RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 096 – 18 June 2021

Humanitarian 'Do No Harm': Plugging Gaps in Data Governance

By S. Nanthini

SYNOPSIS

Data analytics have become a central component of humanitarian work. This is used to inform what affected community needs are and where they need them most. For communities who are already vulnerable, if their data is misused or shared with actors who are not bound by humanitarian principles, they can be exposed to additional risks.

COMMENTARY

FOR HUMANITARIAN actors, the principle of "do no harm" is vital to their work and must apply in all areas – including data handling. While data has long been a necessity in the humanitarian sector, technological advances has meant that data sharing has become easier. This in turn increases the access and availability of assistance that can be provided to vulnerable communities.

Unfortunately, there has also been an increase in the risk that sensitive information can fall into the wrong hands – harming the very people that humanitarian actors are seeking to help. Moreover, with the ongoing COVID-19 pandemic and governments around the world mostly centering technology in their responses, the discourse around the management of sensitive data has gained a renewed sense of urgency.

Data Privacy: A Significant Concern

Humanitarian work in particular can deal with highly sensitive and/or strategically important data. For example, the use of sensitive data in conflict and disaster settings allows the identification of vulnerable communities. Should this information be leaked, it may further expose them to risks such as human trafficking or deportation.

As such, protecting people requires humanitarian actors to not just be aware of, but

also address the threats associated with technology, including the exploitation of humanitarian data for surveillance purposes by governments and private companies.

Data privacy is a significant concern. COVID-19 has further brought into prominence the discourse around the collection and management of highly sensitive data. A key tool used by governments around the world, contact tracing measures via mobile-phone apps are being used to trace the movements of people to identify those who might have come into contact with someone who has COVID-19.

While useful in determining exposure, the necessarily invasive nature of these apps also makes it a useful tool to monitor civilian movements even after the pandemic ends – as is already being proposed. In the United Kingdom, the data of users of the contact who test positive for COVID-19 will be kept in the system for eight years.

Although the government has said that this information will not be used for non-pandemic purposes, they have previously made data useful for immigration enforcement exempt from data protection laws – an exemption which may be repeated.

Gaps in Data Protection: Illegal Attempts to Access Data

The discovery of the security vulnerabilities in the Red Rose system in 2017 and the 2020 ransomware attack on US-based Blackbaud which affected major INGOs such as Oxfam and World Vision are stark reminders of the possibilities of data leakage of already-vulnerable populations. With this near-constant data breach attempts, how certain are humanitarian organisations of keeping valuable data safe in the face of active attempts to gain entry into their systems?

However, as seen by the high-level data breaches of various organisations and agencies, there is only so much an organisation can do to completely protect itself. Therefore, organisations should also be aware of the existing vulnerabilities in their system and rather than rely solely on security software, they should work in such a way as to mitigate the level of harm in the event of a breach.

Importantly, organisations should follow its own data protection policies. While a range of policies and guidelines have been set up by organisations including UN bodies and the Red Cross, implementation have been mixed.

For example, the 2017 internal audit of the World Food Programme revealed gaps in staff implementation of their data policies. This includes the consent practices, assessment of privacy risk, collection of unnecessary data and insecure data sharing despite the presence of an existing data security framework.

Advancing Data Governance in Southeast Asia

With business and other organisations forced to move online for the foreseeable future due to COVID-19, the use of data in Southeast Asia is higher than ever. One such online platform that has emerged as a response to the ongoing pandemic is Malaysia's KitaMATCH.

A collaboration between the government, civil and private sectors, this hub was created to match needs with contributions on a single platform to prevent aid fragmentation – and reduce the strain on already stretched resources.

With privacy a significant concern for a platform reliant on data analytics to help vulnerable communities, measures taken by KitaMATCH to protect data security include only collecting directly relevant data and aggregating it at the NGO-level.

The current digitalisation boom may be an opportunity for stakeholders to further advance data governance in the humanitarian sector. For example, RSIS and the ICRC recently co-hosted an online workshop on "Data Governance and Protection in Humanitarian Action".

This event brought together humanitarian actors from different organisations to discuss the relationship between data protection and humanitarian action. Similarly, humanitarian actors could also partner with other sectors, to generate further discussion on data governance and how the principle of "do no harm" can be applied in a digital age.

Humanitarian Action: Do No Harm

For humanitarian actors, the policy of "do no harm" must be extended to their protection of data. Although COVID-19 is accelerating the need for digitalisation, humanitarian organisations must still take the time to ensure that any adoption of advanced information systems and technologies be undertaken after a thorough internal review.

Only with a thorough understanding as to its possible benefits and harms, can these actors ensure a balance between data gathered for an informed response and ensuring this data cannot be used to harm.

Going forward, as these advanded systems and technologies are increasingly used in the humanitarian sector, data will become an inextricable and inherent part of humanitarian action. Data security and data governance must be treated as a critical feature for the protection of the vulnerable communities that are being assisted.

S. Nanthini is a Research Analyst with the Humanitarian Assistance and Disaster Relief (HADR) Programme at the Centre for Non-Traditional Security Studies (NTS Centre), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.