The two sides of the digital response to the COVID-19 crisis

By Jennifer Easterday and Margherita Parodi

The COVID-19 crisis has unveiled the key role digital technologies play in societies at the global level. Amidst the health crisis, companies have often shown great initiative to use these technologies to educate the public, tackle disinformation and ensure data transparency[1]. However, digitalisation must be handled with care, as it also has the potential to negatively impact communities' human security.

This is not the first time businesses make use of digital technologies to address the challenges of a global crisis: in 2010, after a devastating earthquake hit Haiti, telecom companies such as Digicel partnered with the public sector to deliver health and safety messages to the public[2]. Today, to help address the COVID19 Pandemic, Digicel Tonga is assisting the Ministry of Health and the MEIDECC with the spread of relevant information using its TV channel and communications network[3]. Another telecommunications company, BT Group, is partnering with digital tech organisations to provide resources and information to educate members of the community with little or no digital skills. Through the Skills for Tomorrow initiative, BT aims to have a positive impact on digital literacy, safety online and future innovation, as well as to increase tech talent in the UK[4].

Facilitating communication and online education is only a portion of the corporate usage of digital technologies. Government-business partnerships made substantial use of digital technologies to develop contact tracing apps, which use location tracking or proximity tracking to identify when a user has been near someone who has been diagnosed with COVID-19. While an important tool for stemming outbreaks of COVID-19, these tools need to incorporate appropriate privacy safeguards and security. Technologies aimed at developing contact tracing tools may pose a risk for human security in some vulnerable communities—especially those with a history of conflict, authoritarianism or mass human rights violations. A few examples of worrisome tech tools include:

- China built a mandatory smartphone app to track peoples' movements; impose restrictions on movement, and which appears to send personal data to police.
- In Guatemala, a contact tracing app collects data about users' exact location, even when the app is closed. The data can be held for up to ten years, and the President has indicated that he hopes the app will evolve to cover "security issues."
- In Ethiopia, the state released a COVID-19 monitoring platform where users can report others suspected of having symptoms—based on subjective assessments of their symptoms.

The ICRC warns that the "unsuitable design or usage of such apps could lead to stigmatization, increased vulnerability and fragility, discrimination, persecution, and attacks on the physical and psychological integrity of certain populations."

COVID-19 tech tools simultaneously pose several serious risks to human security, yet also have the potential to enhance human security in the face of the threat of health, social and economic disruption. Finding the balance between using digital technologies to improve individuals' ability to work and communicate and to ensure no threats are being posed to human security is challenging. It

[1] ODI (2020)

[2] Bailey, S. (2014) "Humanitarian crises, emergency preparedness and response: the role of business and the private sector - A strategy and options analysis of Haiti"

[3] International Institute of Communications https://www.iicom.org/covid-19-what-digicel-group-is-doing-to-help/

is imperative that governments, policymakers, civil society and the tech industry work together to develop adequate regulation and enforcement mechanisms so that the potential of tech is realised without the additional risks it currently poses.