International Review of the Red Cross (2020), **102** (913), 27–41.
Digital technologies and war
doi:10.1017/S1816383120000429

IRRC_

Q&A: Humanitarian operations, the spread of harmful information and data protection

In conversation with Delphine van Solinge, the ICRC's Protection Advisor on Digital Risks for Populations in Armed Conflict, and Massimo Marelli, Head of the ICRC's Data Protection Office

In this Q&A, the Review *talks to Delphine van Solinge and Massimo Marelli of the International Committee of the Red Cross (ICRC). Van Solinge is the ICRC's focal point for understanding how digital technologies and the spread of harmful information affect populations living in conflict environments, and what this means for humanitarian action. To this end, her portfolio is focused on exploring, on behalf of the ICRC and through partnerships, how to mitigate the risks that digital technologies bring in humanitarian settings and ensure relevant protection responses in the digital age. Marelli is Head of the ICRC's Data Protection Office (DPO). During his tenure with the ICRC, the organization has chartered new pathways for how it can carry out its operational work, while ensuring that the data of the affected people which it serves, as well those of its employees, are well protected.*

During this conversation, van Solinge and Marelli discuss how their areas of work complement and reinforce each other, forming two halves of the same coin with regard to how digital information and data can both be used for positive change and misused *in humanitarian settings. Marelli highlights how humanitarian organizations process, protect and use data and digital information. Van Solinge discusses how through misinformation, disinformation and hate speech, information can be manipulated and spread using digital technologies – particularly in the age of the COVID-19, when populations are more reliant on digital communication technologies. Among the issues they discuss are how digital technologies can be used positively, the ethical considerations that humanitarian organizations should take into account, and the possible paths forward for public–private sector collaborations on this theme.*

Keywords: spread of harmful information, misinformation, disinformation, hate speech, social media platforms, COVID-19, data protection, do no harm, humanitarian metadata.

: : : : : : :

What does the "weaponization of information" mean for the ICRC? How is it different from misuses of information during armed conflicts and other situations of violence? How do the "do no harm" principle and the work of the DPO relate to the "weaponization of information"?

Delphine van Solinge: As a foreword, it is important to underline that the term "weaponization of information" presents several shortcomings, in particular from a legal perspective. For instance, there is the question of whether, legally speaking, information can become a weapon – and if so, how and when? For such reasons, the ICRC would instead speak about the spread of harmful information, which covers misinformation, disinformation and hate speech [MDH] and the various different facets of these.

The ICRC has been concerned for some time by instances in which digital information and communication systems are being used in ways that have the potential to put populations of concern – such as internally displaced persons, migrants, detainees and minority groups, as well as humanitarian staff and volunteers – at a new or increased risk of humanitarian consequences. For a lack of a better term, the ICRC is using MDH as an umbrella acronym to refer to such phenomena, acknowledging however that information can be used for other purposes or without increased risk of humanitarian consequences (such as in operations that have consequences solely against adversary forces). In this respect, humanitarian consequences can refer to displacement; death; disappearance; loss or destruction of property; loss of income; physical, mental/psychological and social harm or injury; stigmatization; family separation; or denial of access to services such as education, health, shelter or food. Humanitarian consequences can also include the creation or exacerbation of existing humanitarian needs, namely for shelter, food and non-food items, medical care, psychological and psycho-social support, economic support, access to services, access to timely and locally relevant information, legal advice and support, or access to the Internet.

MDH may take the form of misinformation, disinformation, mal-information, viral rumours, digital hate speech, online propaganda, etc.[1]

The way in which information is being used is usually not enough, in and of itself, to "cause" harm. Rather, the "potential" for harm can be exacerbated when combined with underlying social, cultural and historical dynamics; existing social or political tensions; people's lack of digital literacy or critical thinking when browsing for information online; lack of trusted, accurate sources from which to triangulate information; and so on.

One may ask, how is this different from before? As history shows, there are many examples where information and communication systems have demonstrated their capacity to generate harm, such as in the case of Radio Mille Collines in Rwanda.[2] What has changed is the type of vehicle being used to spread information at a global level. Digital technologies, and social media in particular, have increased the speed, scale and impact with which information can spread and impact different audiences. Increased internet penetration, the availability of smartphones and social media have emerged as powerful tools for sharing information and connecting people, but also for exacerbating violence and conflict, such as in the case of hate speech on Facebook in Myanmar. These new variables have impacted the way in which information may be viewed as a potential means to induce civilian harm.

