joep lange
institute

DIGITAL TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE IN HEALTH II: HUMAN RIGHTS PRINCIPLES

Background paper for civil society delegations on the Global Fund Board for a new era of aid

Author: **Sara L.M. Davis**

July 2020

In 2019, the UN Secretary General convened a global multi-stakeholder dialogue, chaired by Melinda Gates and Alibaba founder Jack Ma, "on how we can work better together to realize the potential of digital technologies for advancing human well-being while mitigating the risks". The resulting report included a recommendation to "respect human rights", while noting concerns about digital ID systems (UNSG 2019, 29). At the same time, other UN agencies were also developing guidelines and standards for digital technologies in their sectors, while the tech sector had already collaborated to develop several sets of ethical principles.

Many of those engaged in governance of this fast-moving sector are playing what can feel like a losing game of catch-up, with the economic and social forces driving the digitalization of all aspects of our lives at a high speed, while governance and policy lag behind. However, many of the issues raised by digital technologies and AI are longstanding issues that are shaped by existing discrimination and inequalities. The experience of communities and civil society living with, affected by and working to respond to HIV, TB and malaria have much to offer. As the largest multilateral funder for health, and a donor with established partnerships across government, civil society and the private sector, the Global Fund offers a key platform for advancing rights-based governance of digital technologies for health.

This paper provides an introductory overview to these concerns and the available analyses and tools, before considering some of the analysis developed by UN human rights experts and how these could be useful in the work of the civil society delegations on the Global Fund Board.

A. ABOUT DIGITAL TECHNOLOGIES AND AI FOR HEALTH

The COVID-19 crisis has accelerated a shift towards new digital technologies which was already underway. Faced with the challenge of a highly contagious new virus, and no treatment or vaccine, a small but growing number of developing countries are rapidly implementing new digital technologies to strengthen traditional health systems, for tasks ranging from digital contact tracing to diagnosis. These and other new digital technologies also offer opportunities to fulfill the Sustainable Development Goal on health.

Digital technologies enable faster and larger-scale epidemiological surveillance, contact tracing, and tracking population movements to target health interventions. These new tools and software can enable remote consultation by patients with doctors, and by doctors with medical specialists (aka telemedicine), and remote diagnosis (telepathology). Many hospitals now utilize electronic health records, sometimes linked to digital identities, which may draw on verification of identity using biometric information (ranging from fingerprints to iris scans and facial recognition software). Mobile phones and computers also now facilitate public health education. Health providers can now use digital technologies to track and manage supplies and goods, and to restock supplies. Through budget monitoring, these tools can also facilitate efficiency and transparency in health finance and procurement processes.

Through mobile networks and blockchain, it is possible to distribute risk across larger pools of users, and to send direct financial transfers to individuals in need. And new digital tools can facilitate the work of community advocates, such as women and girls at risk of gender-based violence, who may use online tools to document abuses and advocate for gender equality (GBV AoR Helpdesk).

Many of these technologies either utilize or inform artificial intelligence (AI): the use of computer systems to analyze very large quantities of data in real time, spot patterns and trends, and make decisions. These systems are increasingly developing the ability to learn from experience. In health, AI is used increasingly for medical image analysis. AI is used for other purposes in the private sector (judging creditworthiness, for example) and in the public sector, especially in law enforcement and national security (to predict risk of recidivism, terrorism risks, and to manage prison populations). In China, perhaps the most sophisticated in its development of AI for law enforcement, police use AI that is informed by CCTV video, social media posts, online purchases, travel and facial recognition software.

In fact, China is an example of what the future could hold for other countries. It has been praised for sophisticated use of AI and big data as part of its management of the coronavirus. The government requires citizens to download an Alibaba app (Alibaba is a $500 billion e-commerce company founded by Jack Ma, co-chair of the UN High-level Panel on Digital Cooperation). The app was developed in partnership with the police, and uses a color code to identify those free to travel, at risk, or in need of immediate quarantine, based on data including their travel history and time spent in proximity to others with the virus (Holmes 2020). Subway stations use thermal scanners to check for high temperatures, and also incorporate facial recognition technology (Yuan 2020).

