Wilton Park

Image: Peshkova

Report

Digital Dignity in armed conflict: a roadmap for principled humanitarian action in the age of digital transformation

WP1698 Monday 21-Wednesday 23 October 2019

In association with:

ICRC

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

Norwegian Ministry of Foreign Affairs

Wilton Park

Report

Digital Dignity in armed conflict: a roadmap for principled humanitarian action in the age of digital transformation

Monday 21 - Wednesday 23 October 2019 | WP1698

In association with the International Committee of the Red Cross, Swiss Federal Department of Foreign Affairs and the Norwegian Ministry of Foreign Affairs

Executive summary

The Wilton Park conference was convened to interrogate the implications of digital transformations in humanitarian action in armed conflict and other situations of violence and explore the notion of digital dignity. It brought together representatives of donor states, thought-leaders of research and academia as well as humanitarian practitioners including from the global south to stimulate discussion and develop concrete recommendations on principled ways by which to harness the movement to digital innovation and transformations in the humanitarian sector.

Participants considered: the risks and opportunities of digital transformations in humanitarian action in times of armed conflict; steps towards upholding the humanitarian concept of 'dignity' in the digital realm; requisite next steps towards a common understanding of best practices in data protection by humanitarian actors; raise awareness of how humanitarian protection work in the wider digital realm ("digital protection") needs to adapt; and, ultimately, how to strive towards digital dignity for affected people of armed conflict who receive humanitarian assistance and protection.

The meeting aimed to look at the following crucial issues of the digital transformation of humanitarian action:

- Digital dignity: Build towards a common understanding of digital dignity and promote ways in which digital dignity can be embedded into humanitarian practice and principles to ensure protection of the conflict affected populations.
- Affected people as data agents: Explore how to mitigate risk, increase safeguards, enable informed consent and promote good practice on dignity and privacy with affected individuals and communities.
- Digital risks: Increase awareness of the potential risks associated with data collection in a conflict environment.
- Humanitarian protection in the digital realm: Develop recommendations for best practices in applying recognised understandings of humanitarian protection to the digital realm, drawing on and expanding upon existing frameworks and International Humanitarian Law.
- Build new alliances to protect digital dignity: Catalyse a new network of actors including affected people, practitioners in the field, academics, private sector organisations, and the donor community to take forward future work on furthering the protection of affected people and their digital dignity.

Background

1. The digital transformation of humanitarian action has increased the capacity and efficiency of humanitarian response, but has simultaneously introduced new risks and harms to people receiving humanitarian assistance, as well as humanitarian organisations and key stakeholders. These new and added harms touch on issues ranging from dual-use technology, data incidents, to the use of third-party service providers, and new threats in the digital realm such as the weaponisation of information and cyberattacks.
2. Situations of armed conflict and other situations of violence present unique challenges to the digital dignity of conflict-affected populations. These complex environments require targeted solutions that address the unique challenges of operating in hostile and unstable environments.
3. Digital rights and dignity have emerged as key topics in the humanitarian sector given the increased collection and use of beneficiary data by humanitarian stakeholders, organisations and states alike (host states and donor states).
4. The wide-scale adoption of digital technology and in particular data collection in humanitarian response has led to both an increase in private sector participation in humanitarian efforts and has transformed the relationships of states, both donor and host states, and other non-states actors. These relationships have led to some challenges around the credibility and trust of humanitarian action.
5. In the realm of the risks related to digital data collection there is a lack of shared knowledge and reporting on humanitarian data incidents and best practices for data collection, storage, and data protection.
6. Existing standards and guides[1] provide a strong foundation for discussions around digital dignity but there is a need for regulatory frameworks and evidence-based research and case studies.
7. Given the large-scale challenges around the deployment of digital technology and data in the humanitarian space, multi-stakeholder response efforts are increasingly necessary.

Key Takeaways

Towards an understanding of digital dignity

8. Preparatory documents in the run up to the conference[2] provided suggestions to describe what digital dignity could mean: ‘the state when the agency, autonomy, and identity of individuals, as well as the communities they are a part of, is respected, enhanced, and empowered through how data that is both derived from them and pertaining to them (inclusive of any interventions that utilise this data) are collected, handled, and employed in ways that realise the human rights and enhance the human security of these individuals and their communities.’