Massimo Marelli: I would relate what we do in the DPO to what Delphine has just said. We approach our work about data protection in much the same way: it's not just about the data, it's about how the data are used, or possibly misused. The DPO makes sure that the personal data of the ICRC's beneficiaries, interlocutors and staff are well protected, and that the essential bond of trust remains both within and toward the organization. Within this framework, "do no harm" means recognizing that a failure to protect the personal data of the ICRC's beneficiaries, interlocutors and staff could be incredibly harmful, both to the individuals concerned and to the viability of the ICRC's operations. Data protection as a tool to "do no harm in a digital environment"[3] is also linked to its capacity to provide

[1] For further reading on these terms, see Peter Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media*, Houghton Mifflin Harcourt, Boston, MA, 2018, available at: www.likewarbook.com; Mark Silverman, "Book Review: *LikeWar: The Weaponization of Social Media*", *International Review of the Red Cross*, Vol. 101, No. 910, 2019, available at: https://international-review.icrc.org/sites/default/files/reviews-pdf/2019-12/irrc_101_910_21.pdf; John Mingers and Craig Standing, "What is Information? Toward a Theory of Information as Objective and Veridical", *Journal of Information Technology*, Vol. 33, No. 3, 2018, available at: https://link.springer.com/article/10.1057/s41265-017-0038-6.

[2] Radio Mille Collines, also known as Radio Télévision Libre des Mille Collines, was a Rwandan radio station that spread disinformation and misinformation during its broadcasts between 8 July 1993 and 31 July 1994. The false propaganda that it spread played a dominant role in inciting the 1994 Rwandan Genocide against the Tutsi people in the country. For more information, see Elizabeth Baisley, "Genocide and Constructions of Hutu and Tutsi in Radio Propaganda", *Race and Class*, Vol. 55, No. 3, 2014, available at: https://journals.sagepub.com/doi/abs/10.1177/0306396813509194.

[3] ICRC, *The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era*, 2018, available at: www.icrc.org/en/download/file/85089/the_humanitarian_metadata_problem_-_icrc_and_privacy_international.pdf.

a lens through which we can analyze the data flows generated by the use of technologies and understand what new stakeholders may be involved, the risks that this may generate, and possible ways of mitigating or avoiding those risks. Having said that, data protection brings much more than "do no harm": it is about ensuring the respect of the rights and dignity of affected populations when we process their data, keeping the individual at the centre. It is also about being accountable to affected populations against clear standards.

Can you tell us more about why humanitarian organizations should care about the spread of harmful information and data protection?

Massimo Marelli: Both data protection and combating the spread of harmful information are integral to the ICRC's broader protection mandate. As well, both areas of work are essential if the ICRC is to maintain the trust of affected populations and parties with whom it maintains a confidential dialogue. When it comes to data protection, in addition to serious consequences for the data subjects, a major data breach at the ICRC or any other humanitarian organization could undermine trust in the sector and its ability to access and serve those who need it the most.

The ICRC's use of biometrics in its forensics work and in Restoring Family Links [RFL] is an example of how data protection plays a role in the operational work of a humanitarian organization and speaks to why humanitarian organizations should care about data protection. The ICRC's Biometrics Policy was adopted in August 2019 to address the acute data protection challenges posed by the use of biometric data – fingerprints, facial recognition, DNA, etc. – which is particularly sensitive because once it has been collected, if retained, it creates a permanently identifiable record of an individual.[4] This can be a problem in humanitarian settings, where people may not want to be permanently identifiable, particularly if there is a risk that their information may fall into the wrong hands. The Policy was a response to growing internal interest in the potential that biometrics could bring to the ICRC's operations, and strikes a careful balance between facilitating their responsible use and addressing the inherent data protection risks. The Policy is now helping shape aspects of the digital transformation of the ICRC's Central Tracing Agency, which is developing new tools to enhance our capacity to determine the fate and whereabouts of the missing and, working with partners in the International Red Cross and Red Crescent Movement [the Movement], to restore family links. This includes the possible use of facial recognition technology to match photographs of missing and sought persons, and the use of artificial intelligence to help locate individuals in the databases of the ICRC and its humanitarian partners. Robust adherence to data protection standards will be essential to build trust in the integrity, security and use of these tools.