But worryingly, these tools were developed by some of the same private technology companies (such as Megvii) responsible for developing the AI systems used by Chinese authorities to racially profile and imprison hundreds of thousands of Uighur Muslims. These systems track individual communications, police records, patronage at mosques, and individual movements to identify people considered high risk, who are placed in detention in abusive reeducation camps (Grant 2020). It is even more concerning that China is actively exporting these same AI surveillance technologies to over 60 developing countries, in part through the Belt and Road Initiative (Feldstein 2019).

However, even in China, despite active suppression of civil society and human rights defenders, there continues to be a live debate about the limits of surveillance and privacy rights, including about the use of facial recognition software in the public subways (Shen 2020). This is important to remember, as one of the challenging aspects of the expansion of government use of technology is that it is frequently presented as inevitable: as Alston writes, "crucial decisions to go digital have been taken by government ministers without consultation…Sometimes there seems to be a presumption that even if the move to digital is not currently necessary, it surely will be one day and it is better to move in advance," a move promoted by private corporations with a vested interest (UNGA 2019, 17). Thus, it is a hopeful sign that even in societies with little civic space for NGOs, the limits and governance of digital technologies continues to be actively debated by lawyers and rights experts.

International human rights experts and organizations have begun to analyze the risks linked to digital surveillance and artificial intelligence-led decision-making, and have chiefly focused on civil and political rights issues such as privacy and the impact of digital media on freedom of expression and democratic debate, with less analysis of the related impact on economic and social rights such as the right to health. The rapid expansion of surveillance during the COVID-19 crisis is shifting the focus of the debate. At the same time, global health agencies have been more inclined to embrace the possibilities offered by new digital technologies and "AI for good", with less consideration of human rights concerns.

Civil society groups with experience and expertise in HIV, TB and malaria can help to bridge these two conversations. For HIV and TB, the right to health is clearly dependent on other rights, including the right to non-discrimination, rights in relation to the police and the criminal law, and right to freedom of association (especially for key populations who have had to litigate and advocate in some countries in order to establish NGOs and to do outreach and share information), to name a few. Now is an opportune moment to bring that experience into the conversation.

The next section of this paper briefly introduces standards used in governance of the private sector. It then reviews and responds to white papers developed by UN expert bodies and human rights experts in the past few years, before considering how to raise these issues at the Global Fund.

B. GOVERNING THE TECH SECTOR

Governing the private sector is obviously central to all the concerns discussed below. Zuboff's groundbreaking 2019 book, The Age of Surveillance Capitalism, exhaustively showed how corporations such as Facebook and Google turned data into a source of profit. She urged the breakup of big tech in order to create openings for competition by smaller, more privacy- and consumer-minded alternatives. Worryingly, many new public-private partnerships in development aid include agencies with problematic ethical track records, such as data-mining firm Palantir. In 2018, the World Food Programme's new five-year, $45 million partnership with Palantir was criticized by civil society groups due to the company's history of collaboration with the Los Angeles and New York Police Departments, Immigration and Customs Enforcement, the NSA, the FBI, and the U.S. Army on surveillance and tracking projects, among others (Greenwood 2019). WFP issued a statement affirming that it would place strict controls on access to and use of data by Palantir, but advocates continued to raise concerns about the lack of transparency in Palantir's pricing and algorithms.

The tech sector has not been blind to criticisms, and has worked through a variety of professional associations to develop standards for self-governance. These are useful to consult because they identify specific risks and thinking unique to this sector. The foremost among these is the IEEE (Institute of Electrical and Electronics Engineers) ethics framework, Ethically Aligned Design, which breaks down a set of principles to guide AI creators and users through an ethical approach to design and use of artificial intelligence. These comprehensively address such values as well-being, affect (systems designed to shape behavior ["nudging'] and show emotion), personal data and individual agency, sustainable development, and the problems of embedding universal values into autonomous systems.