[1] For example Signal Code – A Human Rights Approach to Information During Crisis; ICRC Handbook on Data Protection in Humanitarian Action; UN OCHA’s (Working Draft) Data Responsibility Guidelines; Danish Refugee Council/Global Protection Cluster Protection Information Management in Principles in Action

[2] https://www.wiltonpark.org.uk/background-paper-digital-dignity-in-practice-wp1698/ and https://www.wiltonpark.org.uk/background-paper-towards-a-common-understanding-of-digital-dignity-wp1698/

9. Participants identified the need to respect the dignity of an individual in today's digital context, and the primacy of an affected person being respected as data agent, not solely a data subject. Participants also highlighted that digital dignity needs to look beyond data protection and analyse the dynamics of data governance. In order to achieve digital dignity for affected people power dynamics of data governance must be challenged. Participants discussed how dignity is a cornerstone of humanitarian protection work, and includes the evolving digital landscape.

"new forms of digital violence evolving in armed conflict and other situations of violence ultimately transforming humanitarian protection work"

Understanding the scope of humanitarian problems and humanitarian action specific to the challenges posed in the digital age:

There should be a concerted effort to define the shape and scope of the needs of affected people in terms of humanitarian assistance and protection in the digital realm. Understanding the humanitarian protection needs of affected people in the digital space (e.g. weaponisation of information and the inherent protection problems that are presented from weaponisation) pose new challenges to humanitarian action in today's digital age. Defining what role the humanitarian sector, donor states and host states of humanitarian action play in addressing the complex digital realm of misinformation, cyber-warfare, data collection, storage, and use will help to create targeted responses to digital challenges that respect digital dignity. Concretely, humanitarian actors should also assess the information they collect, store, and share to ensure they are not over-collecting or misusing.

10. One of the central challenges of the new digital humanitarian landscape is understanding the complexity of each technology and how it interacts in the larger humanitarian space. In the first instance, it is important to disaggregate and define what data and digital technologies are being referred to when discussing specific solutions and policies to humanitarian technology. Three useful categories to consider when analysing digital technologies and data in the humanitarian context are: opportunities, risks, and unintended consequences.

11. In any examination of the collection, storage and deletion of data, the humanitarian community should ask: "How do we manage data?" "How do we produce data?" "How do we share data?" Data is currently being over-collected, lost and reproduced. Affected populations are often surveyed multiple times, triggering questions regarding the ethics of beneficiary data collection. There should be more meaningful dialogue around these questions in order to address the data chaos that currently exists in the humanitarian sector. Without proper needs assessments for data collection, unnecessary data will continue to be collected.

12. There also needs to be some consideration of group data. Humanitarians may be inadvertently generating target lists by creating group data on populations. It is important to define who is responsible and accountable in situations of data misuse and data incidents.

13. When utilising digital technologies in humanitarian response, it is imperative to take into account non-digitally connected communities. Under and non-connected communities are often comprised of the most vulnerable populations. However, it is also important to note that some under-connected communities may nonetheless be active participants in the digital realm; they may already have a digital footprint generated by data collection from other organisations, including ambient collection.

14. There are new forms of digital violence evolving in armed conflict and other situations of violence ultimately transforming humanitarian protection work. The humanitarian sector as well as states should seek to define whether weaponisation through misinformation or disinformation falls under the scope of humanitarian response in the same way as e.g. the use of lethal autonomous weapons. What prevention mechanisms should be in place to protect digital dignity? Is there a need for a cyber-security cluster?
15. Considerations around data protection should not only take place between humanitarian organisations, private sector or donor states. The presence of representatives from the global south at the conference demonstrated the urgent need to operationalise discussions around digital dignity and data protection in humanitarian action. This also requires robust engagement with host states and displaced people about digital dignity and data protection.

Building trust and accountability

"individuals who receive aid should be perceived as data agents who have agency over their digital identity and digital anonymity, which should move beyond the notion of being data subjects"

In the digital context of humanitarian assistance and protection, it is critical to ensure that trust and accountability are central components of relationships between the different stakeholders. This includes humanitarian actors, affected populations, governments, and donors, with vulnerable populations at the core.

16. Trust is a cornerstone of engagement in principled humanitarian action. It is multifaceted and should be embodied between and across humanitarian organisations and affected populations, as well as with the donor community.
17. The trustworthiness of humanitarian actors should not be undermined by the introduction of digital technologies; trust relationships should include private sector partners, donor states and governments.
18. Individual agency and dignity should be primary considerations when building trust and tackling the power asymmetries inherent in the relationships between humanitarian actors and affected people in need of humanitarian assistance and protection. affected people in need of humanitarian assistance and protection.
19. Accountability to affected populations includes the right to require remedies for breaches and violations, as well as the acceptance of liability on the part of the humanitarian community.
20. Privacy and security of data, and the concept of data ownership, are key. To promote digital dignity, individuals who receive aid should be perceived as data agents who have agency over their digital identity and digital anonymity, which should move beyond the notion of being data subjects. Data ownership is also linked to the "need to know" principal of data sharing. Using the data of affected people for anything other than humanitarian provision is unethical and obstructs the data rights of individuals.