[4] ICRC, "The ICRC Biometrics Policy", 16 October 2019, available at: www.icrc.org/en/document/icrc-biometrics-policy.

Delphine van Solinge: And the same applies when we think about the spread of harmful information, which takes place through acts of misinformation, disinformation, hate speech, etc. The way these practices and dynamics play out has implications for our humanitarian protection work. While these are not new phenomena *per se* and their potential to generate harm is relatively well-established, rapid digitalization – in ICRC operational contexts and beyond – has accelerated the speed with which harmful information can spread and can resonate with and influence different audiences. Rumours are no longer geographically contained; photos and videos can be fabricated quickly, with little overhead cost; and individuals and communities can be identified and targeted.

Myanmar, South Sudan and Ethiopia[5] are a few examples showing that phenomena related to MDH, in particular on social media, are currently and increasingly playing out in contexts struck by violence and war. What does this mean? Basically, it means that humanitarian organizations are more frequently coming face to face with practices and dynamics that exploit information and communication systems, which can be very disruptive. Such practices have the potential to destabilize already fragile environments, increase people's vulnerability and contribute to humanitarian consequences. If we are unable to understand and identify those factors of risk when we design our protection response, we might be missing out on certain harms or provide only a partial response to the needs of affected people.

Another thing that we need to realize is that MDH can directly affect humanitarian organizations' operational response and credibility. What would happen if the ICRC became the target of a coordinated disinformation campaign in a war-torn country? Our credibility might be severely tarnished, thus losing the trust of affected people; we might be denied access to war zones, thus preventing our capacity to bring protection and assistance to the populations on the ground; we might even be attacked.

If we agree that the spread of harmful information can be a vector or a factor that may increase people's vulnerability, contribute to civilian harm or lead to reputational damage or security risks for humanitarian organizations, we may need to have this on our radar.

What are the challenges that the humanitarian sector is facing as a result of the spread of harmful information? Also, we hear a lot about the challenges posed for humanitarian organizations in terms of the collection and protection of humanitarian metadata – can you tell us about the challenges and risks of collecting and protecting this metadata?

Delphine van Solinge: I'll answer your first question. There are many challenges related to the spread of harmful information, but we can look at three of them here.

[5] In those contexts, social media platforms such as Facebook and Twitter have been used to spread misinformation, rumours and hateful speech which have exacerbated tensions and led to acts of violence on the ground.

Firstly, MDH threats are non-localized. They are not generated by one group of people sitting in a bunker, with a unique ability to build harmful content or to create new approaches to spreading false information. In the digital age, every connected individual can consume, create and share content, and with it, they can become an actor who is spreading information that is causing harm, without even knowing it. In the same vein, in some instances, you do not need to do much to achieve a lot when it comes to disinforming or misinforming a potentially large audience. With a two-minute video, filmed and edited with a smartphone and posted on social media, you can achieve a huge effect. We have all watched "flash mob" videos, and this is a similar concept: with one message you have everyone dancing in Central Station in Antwerp.[6] Also, the availability of tools and malware at relatively cheap prices makes the work of malicious actors increasingly easier. This can potentially raise a number of legal questions in terms of responsibility, accountability and participation in hostilities.

Related to this, we know also that MDH is not easily detected or verified by conventional means. In the ocean of news and information that bombards us, it takes time and practice to develop an expert eye. Adding to the complexity is the difficulty of measuring the impact of MDH, which can sometimes be diffuse or intangible. For example, how would you measure the erosion of trust? Or, how would you determine the relationship between online activity and real-world consequences? Some non-profit organizations and academics have been more closely studying the different aspects of "weaponization of information", but they rarely focus on countries affected by war and violence. As for the humanitarian community, it is slowly awakening to the potential risks related to MDH and the spread of harmful information, but it struggles to determine how to integrate this new dimension into its work.

Finally, digital communication and MDH bring in a new set of actors with varied roles and responsibilities, such as the media and the private sector. The question of how to engage with these actors in a meaningful dialogue, beyond just promoting our humanitarian activities, is still very new for us.