Related work has been undertaken to develop the Asilomar Principles, which emphasize the importance of benevolent purposes of artificial intelligence research development; and by the robotics researchers who developed the Principles of Robotics, which assert that robots should not be designed as weapons, should comply with existing laws (for instance on privacy), should be safe and transparent, and should not create illusions of emotions to exploit users, for example. Further analysis of ethics of artificial intelligence in the future explore the questions raised by the idea of a future singularity, in the event that artificial intelligence one day exceeds human intelligence (Muehlhauser and Helm 2012).

However, critics have argued that the development of ethical standards for tech self-governance -- including the establishment of ethics and AI research teams at MIT, Google, Microsoft and IBM for example -- has been little more than a cynical effort to avoid litigation. Ochigame argues that the tech sector faces three possible scenarios:

1. no legal regulation at all, leaving "ethical principles" and "responsible practices" as merely voluntary;
2. moderate legal regulation encouraging or requiring technical adjustments that do not conflict significantly with profits; or
3. restrictive legal regulation curbing or banning deployment of the technology.

"Unsurprisingly," he concludes, the tech sector would prefer to govern itself with ethical principles than be subject to law (Ochigame 2019).

Given these concerns, it is important to also become familiar with how human rights standards – which do have the status of law and which have been developed over decades of court adjudication – can also be used to govern the tech sector.

A key tool for this purpose is the UN Guiding Principles on Business and Human Rights, developed by a commission led by Jacques Ruggie. The Ruggie Framework interprets the human rights obligations of both states and the private sector, including development aid agencies, under human rights law. This "Protect, Respect, Remedy" framework asserts three things:

1. The state's duty is to protect against human rights abuses by third parties, including businesses.
2. Corporations have a responsibility to respect human rights, by doing due diligence in order to avoid infringing human rights, both through a corporation's own activities and through its value chain. As the Ruggie Framework outlines, it is not enough for companies to state that they respect human rights; they must also "know and show" that they have done due diligence in order to identify, prevent and address human rights abuses.
3. Both the state and businesses have a responsibility to ensure access to effective remedy for victims, both through the courts and through non-judicial remedies.

The European Union's ICT Sector Guidance on Implementing the Guiding Principles helps to apply the Ruggie Framework to the tech sector.

With this "Protect, Respect, Remedy" framework in mind, what are the risks that companies and governments should be investigating and preparing to address? The next section explores these issues in more depth, drawing on UN and human rights experts' white papers.

C. UN AND HUMAN RIGHTS ANALYSIS

1. The UN High-level Panel on Digital Cooperation, and the "digital divide"

The first concern to consider in financing digital technologies for health is that access is far from universal. The "digital divide" shapes lack of access to digital services for much of the world's population due to poverty, marginalization and displacement, as well as other inequalities.

The UN High-level Panel on Digital Cooperation was appointed in July 2019 to consider digital cooperation in achieving the SDGs, and to consider governance of the digital sphere. The panel, chaired by philanthropist Melinda Gates and Chinese tech leader Jack Ma (chair of Alibaba Group), included leaders in government, the tech sector, scholars, civil society leaders and other experts, who surveyed the issues overall and produced a report and recommendations.

In particular, the panel raised the digital divide as a concern. It recommends that "by 2030, every adult should have affordable access to digital networks, as well as digitally-enabled financial and health services, as a means to make a substantial contribution to meeting the SDGs" (UN 2019, 4). At the same time, it notes the need to ensure access is guided by human rights norms and frameworks, and calls on all actors to "adopt specific policies to support full digital inclusion and digital equality for women and traditionally marginalized groups" (UN 2019, 4).

Indeed, communities most vulnerable to HIV, TB and malaria have limited access to such tools as mobile phones or laptops. The UN High-level Panel on Digital Cooperation notes that women face "particular challenges in meaningfully accessing the internet, inclusive mobile financial services and online commerce, and controlling their own digital IDs and health records" (UNSG 2019, 29). As humanitarian service delivery in conflicts, emergencies and displacement settings increasingly rely on mobile phones, these programmes may leave out many women and girls who are only able to access digital technologies through their partners or family members (GBV AoR Helpdesk DATE, 8). Similarly, NGOs such as AccessNow have advocated to end the digital divide, and has campaigned against government shutdowns of the internet during COVID-19 outbreaks because it impedes access to life-saving services and information.

