

5 COVID-19, health tech, and sphere transgression in Ethiopia

Kinfe Yilma

Editor note

Yilma's essay challenges us to rethink the sector transgression framework by shifting our attention beyond private technological corporations to include state-owned enterprises, public health authorities, and international aid agencies—actors often assumed to operate in the public interest but whose power and influence can be equally opaque and unchecked. While the framework of sector transgression allows scrutinising the activities of technological firms as creating new dependencies and concentrating decision-making powers in the hands of a few corporate actors, Yilma expands this critique to reveal how the critical partnerships between public health bodies and aid organizations can function outside meaningful and robust regulatory oversight.

Introduction

Ethiopia's tech sector has seen considerable growth in the past decade, but it is still at a nascent stage. Hampered partly by the monopoly of the communications sector and restrictive regulation, the potential of the sector has remained underdeveloped. With recent reforms—including liberalisation of the sector and introduction of an enabling regulatory environment, the sector appears to be taking off. No less part of this new development is the broader national 'digital transformation' agenda. In the wake of the COVID-19 pandemic, Ethiopian health authorities have turned to the fledgling tech sector as well as long-standing international development partners as part of the national public health emergency response. Deploying a qualitative method, this chapter considers Ethiopia's technological response to the COVID-19 pandemic, and the attendant regulatory issues. It reveals that the notions of neither sphere transgression nor transition define the pandemic-induced measures in Ethiopia.

No technology company transgressed or transitioned into a new domain. What made the Ethiopian experience unique is that enhanced partnerships with the private sector formed the central part of the national pandemic response. The collaborative pandemic response was, however, carried out outside the purview of applicable legal and regulatory framework on public

private partnerships. Nor has Ethiopia put in place other pertinent policy instruments to ensure fairness, transparency, and accountability as well as respect for fundamental rights and freedoms in the course of deploying tech in public health emergencies. The chapter takes into account major developments until late 2022.

COVID-19 and health tech

Shortly after the first case of infection was reported, several firms—including local technology companies—rolled out contact-tracing applications (apps). One such app was developed by a local investment consulting firm called YHM Consulting which, through coders in a sister company named ZayRide involved in ride-hailing services, introduced a contact-tracing app named ‘COVID-19 Family Protect App’, later renamed ‘Ethio-Tracking’ (Fortune, 2020). But health authorities did not take up the offer of the firm to deploy the app as part of their contact-tracing endeavours. Instead, the Ministry of Health had briefly deployed another contact-tracing app called Debo—roughly meaning ‘to work collectively’ in Amharic—developed by Ewenet Communications PLC which has had pre-existing partnership with the Ethiopian Public Health Institute (EPHI), a body under the Ministry of Health directly involved in the campaign against the pandemic.¹ Launched on 14 July 2020—about five months after the first case was reported—the app was developed by the company solely on a voluntary basis (interview, 2020).² Before its use was discontinued, the app had approximately 500 downloads on Android.³

Much of the national pandemic response relied, however, on the technological support provided through international aid agencies. Ethiopia’s health authorities have had a longstanding relationship with international development partners who directly procure the services of technology companies. That means technological support to the health sector is often provided in the form of development aid. A good case in point is the Digital Health Activity project of the United States Agency for International Development (USAID), which has been supporting Ethiopia’s Health Sector Transformation Plan since late 2019. Through this project, Jon Snow, Inc. (JSI)—a public healthcare and health systems consultancy firm—has been working with a consortium of tech companies to create a ‘sustainable, resilient, and interoperable health information system’ for Ethiopia’s Ministry of Health. Digitization of the methods and practices used to collect, analyse, present, and disseminate information is part of Ethiopia’s 2015 Health Sector Transformation Plan (Health Transformation Plan, 2015). While this project began before the pandemic, it has been a central part of Ethiopia’s COVID-19 response measures. JSI and its tech partners have been involved in Ethiopia’s pandemic response in the following four ways (JSI, 2019; USAID/Ministry of Health, 2021):

- 1 Point of entry health declaration: Per this procedure, travellers arriving in Ethiopia would be required to use an app to record personal identification

