and uncertainty.

> ‘Novel actors bring new ways of working and thinking to humanitarian activities, but they also revive concerns over legitimacy, ethics and protection’

Field-expansion and the inclusion of emerging actors

Humanitarian settings are seeing an increase in the number and diversity of actors. The innovation agenda has enabled the engagement of actors and businesses that are not traditionally involved in humanitarian contexts. These include private companies, both tech and non-tech, impact investors and new types of civil-society organisations (CSOs). Associated risks with this expansion may stem from regulation, responsibility and dependence, as well as commercialization and privatization.

Novel actors bring new ways of working and thinking to humanitarian activities, but they also revive concerns over legitimacy, ethics and protection. New constellations of actors mean new forms of information and data being collected, as well as new practices, procedures and ways of storing and sharing such data. For example, health data may originate from patients' encounters with an AI chatbot and not be verified or fully accurate. Similarly, other health data such as on abortion that are typically extremely sensitive may be bundled with other data that are not. Risks thus emerge across the data chain, whether in data collection, use or regulation. The privatization of humanitarian services also introduces the risks of commercialization, including the use and sale of data to third parties. Such data may contain intimate biographical, biometric or health-related details, but they can also be aggregated into behavioral data, which is often sold in large quantities for marketization purposes.

Reproducing unequal power structures

The proliferation of actors also produces new or exacerbates existing unequal structures of power affecting beneficiaries. Risks include the widespread de-localization of both capacity and agency 'northwards' to Western tech companies, whose potential lack of contextual knowledge some see as a creatively productive force. Yet, this trend involves the pronounced risks of resource-waste, duplication (e.g. the creation of new mechanisms or technologies in contexts where ones already exist because of private ownership of software or APIs, such as that connecting devices for biometric capture to databases) and disconnect (between a delimited intervention and broader sustained attempts to address an issue). But also of being attentive to the needs of the developers or providers rather than the beneficiaries, and of ethical issues involving commodification and marketization.

Finally, fast-paced solutions or trials with technological innovations, like all interventions in humanitarian settings, create the risks of expectations and the creation of dependence. This risk is more pronounced when actors deliberately pursue experimental approaches in which the aim is to adapt, reorient oneself and change direction constantly, leaving the beneficiaries with frequently changing commitments.

> The increased datafication of humanitarian settings can change interactions between aid staff and beneficiaries and exacerbate existing conflict dynamics

Datafication can challenge privacy protection
Novel actors and the increased use of data in humanitarian settings also pose other risks, including those linked to surveillance and tracking, data-sharing and operational risks, which can all undermine the viability of consent and transparency. Datafication can deepen existing inequalities, as those in power collect, store and control data – in itself a political process of extraction. Tools such as biometric registration come with privacy concerns, the possibility of false matches or the potential for exclusion. The collection of various forms of data from multiple sources increases the risk of reidentification for beneficiaries. This underscores the need for critical reflection on the viability of informed consent, as risks may not be fully known.

Information communication technologies such as mobile phones improve communication and support remote data collection, yet they also introduce new risks to privacy, as both personal communication and location data can be intercepted by or transmitted to third parties, often without being detected. Technological tools such as location trackers (GPS) or remote surveillance using unmanned aerial vehicles can track and monitor movements on the ground, exposing beneficiaries to constant surveillance and increased vulnerability if data is intercepted. Increased reliance on technology for purposes of communication risks prioritizing those with access to technology. It may increase the risk of theft, interception, or the unintended and unaccountable exchange of private data, despite the proliferation of encrypted services.

Finally, the increased datafication of humanitarian settings can change interactions between aid staff and beneficiaries and exacerbate existing conflict dynamics. In some cases, datafication processes are implemented without securing the buy-in of all the actors and communities involved, or without paying sufficient attention to ensuring that data

Mobile phones are both a lifeline for refugees such as this Rohingya-family stranded in a refuge camp ind Bangladesh - and a liability, putting them at risk of surveillance and location tracking. Photo: Munir uz Zama/Ritzau Scanpix infrastructures can handle large amounts of data in local communities. Risks include faulty use of technology, partial data uploads or technical failures and the increased remoteness of local communities and aid staff, as technological tools may introduce a distance and a focus on technological goal attainment instead of on context-sensitive dialogue and solutions.

Implicit Biases in 'Objective Tech'?

The proliferation of data-based technological approaches that harness artificial intelligence (AI), machine learning and algorithms aims to identify needs and effectively distribute humanitarian assistance. AI systems are used to predict health-care risks, food insecurity and droughts, as well as to map refugee settlements and disaster-affected areas. These automated prediction tools are thought to mitigate repetitive and labour-intensive decisions, identify outcomes human analysts cannot foresee and increase the capacity to observe the principles of universality and neutrality.

However, algorithms are often developed in isolation from the contexts in which they are to be used and are prone to biases. Invisibly embedded in algorithmic systems, biases, (unconscious or otherwise, are introduced by homogeneous groups of developers or investors, are already incorporated into training datasets, or stem from a lack of diverse and comprehensive data). Non-representative datasets of humanitarian contexts and populations can cause facial recognition and remote-sensing imagery software to misidentify non-white faces or misinterpret disaster-affected areas. Racial and gender biases in medical datasets may likewise cause health-care AI systems to favor certain patient groups over others or to wrongly interpret correlating metrics. Risks include prioritizing majority groups and the uneven distribution of resources in humanitarian response.

Moreover, the inputs and mechanisms of self-adapting algorithms can be opaque to their developers (the black-box effect), and the inability to trace processes behind biased outcomes may automate discrimination and inequality. This accountability issue is pertinent in humanitarian settings, where the vulnerability and dependence of beneficiaries undermine their ability to evaluate decisions that directly affect them and potentially to appeal against them.

The adoption of technologies in humanitarian settings does not circumvent real-world bias and discrimination and has both the obvious and less obvious risks of entrenching inequalities or unintentionally violating humanitarian principles. Protection frameworks and the active monitoring of biases and automation processes to protect and also include those they are intended to serve must remain a prerequisite for technology use in vulnerable settings.

Authors: **Adam Moe Fejerskov, senior researcher (admo@diis.dk), Maria-Louise Clausen, senior researcher (mlc@diis.dk) & Sarah Seddig, Ph. D-student (ssed@diis.dk)**

Cover photo: Rohingya refugee children at Kutupalong refugee camp in Bangladesh. Photo: Munir uz Zama/Ritzau Scanpix