The UN High-level Panel on Digital Cooperation restates that respect for human rights remains fundamental in digital technologies, as "human rights apply fully in the digital world" (UN 2019, 29). It also urged the UN Secretary-General to institute an agencies-wide review of how existing international human rights accords and standards apply to new and emerging digital technologies. Civil society, governments, the private sector and the public should be invited to submit their views on how to apply existing human rights instruments in the digital age in a proactive and transparent process (UN 2019, 30).

In addition, the panel called on the private sector to work with governments, civil society and other experts to ensure that artificial intelligence systems are transparent, accountable and designed in ways "that enable their decisions to be explained and humans to be accountable for their use" (Ibid.).

While the report helpfully frames these overarching concerns, including the digital divide, it skims the surface of the human rights risks while focusing on the positive opportunities – perhaps because its co-chair and many members are themselves deeply interested in promoting digital technologies. For a more specific explanation of the risks, we need to turn to UN human rights experts.

2. UN Human Rights Analyses

Human rights is a system of laws, norms and standards that articulate fundamental human rights principles as obligations that uphold human dignity. The core human rights treaties have been ratified by most countries and are legally binding. States, as duty-bearers, have the obligation to respect, protect and fulfill these standards through their internal governance, national laws and through national court systems. They are held accountable by a peer review system, in which UN human rights treaty bodies and the UN Human Rights Council periodically review states' performance, with input from civil society and other experts, and issue recommendations to which states are held accountable.

UN Special Rapporteurs operate as independent experts, investigating specific issues or countries in line with their mandates. The human rights framework continues to evolve, with new standards taking effect – for instance, with the rights of persons with disabilities, which were only recently recognized. At an early stage of development of the human rights analysis of a given problem, UN human rights special rapporteurs often do the initial analytical work, which may lead to resolutions by the UN General Assembly, recommendations by UN treaty bodies, or other applications of their analyses in human rights law. For example, the UN Special Rapporteur on the Right to Health has developed analyses of the rights of people who use drugs to harm reduction and to freedom from torture, and this thinking has influenced other parts of the UN to uphold the rights of people who use drugs.

As digital technologies and AI are a new area of work for human rights experts, this initial thinking has been developed quite recently by two UN Special Rapporteurs: the UN Special Rapporteur on Extreme Poverty and Human Rights, Philip Alston, and the UN Special Rapporteur on Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye. They have identified a related set of issues, discussed below:

- The rise of a "digital welfare state"
- The debate over digital identities, and related debates over biometrics
- The right to privacy and effective data governance
- The risk of algorithmic bias
- The use of AI for malicious purposes

A. Rise of a "digital welfare state"

In October 2019, the UN Special Rapporteur on extreme poverty and human rights, Philip Alston, delivered a report to the UN General Assembly that set out concerns about digital technologies in social protection, or "welfare" (UN General Assembly [UNGA] 2019). The report was significant as the first UN human rights report to consider the impact of digital tools and AI on economic and social rights. It was preceded by a one-day consultation with European human rights groups hosted by the Digital Freedom Foundation (Reventlow 2019).

Alston's report notes that digital technologies used in welfare are now widespread, and acknowledges their appeal, but also warns of "a grave risk of stumbling zombie-like into a digital welfare dystopia". With the rapid increase in automation, prediction, surveillance and other functions, Alston warns that the consequence is often a reduction in economic and social rights, rather than an expansion; and that the effect of these technologies is to reduce state accountability (UNGA 2019, 4). In the name of efficiency and fiscal consolidation, he writes,

> Often...the digitization of welfare systems has been accompanied by deep reductions in the overall welfare budget, a narrowing of the beneficiary pool, the elimination of some services, the introduction of demanding and intrusive forms of conditionality, the pursuit of behavioral modification goals, the imposition of stronger sanctions regimes, and a complete reversal of the traditional notion that the state should be accountable to the individual (UNGA 2019, 3).

Alston reviews the development of digital identities, automated eligibility assessments for benefits, benefit fraud detection and prevention, risk scoring, communications between beneficiaries and welfare authorities, and points out the ways that these new approaches actually make welfare benefits less accessible, creating bureaucratic hurdles for beneficiaries, while reducing transparency.