Massimo Marelli: I think that much like the spread of harmful information, there are a number of challenges when it comes to how humanitarian organizations protect and store metadata. But first, let me start with the terminology we're working with here. Metadata is data about data. This includes information about communications, such as who contacted whom and when, and the digital traces left behind when computer devices, applications and networks interact with one another.

Why is the gathering and protection of metadata important? Well, because metadata reveals a lot about its subjects. Metadata is what online advertising companies use to profile users of the Internet, and what intelligence and security agencies use to identify persons and groups of interest. In a humanitarian context, the challenges and risks of collecting metadata relate to how metadata

[6] The referenced flash mob dance can be seen at: www.youtube.com/watch?v=7EYAUazLI9k.

can be used to reveal the location, movements and interactions of humanitarian organizations and affected populations – information which could betray confidentiality and be used for non-humanitarian purposes, for example by parties to a conflict. In some contexts, though, metadata can also be incredibly useful to humanitarian organizations, allowing them to better understand how their services are used and where they are needed most. Metadata can also be used to help determine the fate of missing persons in online environments. The ubiquity of this kind of information is what makes the data protection risks so difficult to manage. In this respect, the ICRC has partnered with Privacy International to help the raise awareness of the "humanitarian metadata problem"[7] and has collaborated with the Brussels Privacy Hub to produce data protection guidance on how to manage these risks.[8]

How do pandemics like COVID-19 affect the cases and prevalence of spread of harmful information and the need to be vigilant about data protection in the humanitarian sector?

Delphine van Solinge: The outbreak of an infectious disease often leads to increased MDH. Ideas around pandemics tap into our deepest and strongest emotions, inciting fear and creating waves of panic. With growing levels of uncertainty and anxiety, people seek answers by turning to information outlets. News on social media spreads faster and wider, and has low levels of curation. In this context, information can be manipulated for economic, ideological or political gain.

In the case of COVID-19, misinformation, viral rumours and disinformation have been observed on many digital platforms and websites. The spread of information has attained such levels that it has been labelled as an "infodemic".[9] Certain unverified content related to infectious diseases, imminent threats and death can override people's rational minds and increase polarization within societies. In some cases, these frameworks of thinking can manifest in the form of extreme, possibly violent behaviours, including direct physical attacks on medical staff or facilities, riots followed by police or military use of force, etc. Misleading or wrong information spread through social media about the location of quarantine sites, for instance, has increased public uncertainty and fear, prompting citizens to attack convoys transferring patients and to block evacuations.

[7] ICRC, "Digital Trails Could Endanger People Receiving Humanitarian Aid, ICRC and Privacy International Find", 7 October 2018, available at: www.icrc.org/en/document/digital-trails-could-endanger-people-receiving-humanitarian-aid-icrc-and-privacy.

[8] ICRC, *Handbook on Data Protection in Humanitarian Action*, 23 August 2017, available at: www.icrc.org/en/data-protection-humanitarian-action-handbook.

[9] For example, see UN Department of Global Communications, "UN Tackles 'Infodemic' of Misinformation and Cybercrime in COVID-19 Crisis", 31 March 2020, available at: www.un.org/en/un-coronavirus-communications-team/un-tackling-'infodemic'-misinformation-and-cybercrime-covid-19; Farah Lalalni and Juraj Majcin, "Inside the Battle to Counteract the COVID-19 'Infodemic'", World Economic Forum, 9 April 2020, available at: www.weforum.org/agenda/2020/04/covid-19-inside-the-battle-to-counteract-the-coronavirus-infodemic/.

The spread of misinformation or disinformation over social media may also be increasing because platforms' content moderators have been sent home, leaving the removal of misleading content to machines. While promising, the ability of artificial intelligence and automated systems to take down misleading content is still insufficient.

Misinformation or disinformation can affect humanitarian organizations, particularly those affiliated or perceived to be affiliated to countries with high levels of COVID-19 infection. Foreign humanitarians can be perceived by the population as carrying the virus. This could have far-reaching consequences in terms of security and operational capacity.

What has the ICRC done so far about MDH in terms of its humanitarian operations, and about applying the "do no harm" principle to its work on data protection?

Delphine van Solinge: In terms of operational work regarding MDH, in December 2018, the ICRC organized a symposium on digital risk in London.[10] This event was aimed at understanding how digital technologies and the ways they are being used affect civilian populations in armed conflicts, and the implications in terms of protection and humanitarian response.