- information, including phone numbers, travel history, health symptoms, and their Ethiopian residence geo-location. This work was undertaken in collaboration with the Data Use Partnership (DUP), a project funded by the Bill and Melinda Gates Foundation;
- 2 National COVID-19 Surveillance and Tracking System: This system was used for demographic enrolment, *inter alia*, and was being undertaken in collaboration with the DUP project;
 - 3 Community House-to House Screening: This was being undertaken using an app developed by the JSI and its partners. The app was used by extension health workers as a data collection tool. In Addis Ababa alone, this app had been used by more than 173 health workers; and
 - 4 WhatsApp Helpline: JSI and DUP helped configure WhatsApp to provide accurate and timely health information to the public through a WhatsApp bot.

With the advent of other public health emergencies such as the most recent mpox pandemic, Ethiopian health authorities are likely to continue relying on the technological support of aid agencies (Xinhua, 2022). But this gives rise to a question of legality—what is the legal basis for such public-private partnerships? Moreover, the question of whether partnerships between the Ministry and the private sector as well as aid agencies are—or at least should be—subject to Ethiopia’s Public Private Partnership (PPP) legal framework remains. The Institute is indeed empowered by its establishment legislation to collaborate with third parties (‘concerned bodies’) in its response to public health emergencies (Regulation No 301/2013, Art 5(2)).⁴ Arguably, this would capture most of the Ministry of Health’s partnerships highlighted previously. But the lack of transparency or accountability mechanisms should be a cause for concern. A related concern is the risk of government (over) dependence on the technological services of unaccountable private actors. Because the previously highlighted partnerships with health authorities involve the routine collection, processing, and disclosure of sensitive personal data, privacy concerns also arise. I return to consider such regulatory concerns in some detail in the section on regulatory blind spots.

What, however, transpires from the preceding overview is that notions of neither sphere transgression nor transition define the pandemic-induced measures in Ethiopia. No technology company transgressed or transitioned into a new domain, but the Ethiopian experience has been unique in the way partnerships with the private sector have been central to the national pandemic response. Yet, the involvement of technology companies has also been quite peculiar in that Ethiopian authorities had little role in procuring the services. Technological support has been provided as part of broader aid packages with little room for authorities to negotiate the ways in which the services of third-party tech companies should be provided. This adds up to the regulatory challenges considered in what follows.

Regulatory blind spots

Regulatory blind spots—that is, regulatory concerns that did not seem to be taken into account or were wholly overlooked in the process of deploying health tech—take different forms. One such concern is the lack of transparency regarding collaborations between technology companies and health authorities. Details about the contracts, procurement process, technological architecture, and more importantly, possible data sharing arrangements are often unclear (Pollicy, Article 19 and KICTNET, 2021: 4). PPP laws in many countries are adopted primarily in response to such opacity concerns.

Such laws lay out systems, procedures, and institutional arrangements by which the involvement of the private sector in public sector projects are overseen to ensure fairness, accountability, and transparency. Ethiopia's PPP legal framework applies to all types of partnerships, including those involving the provision of public health services (Proclamation 1076/2018, Arts 4–5).⁵ As a result, the involvement of the private sector in public health services in Ethiopia engages the PPP legal regime. But the public-private partnerships in health tech alluded to earlier have been taking place outside Ethiopia's PPP legal framework. An interview with an official at the PPP Directorate of the Ministry of Finance revealed that none of the PPPs in the health sector went through the procedure set out in the PPP Proclamation (interview, 2020).⁶ No project relating to public health was under consideration at the time of interview.

Partnerships in the health sector take essentially a form of international aid—or in the context of collaboration with local technology companies, in the form of voluntary corporate social responsibility undertakings. The private actors are not directly awarded contracts by the Ethiopian government. This might be taken to argue that Ethiopia's PPP legal framework would not, as a result, apply to the kind of partnerships in the health sector alluded to earlier. But a closer consideration of the complex relationships among the partners might suggest otherwise. The Ethiopian government does not, of course, directly procure the services of private contractors. International aid agencies essentially engage the services of private technology companies for consideration.