Stakeholder relationships and informed consent

As digital technologies and data are increasingly adopted to make humanitarian action more efficient and effective, it is necessary to continuously examine and challenge asymmetrical power dynamics between affected populations, humanitarian actors, donors, and governments. Informed consent is key to any discussion on the protection and promotion of digital and data rights of vulnerable populations.

21. The notion of informed consent should be reformulated as meaningful consent, addressing coercive consent practices. Alternatives to the current framework of informed consent should provide an opt-out for people who choose not to provide information. This should not prevent access to services. An opt out will shift the power dynamic and go some way to addressing the relationship imbalance.
22. Informed consent is contingent on data literacy, including an understanding of the implications of data collection, storage, and use. This literacy is necessary not just for individuals whose data is collected, but also for practitioners and field workers.
23. In the current digital landscape, the collection, transfer and use of information in a transactional manner risks creating a commodified humanitarian environment and further impacts the power dynamic.

"The existence of a beneficiary inside the humanitarian system is often shaped by their personal data. In some instances, beneficiaries are not entitled to humanitarian assistance because of how their data does, or does not, define them"

24. The existence of a beneficiary inside the humanitarian system is often shaped by their personal data. In some instances, beneficiaries are not entitled to humanitarian assistance because of how their data does, or does not, define them. It is important to ensure that this does not distort or damage support for vulnerable populations.
25. Existing humanitarian power dynamics are further entrenched by the collection and sharing of beneficiary data. Specifically, it is noted that donors as well as host states are increasingly requiring data be collected, stored and shared in their preferred data management systems. In some cases, humanitarian organisations do not have access to the final data analysis. Additionally, donor's specific data requirements are seen to be a precondition to funding, which can lead to unnecessary data collection and can be seen as problematic to the digital dignity of affected populations.
26. Central to the stakeholder discussion is the role and meaningful involvement of affected populations in navigating the concept of digital dignity. This includes consent to data collection, determination for what and for how long their data is used, and the right to opt-out. Currently, most affected populations have limited access to their data and no material options for recourse if it is misused.
27. While some humanitarian organisations provide these services, the larger humanitarian system must seek to create more space to both listen and act on behalf of affected population's wishes with regards to their data. Advocating for digital rights is a positive step but ensuring remedies will do much to cement trust with affected populations.

Pathways to ethical multi-stakeholder engagement

"humanitarian organisations fear donor flight if digital harms and incidents are revealed and shared. There should be an environment where data incidents and challenges can be openly discussed with donors and other humanitarian organisations without loss of confidence and funding support"

A multi-stakeholder approach should be adopted to bring in those with expert skills, knowledge, experience and funding to work toward the promotion of dignity in the digital humanitarian era. This requires positive and sustained relationships between humanitarian actors, governments, donors and the private sector, particularly the technology sector, in order to bolster the technology security, data protection, digital literacy skills of humanitarian stakeholders.

28. Create shared language, knowledge and understanding of the digital humanitarian landscape requires cross-sector collaboration and partnerships. There needs to be an increase in overall digital literacy, hygiene and capacity building among humanitarian organisations, governments and donor states. The private sector on the other hand needs to better understand the spectrum of humanitarian action. This can be done with technical training, support and funding from the private-sector and donors. While the private sector has more technical capacities, it should also work with the humanitarian sector to better understand the principles and ethos that underline humanitarian work.

29. In an emerging field with rapidly evolving challenges and risks, there is anxiety about public sharing of mistakes, such as data incidents. Specifically, humanitarian organisations fear donor flight if digital harms and incidents are revealed and shared. There should be an environment where data incidents and challenges can be openly discussed with donors and other humanitarian organisations without loss of confidence and funding support. Moreover, sharing these risks will provide a better understanding around the level of need for donor support and funding to mitigate.

30. There should be more concerted efforts to bring the private and technology sectors into the humanitarian domain. Clear contracts that hold third parties liable and accountable should be drawn up in conjunction with efforts to integrate the core principles into third party work. This is not beyond the control of humanitarian actors and donors and is the responsibility of both.

31. Ensuring and pooling appropriate funding and resources for digital transformation work is imperative. Without proper funding to innovate and keep up with evolving digital risks and harms, the humanitarian sector will fail to adequately manage and promote the digital dignity of affected populations.

32. There is a need to operationalise the discourse around digital dignity and data protection and bring them into the complex, challenging and dangerous realities of armed conflict and other situations of violence. This requires a more comprehensive engagement with host states and other stakeholders to establish a common approach and framework for the protection of individual protection and data protection that align with contemporary discussions on digital practices.