Based on some of the key highlights from the event, the ICRC initiated a programme of work on MDH. The first phase of this programme was conducted in 2019, and its focus was on understanding the key barriers and challenges that prevent ICRC staff from integrating MDH into their analysis and work. This research was carried out in two ICRC delegations: Sri Lanka and Ethiopia. Based on some of the initial needs identified during the research, we have developed a practical guide on MDH for ICRC field staff to help them become more familiar and at ease with this concept.

Last but not least, we are now embarking on the creation of a research network on MDH with academia and interested humanitarian organizations. Our aim is to build evidence-based research around MDH and humanitarian consequences with a view to developing the conceptual foundations that humanitarian organizations will need to address this issue. This will help in defining the implications of MDH for protection and humanitarian work. It will also elucidate how the ICRC and other interested humanitarian organizations can best incorporate MDH into their analyses and responses to affected people.

Massimo Marelli: The work we're doing in terms of data protection similarly focuses on carefully assessing the risks of harm of a specific course of operational action and then taking steps to mitigate those risks, which may include not going ahead with the operation or rethinking operational strategy. With regard to "do no harm", we have now adopted several specific safeguards in the ICRC's Rules

[10] The report of the London Symposium on Digital Risks in Armed Conflicts can be found at: www.icrc.org/fr/publication/4403-symposium-report-digital-risks-armed-conflicts.

on Personal Data Protection, adopted in 2015, which are designed to reduce the risk of unauthorized use or access to personal data by applying data protection standards and requirements to data processing throughout the organization.[11] Where new technologies or riskier data processing operations are considered by the ICRC, a Data Protection Impact Assessment must be conducted to identify and mitigate the risks of harm.[12] The Rules also require the ICRC to follow a "data protection by design"[13] approach to minimize the collection of personal data to that which is necessary for the operation and ensure that data subjects' rights are respected.

As a humanitarian community, what can we do to start addressing the challenges arising from the spread of harmful information (MDH) and data protection concerns?

Delphine van Solinge: To start addressing the challenges arising from the spread of harmful information, we need a deeper understanding about MDH and humanitarian consequences, a strategic orientation supported by solid conceptual foundations, and a willingness to engage with new actors in uncharted waters.

However, to do this we need to keep in mind the following. If we start working on solutions in silos and without shared priorities, the impact will be limited, and we will waste energy. MDH is an issue that concerns many of us, and it is a complex problem in which many different dynamics, systems and actors are present and interacting. For this work on MDH, we need to follow a systemic approach.

Finally, we need to develop the conceptual foundations for the spread of harmful information. This includes a clear and thorough understanding of the potential risks and harms that digital information technologies and their uses can introduce for affected populations and humanitarian organizations, as well as how to respond to and mitigate those risks. We therefore need a theory of digitally derived harm, and to connect theory to practice, we need a conceptual framework. Given the breadth of this endeavour, there is a need to partner and join forces with one another – for example, with other organizations or academics and academic institutions.

Massimo Marelli: I agree with Delphine – we need to break down the silos and identify some shared priorities across the humanitarian sector if we want to effectively address the spread of harmful information and data protection concerns. In terms of data protection, the embrace of new digital technologies by the humanitarian sector and the specific risks that these technologies have

[11] ICRC, *ICRC Rules on Personal Data Protection*, 2015, available at: www.icrc.org/en/publication/4261-icrc-rules-on-personal-data-protection.

[12] *Ibid.*; see also ICRC, "Policy on the Processing of Biometric Data by the ICRC", 28 August 2019, available at: www.icrc.org/en/download/file/106620/icrc_biometrics_policy_adopted_29_august_2019_.pdf

[13] ICRC, above note 11.

brought with them have prompted the ICRC to think seriously about what it means to "do no harm in a digital environment". To this end, we have actively formed strategic partnerships with data protection-conscious organizations[14] and service providers, and have engaged in "digital diplomacy" to address some of the specific challenges facing the humanitarian sector. This includes efforts to safeguard the "digital humanitarian space",[15] ensuring that data collected for humanitarian purposes can only be used for those purposes in accordance with the principles of neutrality and independence.