USAID, for instance, is procuring the services of private contractors for—if not on behalf of—Ethiopian health authorities. JSI has been contracted by USAID to run the 'Digital Health Activity' project in Ethiopia, for the purpose of which it—in turn—procures the services of a number of technology companies (JSI, 2019). And for a stronger reason, services offered to the Ethiopian government via development partners should come under the regulatory purview of the PPP legal regime. But still, the question of how the PPP legal and regulatory framework would apply remains. Addressing this question is beyond the scope of this chapter.

Protection of human rights is the other concern associated with the unchecked recourse to technology in the provision of public health services. The primary concern relates to data privacy. Pandemic-induced reliance on technology involves the routine collection, processing, retention and sharing of

personal data, thereby raising data privacy concerns. Part of the Ministry of Health's COVID-19 response has been phone tracking of patients, both in government-mandated isolation centres and home isolation, as well as app-based contact tracing. According to an official at EPHI, the tracking was undertaken by the Information Network Security Administration (INSA) in collaboration with Ethio-telecom (interview, 2021).⁷ What, however, compounds the concern is that privacy is an enabling right, threats to which would hamper the exercise of other fundamental rights such as freedoms of expression, assembly, and association.

The right to privacy is guaranteed under the Ethiopian federal constitution (Ethiopian Constitution, 1995: Art 26). Any restriction to the constitutional right to privacy should fulfil the three-part test of legality, necessity, and legitimacy (Ethiopian Constitution, 1995: Art 26(3)). The principle of legality requires, according to the United Nations Human Rights Committee, restrictive measures to be based on clear, specific, and accessible legislation (General Comment 34, 2011: paras 24–25). It is to be noted that General Comment 16 of the Committee on the Right to Privacy does not unpack elements of the requirements of legality (Yilma, 2023: ch 2). But the legal basis for intrusive measures highlighted earlier has not been entirely clear. The Terms and Conditions of Debo Contact-tracing app, for instance, stipulate the following stern requirement without invoking any clear legal basis:

[...] any relevant person shall upload the application and information s/he (sic) holds and any of his/her (sic) Bluetooth pieces of information may be uploaded on the server and may be used when deemed necessary. [...] You are required to put on Bluetooth and to charge the battery of your device as well as on your daily basis to register the name, phone number and other necessary information of persons who have contact with you.⁸

A legal basis often raised to justify the use of various intrusive measures, including phone tracking and contract-tracing apps, is the EPHI's broader surveillance powers. The Terms and Conditions of the Debo app, for instance, invoke Regulation No 301/2013—the law that established the Institute—to justify the power of EPHI 'to conduct, during epidemics or any other public health emergency or public health risk, surveillance and investigation'.⁹ Per Article 5(2) of the Regulation, one of the legislative objectives of the Institute is the following:

In collaboration with the concerned bodies, conduct surveillance for the early identification and detection of public health risks and prevent public health emergencies through adequate preparedness, [...] respond effectively and timely and ensure rapid recovery of the affected population from the impact of the public health emergency.

(Regulation No 301/2013, Arts 6(6) & 6(12). [Emphasis added])

This provision is evidently framed broadly, and hence, may mean that it does not quite meet the requirement that any right-restrictive legislation should be

clear, specific, and accessible. Added to that, the fact that this is provided in the ‘non-operative’ or non-substantive part of the legislation further casts doubt on the tenability of justifying the Institute’s intrusive measures under the law. One finds a clearer, albeit tentative, legal basis for some of the pandemic surveillance measures in the State of Emergency (SoE) decrees adopted by the Council of Ministers in the wake of the pandemic (Proclamation No 3/2020).¹⁰ While these sets of ‘temporal’ laws have since expired they formed part of Ethiopia’s pandemic legislative repertoire.