He concludes by urging all such systems to be built on respect for human rights, by ensuring legality and transparency in the design of tech systems; promoting equality in digital systems (so that access is not limited to those with digital literacy and tools, or with high-speed internet); protecting economic and social rights for all and not requiring access to depend on applicants' meeting rigid systemic rules; and protecting civil and political rights by not using digital technologies to expand surveillance (UNGA 2019, 16).

In particular, he underscores the importance of the human rights to social protection and to social security (UNGA 2019, 14). He points out that the expansion of digital welfare states often undermines a human right to dignity, which the Human Rights Committee says should be upheld through "measures designed to ensure access without delay by individuals to essential goods and services such as food, water, shelter, health-care, electricity and sanitation, and other measures designed to promote and facilitate adequate general conditions ... ." (UNGA 2019, 15).

Alston's important report raises areas of concern that have also been raised by others: the rise of digital identities, privacy rights, and the risk of algorithmic bias in autonomous decisions.

B. Digital identities

Many UN and development actors are embracing digital identities for identity verification and to enable access to health services, including for millions of people who lack birth registration. The World Bank, USAID and others have promoted this approach, sometimes in partnership with private sector actors that may benefit financially, such as MasterCard (World Bank and Center for Global Development 2017).

Alston warns of risks to privacy and cybersecurity and points to controversies that have emerged in roll-out of digital identities in India and Kenya (UNGA 2019, 6). In India, critics of the Aadhaar 12-digit unique identifying number that links to demographic and biometric information have warned of breaches of privacy, given the lack of strong legal protections in India (Gopichandran et. al. 2020). After several lawsuits, India's Supreme Court upheld the right to privacy, finding that registering for an Aadhaar number must be voluntary, and that it should not be a condition of access to health services. Nonetheless, Gopichandran et. al. find that in practice it is often still insisted on by health care workers (Ibid., p. 278). The Kenyan government has also begun requiring a national ID, the Huduma Namba, which is linked to biometric data, in order to access welfare benefits. Litigation resulted in a court decision to make the number voluntary. However, here again, voluntariness may not always be real in practice (UNGA 2019, 6-7).

Similarly, in the UK, Kuntsman and colleagues (2019) find a lack of voluntariness:

they find a discrepancy between the information presented to digital health app users and the apps' actual handling of user data, and that in reality there is no "opting out".

C. The right to privacy and effective data governance

A series of reports by the UN Special Rapporteur on Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, highlight the systematic use of surveillance and other technologies to violate privacy rights. This includes the surveillance and targeting of human rights defenders and journalists, sometimes leading to arbitrary detention, torture and extrajudicial killings (UN HRC 2019). In 2013, the UN General Assembly adopted a resolution 68/167 expressing deep concern at the negative impact of surveillance on human rights.

The rapid scale-up of digital technologies in the COVID-19 response has intensified these concerns about privacy, given that states are putting in place expansive systems of surveillance for COVID that in some cases may later be utilized for other political purposes. In addition, even where states do not retain the data for other purposes, the data gathered for digital contact tracing apps could enter the public domain, as was the case in Singapore and South Korea. This could expose women to risks of violence given gender inequalities; and could expose marginalized groups in the atmosphere of blame around COVID transmission (Davis 2020).

Biometric data-gathering has also sparked related protests by key populations groups, out of fears of function creep, with police gaining access to health data and using it to target individuals for arrest (KELIN 2018). The Global Commission on HIV and the Law similarly warns of the risk of digitally-collected health information being used by the police or for commercial purposes (2018, 8).

These concerns are amplified in settings of conflict and displacement: in 2019, the ICRC adopted a biometrics policy to limit use of biometric data and address data protection risks, including risks that states or non-state actors would use data gathered for humanitarian purposes to target individuals or groups for harm (Hayes and Marelli 2019). The resulting ICRC biometrics policy is a useful model for advocacy with other agencies. It sets out legitimate uses of biometric data, commits to impact assessments for data processing, and sets out constraints on partnerships with the private sector, among other things.