In addition to ensuring that data protection rules are incorporated into partnership agreements at the operational level, the ICRC has, for example, worked closely with the Movement to develop data protection standards for RFL, which are represented in a Movement Code of Conduct.[16] Data protection issues also figured prominently at the 33rd International Conference of the Red Cross and Red Crescent in December 2019,[17] where doing no harm in digital environments was widely discussed in the context of "Shifting Vulnerabilities" and "Trust in Humanitarian Action". The Conference also adopted a groundbreaking resolution on RFL and data protection which recognizes that the acquisition and use of humanitarian data for non-humanitarian purposes undermines trust in humanitarian organizations and threatens their ability to operate. The resolution "urges States and the Movement to cooperate to ensure that personal data is not requested or used for purposes incompatible with the humanitarian nature of the work of the Movement".[18]

[14] For example, the ICRC and the Brussels Privacy Hub have collaborated together on the Data Protection in Humanitarian Action Project, aimed at the staff of humanitarian organizations involved in processing personal data as part of humanitarian operations, particularly those in charge of advising on and applying data protection standards. Outputs include the *Handbook on Data Protection in Humanitarian Action*, available at: www.icrc.org/en/data-protection-humanitarian-action-handbook. The ICRC has collaborated and/or consulted with experts from numerous organizations in its data protection work, including but not limited to the Brussels Privacy Hub, the Swiss Data Protection Authority, the European Data Protection Supervisor, the Office of the United Nations High Commissioner for Refugees, the International Organization for Migration, the International Federation of Red Cross and Red Crescent Societies, the United Nations Office for the Coordination of Humanitarian Affairs, Yale University, Privacy International, the French-Speaking Association of Personal Data Protection Authorities, the Swiss Federal Institute of Technology in Lausanne, Doctors Without Borders, and the Senegalese Data Protection Authority.

[15] For a more detailed analysis of the ICRC's role in safeguarding the "digital humanitarian space", see Massimo Marelli, "Hacking Humanitarians: Moving Towards a Humanitarian Cybersecurity Strategy", *Humanitarian Law and Policy Blog*, 16 January 2020, available at: https://blogs.icrc.org/law-and-policy/2020/01/16/hacking-humanitarians-cybersecurity-strategy/.

[16] International Red Cross and Red Crescent Movement Family Links Network, *Code of Conduct on Data Protection*, November 2015, available at: www.icrc.org/en/download/file/18229/rfl-code-of-conduct.pdf.

[17] International Conference of the Red Cross and Red Crescent, "33rd International Conference: At a Glance", available at: https://rcrcconference.org/about/33rd-international-conference/.

[18] International Conference of the Red Cross and Red Crescent, "Resolution: Restoring Family Links While Respecting Privacy, Including as It Relates to Personal Data Protection", 33rd International Conference, 9–12 December 2019, available at: https://rcrcconference.org/app/uploads/2019/12/33IC-R4-RFL-_CLEAN_ADOPTED_en.pdf.

What are some examples of how digital information and communication systems can be used positively?

Delphine van Solinge: Digital information technologies offer opportunities to improve the humanitarian responses to affected populations, including, but not limited to, by facilitating two-way communication between humanitarian staff and people affected by crises, or by using innovative ways of capturing and using crisis-related information to inform responses. Human rights defenders and humanitarian practitioners have made use of the enhanced situational awareness and actionable information afforded by the digital age. There are many examples, but I'll note a few now: they've employed remote sensing tools for augmenting conflict early warning capacities and documenting human rights abuses. They have leveraged mobile data solutions for tracking the conditions, profiles and routes of transit of migrant and refugee populations; extracted metadata from call detail records to understand the spread of infectious diseases; harvested social media for sentiment analysis and rumour tracking in fragile contexts; and of course, they've deployed aerial robotics for surveillance of damaged locations and monitoring critical infrastructure.

In the case of COVID-19, digital tools, artificial intelligence[19] and "big data" analysis are being used in various contexts to support health-based responses. They can help us collect, analyze and transmit critical information in order to organize health resources and capabilities, accelerate medical logistical and procurement chains or manage the public safety and security dimensions of confinement.