A concern with SoE laws, though, is that they suspend a broad range of human rights for the duration of the public health emergency (Ethiopian Constitution, 1995: Art 93(2)). Moreover, the SoE laws are known to impose onerous obligations which, in certain instances, may encroach upon human rights, including the right to privacy. For instance, the Ministerial Committee—a body installed to oversee the decrees—may require ‘any service provider’ to provide a ‘service or manufacture a new kind of product’ needed to support the effort of countering and controlling the spread of the pandemic (Regulation No 466/2020, Art 4(16)). In that sense, it goes beyond voluntary collaboration in that the government can compel private actors to avail their services or create a product that may undermine human rights.

What this state of affairs suggests is that rule of law and human rights considerations were not part of the overall experimentation with health tech. A manifestation of this is that the Terms and Conditions of the Debo app do not envisage any privacy policy. This omission—deliberate or otherwise—is in stark contrast with the experience in other countries. For example, in Uganda the communication sector regulator and the Ministry of Health developed a privacy policy for the national contact-tracing app (Pollicy, Article 19 and KICTNET, 2021: 11). Neither the Ethiopian Communication Authority nor the Ministry of Health took similar steps.

Ethiopia introduced data protection legislation only recently, in April 2024 (Personal Data Protection Proclamation 1321/2024). While this legislation is yet to be made publicly available, privacy standards scattered across various pieces of legislation have been the only sources of data governance for decades, including during the pandemic (Yilma, 2021: 26–77). This meant that pandemic response measures involving data processing were not subject to any meaningful regulatory oversight. That lends weight to the argument that the lack of a pertinent legal framework is part of the broader problem that human rights protection had not been among relevant considerations in the government’s overall endeavour of containing the pandemic.

Peculiar about the Ethiopian case, though, is not only the lack of a data privacy legal framework, but also that the government has been notorious for introducing legislation that undermines the constitutional right to privacy. A good (and recent) case in point is the law governing the provision of electronic taxi services which introduces not only a data localization requirement but also obliges service providers to provide unfettered access to the government, including personal and location data (Directive No 05/2019, Arts 5.1(i), 7.3, 9.6–9.7, 7.14 combined with Arts 7.1 and 7.8). In the absence of data

protection legislation and an independent oversight body, public health-related surveillance and data processing measures will go unchecked, at the expense of individual rights. Added to the hitherto weak application of the nation's PPP framework, the government's overtures to health tech require closer attention from all stakeholders.

Conclusion

While problematic sphere transgression might not have occurred in Ethiopia, the unchecked use of invasive technologies in response to public health emergencies should be a cause for concern. This is not an isolated phenomenon, however. Most initiatives involving invasive technologies, including in the health sector, appear to be procured with little consideration of the attendant regulatory or human rights implications. The overall national hype about 'digital transformation' is driven by tech solutionism where technologies are often portrayed as the panacea for the nation's complex socio-economic predicaments.

A paucity of qualified personnel in relevant government departments is partly responsible for this myopic perception of technology. Without the requisite expertise, the adverse impact of technology is unlikely to be properly recognised and addressed. But of course, there is little that could be done when technological support is provided in the form of humanitarian aid. In the absence of a push-back against problematic technological interventions, data collected in the process will be prone to abuse. Additionally, the attendant implications of opaque public-private partnerships to other equally important values of fairness, transparency, and accountability will not garner sufficient attention.

Further punctuating the problem is the absence of local civil society groups that would run public interest advocacy campaigns against problematic government initiatives. Due to restrictive regulations, such groups working in the human rights field have been few and far between. Recent changes in legislation offer some hope, with local civil society groups working on digital rights and data justice emerging. Civil society advocacy will be critical not only in bringing to light unchecked tech solutionism in the public sector but also in helping retool existing accountability mechanisms such as the PPP framework. No less exigent is building the technical capacity of personnel in relevant government offices, as well as quickly putting into action the newly adopted data protection law.

Notes

- 1 See <https://insa.gov.et/product/debo>; Note that another mobile app—called COVID-19 Ethiopia—was launched by EPHI in collaboration with Ewenet Communications PLC, the company that developed Debo. But the app was meant to provide information to health professionals as a learning/training platform. See more at Google Play Store <https://bit.ly/3rIQCn2> (Last accessed on 31 January 2023).