To address these concerns, a growing number of countries have new data privacy laws (Greenleaf 2019). These laws vary a great deal in strength and comprehensiveness. Some address only minimal data protections, including requiring informed consent, requirements for cross-border data transfers, and placing restrictions on data processing.

The European Union's General Data Protection Regulation (GDPR), which took effect in May 2018, may be the world's strictest data protect law. It creates unified provisions on data processing for both public and private actors, and creating restrictions on companies as to how they can gather and use individual data. It also imposes high fines on violations. Those processing personal data must respect seven principles:

1. **Lawfulness, fairness and transparency** — Processing must be lawful, fair, and transparent to the data subject.
2. **Purpose limitation** — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
3. **Data minimization** — You should collect and process only as much data as absolutely necessary for the purposes specified.
4. **Accuracy** — You must keep personal data accurate and up to date.
5. **Storage limitation** — You may only store personally identifying data for as long as necessary for the specified purpose.
6. **Integrity and confidentiality** — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
7. **Accountability** — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles (Wolford 2020).

In addition, GDPR gives individuals rights to be informed, to access the data, to rectify it, to erase it, to restrict processing, the right to data portability, right to object, and rights in relation to automated decisions and to profiling (Wolford 2020). The widespread application of GDPR has now caused other countries to contemplate reviewing their own laws in order to make them GDPR-compliant.

D. Algorithmic bias

Another important concern raised by Alston in his report on "digital welfare states" is the problem of algorithmic bias.

Algorithms are increasingly used for decision-making purposes, from search engine results and social media platforms which shape the news and information we receive, to artificial intelligence used to determine credit ratings and school placements. While algorithms project authority because they appear neutral, they are written by humans, and both their assumptions and the data used to create them may encode, perpetuate or even worsen existing inequalities and discrimination.

Algorithms remove human accountability from decision-making, leaving it unclear who should ultimately be held responsible for discriminatory decisions.

In the US, community-based researchers such as Hamid Khan have found that programs used by police to predict crimes leads to aggressive policing in communities of color where reported crimes rates may be higher (Moravec 2019; see also Stop LAPD Spying Coalition). The American Civil Liberties Union (ACLU) and a coalition of US civil and human rights organizations warned of risks of racial discrimination, and noted that the "complexity and secrecy of these tools" makes public accountability impossible (2016).

E. Governance of AI

Building on Alston's work, in her 2019 speech "Human rights in the digital age" UN High Commissioner for Human Rights Michele Bachelet raised related concerns about AI: she warned of a potential dark side to digital technologies and social media, including their use to drive violence and hate speech, the misuse of data and manipulation of voters, respect for rule of law and responsible governance. Security experts have documented the growing use of AI systems for malicious purposes, including to attack digital security (through phishing attacks, speech synthesis for impersonation, automated hacking, and data poisoning); physical security (attacks using autonomous weapons systems, micro-drones, or subverting cyber-physical systems (e.g. causing autonomous vehicles to crash); or through attacks on political security (e.g. analyzing human behaviors and beliefs based on data and manipulating these using targeted propaganda, deceptive videos, or other attacks aimed at subverting or manipulating democratic systems (Brundage et. al. 2018, 4) .

At about the same time as Alston's report, UN Special Rapporteur on Freedom of Expression, David Kaye, published a report to the UN General Assembly which set out a "human rights legal framework" for AI which interprets the rights to freedom of opinion, freedom of expression, right to privacy, obligation of non-discrimination, and right to effective remedy, among others, in relation to AI. Kaye's recommendations include that human rights standards should be central to companies' design and implementation of AI, and that AI regulation be developed in consultation with diverse stakeholders, including civil society. He urged stronger state recommendation, and also recommended that companies should take proactive measures to address algorithmic discrimination, including, at a minimum, addressing sampling errors (where datasets are non-representative of society), scrubbing datasets to remove discriminatory data and putting in place measures to compensate for data that "contain the imprint of historical and structural patterns of discrimination" and from which AI systems are likely to develop discriminatory proxies (UNGA 2019a, 18).