Digital information technologies can be valuable for exchanging key information and thus for advancing medical and epidemiological research in laboratories. In terms of prevention and awareness, information applications for sharing relevant and accurate information with affected populations have also been widely used during the COVID-19 crisis. They have come with different models, interfaces, content, and levels of privacy compliance and security. Overall, when associated with and validated by official public health agencies, these apps are useful for helping to improve the awareness and level of information of the population, who are then better equipped to take appropriate measures in terms of prevention and wellness.

Overall, there are many different digital tools that are being promoted and discussed in the context of the COVID response. They can play different roles and functions depending on their purpose and design, but also on the moment and places in which they are deployed and used. Thus, while digital technologies can be helpful to the COVID response, the analysis of their relevance, data protection compliance

[19] Shana Lynch, "Artificial Intelligence and COVID-19: How Technology Can Understand, Track and Improve Health Outcomes", *Stanford Institute for Human-Centered Artificial Intelligence Blog*, 1 April 2020, available at: https://hai.stanford.edu/blog/artificial-intelligence-and-covid-19-how-technology-can-understand-track-and-improve-health.

and adequacy needs to be systematically pushed further and be based on a case-by-case and contextualized assessment, as their relevance and added value will vary widely.

Massimo Marelli: I think digital information and communication systems can have positive effects if we regulate them properly. For example, data protection laws ensure that digital technologies can be used in ways that bring "digital dignity" or "data dignity", by giving the data subject the information, control and rights that they need to exercise control over how information about them is used. These laws also seek to impose limits on what data controllers can do with our information, to ensure that we are treated fairly and not discriminated against or exploited. By incorporating these laws into our work, we can ensure that digital technologies' positive effects outweigh their negative ones. Based on this understanding, these fundamental principles for data protection are the basis for the ICRC's Rules on Personal Data Protection.[20] Of course, it's easy to say that it can be difficult to apply these principles to humanitarian action because of the circumstances on the ground, or because our beneficiaries "don't care" – but if we are serious about ensuring that digital technologies have an overall positive net effect, and we are serious about respecting the dignity of affected people, doing no harm, being accountable and retaining trust, then this is not good enough. We have no choice but to try to overcome these challenges and ensure that our actions meet up with the principles that define humanitarian work in this area.

Why should the humanitarian sector engage with the private sector's tech industry?

Delphine van Solinge: I'll take this one. The rapid evolution in technology, connectivity and data is driving multilayered changes in societies, and in the way we work and communicate. In humanitarian settings, this is affecting not only the expectations and needs of affected populations and other stakeholders, but also the way humanitarian programmes and services can be delivered.

While offering new opportunities for the humanitarian sector to implement and scale its response, the digital transformation is also creating new and/or amplified risks for conflict-affected populations. Yet, the digital transformation of societies and businesses is no longer something you can really opt out from. It is happening, and we need to learn to live and work with it.

The humanitarian sector has a double obligation to look into the relevance of digital solutions and find the right type of ethical engagement with the tech industry. The first reason for this is because technology and data have the potential to improve humanitarian responses and therefore help alleviate the suffering of affected populations. The second reason is because these technologies, depending on their uses and misuses, can create risks for populations and/or damage the credibility of humanitarian organizations. This potential for improved humanitarian response through the use of digital technologies needs to be

[20] ICRC, above note 11.

analyzed, understood, explored and deployed responsibly, following the "do no harm" principle and relevant rules of data protection.

In the same vein that the humanitarian sector can learn from the tech industry in designing a more efficient response, the tech industry can learn from the humanitarian sector in thinking beyond its labs, in understanding the real-world consequences that "technocolonialism"[21] can have on the lives and safety of affected populations, and in jointly finding ways to mitigate those consequences.

Massimo Marelli: I think Delphine has just about covered what I would have to say on this front. I echo her statement that we can no longer "opt out" from digital transformation processes, and we see this with the dominance of the private sector's tech industry. On our end, in the humanitarian sector we have an obligation to engage with these actors and to ensure that we adapt our work in such a way that we continue to put the safety and trust of affected people first in our operational work.

Are social media giants responsible for having policies that protect affected populations from widespread misinformation or disinformation campaigns?

Massimo Marelli: I think Delphine is best placed to speak to this.

Delphine van Solinge: Thanks, Massimo. Well, I think it is a shared responsibility. MDH does not happen in a vacuum; it is rooted in history, societal behaviours, chronic tensions and politics, to name just a few factors.