System-wide legislative and normative changes

It is necessary for humanitarian actors, academics, researchers, host states and donors to actively share best digital practices, templates and toolkits as well as report on critical data incidents and existing challenges. The humanitarian community and key stakeholders should continue to explore existing legal frameworks, and push for new frameworks where needed, to govern data and digital practices towards better protection and the dignity of affected populations.

33. Despite the adoption of new technology and the culture of humanitarian techno-optimism, the humanitarian sector continues to fall short in its efforts to ensure accountability and create material change for affected populations. Efforts to promote digital dignity should not become another niche humanitarian initiative of the moment. Digital dignity should be part of the larger humanitarian mandate to ensure dignity writ large.

34. There is a need to understand the legal framework regarding data security in countries where humanitarian operations take place. If such frameworks do not exist in the relevant countries, it is imperative that the humanitarian community, donor states and other stakeholders develop best practices based on the most robust legal framework for data security available that can be applied in countries lacking the necessary legal framework.

35. In countries where humanitarian operations occur and there are weak or incomplete legal frameworks for data protection, the donor community, in conjunction with development and humanitarian actors, and relevant stakeholders should encourage and facilitate the establishment of legal frameworks for data security and digital practices in the host country that align with international norms.

36. There is a need to understand the applicability of legal frameworks in the digital realm, especially International Humanitarian Law and International Human Rights Law. There is a need to better define the operational application of IHL and IHRL in the digital realm so that such conclusions can frame the legal obligations of all relevant stakeholders in humanitarian action.

37. As digital transformations evolve and expectations from affected people and humanitarian organisations vis-à-vis digital practices and needs shift, there is a need for continuous interrogation of the normative and legal landscapes that accurately reflect the use of data and digital technology in the humanitarian sphere.

38. The complex nature of the digital and data landscape, combined with the limited capacity of humanitarian organisations and other stakeholders, such as donor states or host states, requires innovative and open practitioner communities. This space would allow for gaps and critical incident management to be communicated in a safe way. Practitioner communities should go beyond headquarters to encompass diverse perspectives, including those operating in challenging and complex field environments. Additionally, there is a need to publish scenarios of risks, harms and benefits to share across humanitarian organisations.

Conclusion and next steps:

The Wilton Park conference provided a starting point for more robust engagement within the humanitarian community and affected people about digital transformations of humanitarian assistance as well as protection, digital dignity and data protection in the humanitarian realm. Participants identified the following initiatives to further the integration of digital dignity within humanitarian action.

1. Delete your data': Apply the 'delete your data' approach to humanitarian data. Humanitarian organisations need to commit to reviewing and scrutinising their data collection and retention practices, deleting data that is no longer needed and avoiding unnecessarily collection.

2. Protection work to address today's digital threats: humanitarian protection work needs to adapt to the threats posed in the digital context needs to explore unified protocols for addressing data security and protection as a means to achieving digital dignity. Such unified protocols and tools can be built on existing standards, particularly chapter six of the current edition of the Professional Standards for Protection Work[3]. Such efforts need to go beyond the field of protection of data and information and explore how humanitarian protection work has to adapt in order to respond to digital threats

3. Donor requirements for data collection: The donor community, through relevant donor forums, will explore how to leverage its position in order to put pressure on organisations to prioritise data security and privacy initiatives. This should include a requirement for data security plans.

4. Investment in digital literacy: Donors and humanitarian organisations should pool funding and resources to invest in toolkits, frameworks, and prevention mechanisms to promote and protect the digital dignity of crisis-affected populations.

5. Track critical data incidents: A small group of participants agreed to work together to collect, track, and analyse critical data incidents to better inform how to address and mitigate such issues.

6. 75th anniversary of the United Nations: Use the 75th anniversary of the United Nations as a platform to further the topic of digital dignity and data security: the theme for the 75th anniversary is digital cooperation.

[3] See https://www.icrc.org/en/document/professional-standards-protection-work, chapter 6 "Managing data and information for protection outcomes"

7. Enhance the digital literacy of key humanitarian stakeholders: Enhance digital literacy for key stakeholders, including humanitarian actors and government duty-bearers. Digital literacy for humanitarian actors would include understanding the data collected and stored, as well as promoting humanitarian actors to be champions of data security. Digital literacy for government duty-bearers should be in the establishment of robust legal frameworks related to data security.

Natalie Cilem
MSc in International Development and Humanitarian Emergencies, the London School of Economics

Ann Marie McKenzie
MSc in International Development and Humanitarian Emergencies, the London School of Economics

Wilton Park | November 2019