C. RECOMMENDATIONS TO THE GLOBAL FUND

The above list of human rights risks linked to digital technologies and AI is by no means exhaustive. It is concerning then, that to date, there has been no high-level statement or commitment by any of the global health agencies to addressing the human rights issues raised by UN special rapporteurs, or even consideration of the ethics principles developed by the tech sector, to health.

To date, the major commitment in relation to digital technologies by global health agencies has been the Digital Investment Principles which were endorsed by the Global Fund, GAVI, Unitaid, USAID, and others at the World Health Summit in 2018. These principles do not address human rights risks, but focus on collaboration, alignment with national plans, the need to quantify costs, track progress, and invest in country capacity.

Generally, health donors have been ready to express their commitment to human rights and equity in principle, but slow to integrate specific human rights standards grounded in law into their work. The Global Fund is the only health donor to have explicitly integrated human rights standards into its legal relationships with aid recipients, and this provides a basis that can be used in discussing digital technologies and AI in health.

While the Ruggie "Protect, Respect and Remedy" Framework was developed for the private sector, it applies to development aid actors, and it was the foundation of the Global Fund's approach to human rights standards and accountability in 2012. In keeping with that framework, the Global Fund and its PRs should "know and show" that they have done due diligence in order to identify, prevent and address human rights abuses linked to digital technologies in health. Country Coordinating Mechanisms (CCMs) should be assessing this as part of the development and implementation of financing. Risks to consider include:

- Risks in access created by the digital divide, particularly for women and girls and key populations
- Risks of weak national data protection and privacy laws, and weak enforcement of them by government and courts
- The risk that employing digital identities may actually reduce access to health services, especially for marginalized groups who avoid using digital identities or giving biometric data out of fear of stigma, discrimination and arrest
- The risk of privacy violations, especially for key populations and other marginalized groups, and women and girls
- The risk of algorithmic bias in technologies financed by the Global Fund
- The risk of surveillance and restrictions on freedom of expression for HIV, TB and key populations groups, as well as groups advocating for SRHR
- The risk of function creep and targeting of individuals and groups based on their behavior or ethnicity by malicious actors or hostile states

In addition, it would be reasonable to ask whether the Global Fund, UNAIDS or WHO have:

- Developed a position on these technologies and the related risks, and otherwise analyzed how these human rights risks could affect the ability to meet SDG 3 and related targets
- Analyzed how the Global Fund's minimum human rights standards apply to digital technologies and AI in the interventions it may finance
- Integrated consideration of these risks into risk assessment tools and protocols
- Done due diligence into the ethical and human rights track records of companies with which they do business
- Developed biometrics and data management policies, for instance like those used by ICRC
- Communicated risks, and mitigating measures, to country offices of UNAIDS and WHO, Global Fund country teams, technical assistance providers, the TRP, CCMs, and PRs, etc.
- Consulted with civil society and, in particular, communities affected by health issues, to understand potential risks and ensure their involvement in decision-making and accountability

At the national level, civil society activists should ask:

- Whether a national data protection exists and whether it adequately protects privacy: the EU has produced guidelines for conducting a data protection impact assessment
- Whether digital technologies have restrictions on purpose, use, and length of time to store data; adhere to data protection laws; use decentralized protocols; are monetized or charge fees for users that may impede access to health services; use targeted ads; are sharing or disclosing data with other users or for other purposes; or are developed by or rely on collaborations with companies that have a track record of human rights abuses
- Whether national strategies for HIV, TB and malaria include plans to advocate for stronger governance of data and digital technologies, including regulation of the tech sector

In addition to exploring these issues with global health agencies, the civil society delegations to the Board may wish to consult with the civil and political rights groups (such as Access Now, the Digital Freedom Fund, Privacy International, Article 19 and others) and the UN Special Rapporteurs who have engaged on these issues already. Many of these groups and actors will meet at the RightsCon which Access Now will organize from July 27-31. Civil society delegations could urge the new Special Rapporteur on the Right to Health (the current mandate holder's term expires in 2020) to issue statements or develop a report on digital technologies, AI and the right to health. They could also encourage members of their constituencies at the country level to raise these issues when their countries are reviewed by UN treaty bodies.