The platforms are not the cause of the spread of harmful information *per se*; they certainly have a role in amplifying, magnifying and increasing the speed of how information is shared, but they do not initiate the post. This should not be interpreted as a way for social media companies to "wash their hands" and do nothing about the dangerous content that is mushrooming on their platforms. Since they provide this lucrative service to people, where algorithm, artificial intelligence and data analytics play a major role in making content more or less visible and accessible based on one's profile, interest and/or social behaviour, they have a responsibility to put in place the necessary mitigating policies and technical measures to limit the spread of information in ways that can be harmful for individuals.

During the COVID crisis, many social media platforms, such as Facebook and Twitter, have taken steps to limit, for example, the amount of misinformation circulating around curative treatments which could clearly have lethal consequences

[21] "Technocolonialism", as defined by Mirca Madianou, refers to "how the convergence of digital developments with humanitarian structures and market forces reinvigorates and reshapes colonial relationships of dependency". See Mirca Madianou, "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises", *Social Media and Society*, Vol. 5, No. 3, 26 July 2019, available at: https://journals.sagepub.com/doi/full/10.1177/2056305119863146.

for people – that is, incorrect and potentially harmful medical advice.[22] While many people would argue that such information is obviously and totally false, in the midst of a health crisis, the fear of death can make people think irrationally. In situations of armed conflict and even dormant violence, primal fears and survival instinct can be easily tapped into. Posting and circulating alarming or decontextualized information in these circumstances can foster polarization, increased stress and fear, unreasonable behaviours and, ultimately, violence.

This is why it is important to look at the different actors, roles and responsibilities beyond the platforms. Politicians, authorities and civil society have a responsibility and a role to play, in their different capacities and functions, to help limit the creation and spread of MDH on social media. However, we also need to be realistic: misinformation and disinformation are deeply rooted into politics, power and social behaviour, and as such, they will continue to be used in different ways, shapes and forms. What can be done, however, is that we can increase people's resilience to MDH by promoting digital literacy, critical thinking and – let's be idealistic a notch – humanitarian values.

What are the benefits and disadvantages of affected populations having increased access to digital connectivity?

Delphine van Solinge: I'll let Massimo take this one.

Massimo Marelli: Thanks, Delphine. First, let me start by saying that we have to see connectivity as a fact of life and not simply as a challenge or opportunity. As more and more social and material life moves online, and more and more of the world is connected, humanitarian organizations have no choice but to carve out a presence in the online spaces that affected populations congregate in, leverage new resilience mechanisms that are enabled by connectivity, and factor connectivity into their programming. This can be relatively simple, for example by providing "connectivity as aid"; but it can also be more complex, for example where new digital services are concerned. Beyond data protection compliance – and remaining fully responsive to the needs of those who are not connected – we see the main challenge as one of responsible innovation. We have to invest in building safe and protected digital humanitarian spaces where we can be confident that we are actually doing no harm as well as working within the confines of digital environments as we find them today. This is far from easy. It means educating partners, States and technology providers as to why these spaces

[22] For example, Google is removing false or misleading information about COVID-19 from its various platforms and in advertisements; see Sundar Pichai, "COVID-19: How We're Continuing to Help", *Inside Google*, 15 March 2020, available at: https://blog.google/inside-google/company-announcements/covid-19-how-were-continuing-to-help/. Twitter now verifies tweets and Twitter accounts for the credibility of information they offer, and has put in place informative #KnowTheFacts search prompts; see "Coronavirus: Staying Safe and Informed on Twitter", *Twitter Blog*, 3 April 2020, available at: https://blog.twitter.com/en_us/topics/company/2020/covid-19.html.

are needed and working with them to develop the infrastructure and applications that neutral, independent and trusted humanitarian action requires.

What are some of the ethical implications of, for example, using digital technologies, such as facial recognition software, to identify missing persons? How do these ethical considerations shape the ICRC's work?

Massimo Marelli: Ethics and data protection frequently overlap. Data protection laws, like most laws, are in the end a reflection of the responses that societies give to ethical questions and the rules they decide to give to themselves to stay loyal to those responses. I think that in the context of the technologies you've mentioned, the key questions are: can these technologies bring real benefits to the ICRC and affected populations, on the one hand, and can we utilize them responsibly and accountably, keeping the affected populations at the centre, on the other?