- 2 Interview with Mr Addis Alemayehu, Managing Director at Ewenet Communications PLC, held on 20 May 2021.
- 3 See more at Google Play Store <https://bit.ly/2Va7R4k> (Last accessed on 31 January 2023).
- 4 Note the terms ‘concerned bodies’ appear to refer to relevant government bodies but the Amharic version of the terms ‘ከሚመለከቱት ዕኩዳት ጋር’ roughly translates to ‘any relevant party’, and hence may potentially include private actors.
- 5 Note also that Ethiopia introduced a PPP Policy in 2017 and Directive No 55/2018 in 2018. See relevant legal instruments here: <https://www.mofed.gov.et/programmes-projects/ppp/> (Last accessed on 31 January 2023).
- 6 Interview with Mr Ashenafi Abera, Officer at the Public Private Partnership Directorate of the Ministry of Finance, held on 21 June 2021.
- 7 Interview with Mr Mebratu Massebo, Senior Advisor to the Minister of Health and National COVID-19 Response Task Force Coordinator, held on 3 June 2021.
- 8 See Terms and Conditions at <https://insa.gov.et/product/debo> (Last accessed on 31 January 2023).
- 9 See Terms and Conditions of Debo at <https://insa.gov.et/product/debo> (Last accessed on 31 January 2023).
- 10 Note that three Directives have also been issued by a Ministerial Committee that was created to oversee the implementation of the SoE decree. See Proclamation No 3/2020, *Id*, Art 5.

Bibliography

- Digital Health Activity Annual Report. USAID/Ethiopia Ministry of Health, 2021.
- Electronic Tax Services Directive No. 05/2019, Government of Ethiopia. 2019. Amharic: Author’s Translation.
- Ethiopia Heightens Surveillance for Monkeypox (Xinhua, 28 July 2022). <https://bit.ly/3PtWgbz> (Last accessed on 31 January 2023).
- Ethiopia’s Digital Health Response to COVID-19 (JSI, 14 May 2020). <https://www.jsi.com/ethiopias-digital-health-response-to-covid-19/> (Last accessed on 31 January 2023).
- Ethiopian Constitution, Federal Negarit Gazeta, Government of Ethiopia, Proclamation No. 1/1995.
- Ethiopian Public Health Institute Establishment Council of Ministers Regulation No 301/2013, Federal Negarit Gazeta, 2013.
- Health Sector Transformation Plan: 2015/16–2019/20. Government of Ethiopia, October 2015.
- Human Rights Committee, General Comment 34: Art 19—Freedom of Opinion and Expression, UN Doc CCPR/C/GC/34, September 2011.
- JSI Awarded Ethiopia Digital Health Activity, JSI, 13 November 2019. https://publications.jsi.com/JSIInternet/Inc/Common/_download_pub.cfm?id=25603&lid=3 (Last accessed on 31 January 2023).
- Personal Data Protection Proclamation 1321/2024, Federal Negarit Gazeta, 2024.
- Public Private Partnership Proclamation 1076/2018, Federal Negarit Gazeta, 2018.
- State of Emergency Proclamation Enacted to Counter and Control the Spread of COVID-19 and Mitigate Its Impact Proclamation No 3/2020, Federal Negarit Gazeta, 2020.
- State of Emergency Proclamation No 3/2020 Implementation Regulation No 466/2020, Government of Ethiopia Federal Negarit Gazeta. 2020.
- Tech Savvy Firm Crafts Close Contact Detector App, Fortune, 17 April 2020. <https://bit.ly/2T7a0gr> (Last accessed on 31 January 2023).

Unseen Eyes, Unheard Voices: Surveillance, Data Protection and Freedom of Expression in Kenya and Uganda During COVID-19, Pollicy, Article 19 and KICTNET, April 2021.

Yilma, Kinfe. 2021. Privacy and data protection in Ethiopia. In *Privacy and Personal Data Protection in Africa: A Rights-based Survey* edited by Alan Finlay, 26–77. Melville: Association for Progressive Communication.

Yilma, Kinfe. 2023. *Privacy and the Role of International Law in the Digital Age*. New York: Oxford University Press.