The health sector is in the early stages of developing strategies and approaches to governance of digital technologies in health. As these cutting-edge issues continue to evolve, it will be critical to have a strong and informed voice from civil society and affected communities at the center of their governance.

Sara L.M. Davis, 24 July 2020

SOURCES

American Civil Liberties Union et. al. 2016. "Statement of concern about predictive policing by ACLU and 16 civil rights, privacy, racial justice and technology organizations". August 31.

Brundage, Miles; Shahar Avin, Jack Clark, et. al. 2018. The malicious use of artificial intelligence: Forecasting, prevention and mitigation. Future of Humanity Institute, University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation, and Open AI.

Davis, Sara L.M. 2020. Contact tracing apps: Extra risks for women and marginalized groups. Health and Human Rights Journal blog, 29 April.

European Union. 2017. Guidelines on data protection impact assessment (DPIA). 13 October.

Feldstein, Steven. 2019. The global expansion of AI surveillance. Carnegie Endowment for International Peace.

Gopichandran, Vijayaprasad, Parasuraman Ganeshkumar, Sambit Dash and Aarthy Ramasamy. 2020. "Ethical challenges of digital health technologies: Aadhaar, India". Bulletin of the World Health Organization 98: 277-281.

Grant, Melissa Gira. 2020. "The pandemic surveillance state". The New Republic, 8 May.

GBV AoR Helpdesk. 2019. Harnessing technology to prevent, mitigate and respond to Gender-Based Violence in emergencies: Developments, good practices and lessons learnt. Guidance note, November.

Aaron Holmes. 2020. "China is reportedly making people download an Alibaba-backed app that decides whether they'll be quarantined for coronavirus". Business Insider, 2 March.

Global Commission on HIV and the Law. 2018. Risks, rights and health: Supplement. UNDP: New York.

Greenleaf, Graham. 2019. "Global data privacy laws 2019: 132 national laws and many bills". Privacy Laws & Business International Report 157: 14-18.

Hayes, Ben and Massimo Marelli. 2019. "Facilitating innovation, ensuring protection: ICRC Biometrics Policy". 2019. Humanitarian Law and Policy, October 18.

KELIN and the Key Populations Consortium. 2018. "Everyone said no": Biometrics, HIV and human rights, a Kenya case study. Report.

Kuntsman, Adi; Esperanze Miyake and Sam Martin. 2019. "Re-thinking Digital Health: Data, Appization and the (Im)possibility of 'Opting Out'." Digital Health 5: 1-16. DOI: 10.1177/2055207619880671.

Massé, Estelle. 2020. "Privacy and public health: The dos and don'ts for COVID-19 contact tracing apps". AccessNow, 4 May.

Moravec, Eva Ruth. 2019. "Do algorithms have a place in policing?" The Atlantic, September 5.

Muehlhauser, Luke and Louie Helm. 2012. Intelligence explosion and machine ethics.

Ochigame, Rodrigo. 2019. "The invention of 'Ethical AI'". The Intercept, December 20.

Reventlow, Nani Jansen. 2019. "Digital rights are *all* human rights, not just civil and political". February 27.

UN General Assembly. 2019. "Report of the Special Rapporteur on extreme poverty and human rights", A/74/48037, 11 October.

UN General Assembly. 2019a. "Report of the Special Rapporteur on promotion and protection of the right to freedom of opinion and expression". A/73/348, 29 August.

UN Human Rights Council (UN HRC). 2019. "Report of the Special Rapporteur on promotion and protection of the right to freedom of opinion and expression". A/HRC/41/35, 28 May.

UN Secretary-General's high-level Panel on Digital Cooperation. 2019. The age of digital interdependence.

Wolford, Ben. 2020. "What is GDPR, the EU's new data protection law?" GDPR.EU.

World Bank and Center for Global Development, Principles on identification for sustainable development: Toward the digital age. February 2017.

Yuan, Shawn. 2020. "How China is using AI and big data to fight the coronavirus". Al Jazeera, 1 March.

Joep Lange Institute
Paasheuvelweg 25, Tower C4
1105 BP Amsterdam Zuidoost
The Netherlands