GISWatch
SNEAK PEEK

GLOBAL INFORMATION SOCIETY WATCH 2021-2022

Digital futures for a post-pandemic world

Association for Progressive Communications (APC)
and Swedish International Development Cooperation Agency (Sida)

GISWatch
SNEAK PEEK

Global Information Society Watch 2021-2022 SNEAK PEEK
Digital futures for a post-pandemic world

Sida

APC would like to thank the Swedish International Development Cooperation Agency (Sida) for their support for Global Information Society Watch 2021-2022.

Published by APC
2022

Disclaimer: The views expressed herein do not necessarily represent those of Sida, APC or its members.

GISWatch SNEAK PEEK

Table of contents

Introduction

Valeria Betancourt and Alan Finlay
Association for Progressive Communications

Rebalancing and reimagining our futures

In 2005, at the culmination of the second phase of the World Summit on the Information Society (WSIS), civil society organisations clearly stated that societies will not be able to advance towards social justice if the development and use of the internet does not contribute to the strengthening of the exercise of human rights.

The capabilities of digital technologies are a thousand times greater than they were in 2005 and, although progress has been made, we have not yet managed to determine the scope of the reinterpreted vision of WSIS that is needed to respond to the implications of ever-changing digital societies. Nevertheless, we probably thought we were getting closer to some answers before the COVID-19 pandemic hit us, revealing the stark dimensions of digital exclusion and rights violations across the world.

With lockdowns forcing more people online for longer periods of time, alongside the techno-centric, "top-down" interventions adopted by governments,[1] the immediate consequences of a lack of digital rights and meaningful access were for many harsh, visceral and ubiquitous.

While many activists found themselves at a crossroads – either get online and learn new ways of interacting, or risk being stranded – people without a stable and affordable internet connection were unable to work, or to access education and government services, including health services. Meanwhile, hastily drafted regulations and technologies put to new use limited people's right to freedom of expression and association, personal data security and privacy, and freedom from unwarranted surveillance. The pandemic also amplified online violence against both women and children, despite over a decade of work in this area.

Many of these are rights that civil society organisations have been advocating for since 2005 – with some concerns, such as access for poor and marginalised communities, stretching back to the origins of internet advocacy in the 1990s.

What then can we learn from this period of "accelerated transition", as one report describes it here?[2]

The purpose of this GISWatch was to ask two fundamental questions:

- How has the COVID-19 pandemic changed or shaped the ways in which civil society organisations do their advocacy work around digital technology-related issues, including digital rights?
- How have internet rights advocacy priorities shifted due to the pandemic?

It includes a series of thematic reports, dealing with, among others, emerging issues in advocacy for access, platformisation, tech colonisation and the dominance of the private sector, internet regulation and governance, privacy and data, new trends in funding internet advocacy, and building a post-pandemic feminist agenda. Alongside these, 36 country and regional reports, the majority from the global South, all address the two questions in different ways, offering some indication of how we can begin mapping a shifted terrain.

Through the lens of the COVID-19 pandemic, the reports highlight the different and complex ways in which democracy and human rights are at risk across the globe, and illustrate how fundamental meaningful internet access is to sustainable development. While the majority focus on the impact of the pandemic on digital rights and access in the global South, the inclusion of reports from countries in the North, such as Canada, suggests that developed countries have not been immune to new threats to freedoms, and that there is a need to address these risks collectively with fresh vigour.

[1] See Jinbonet's report on South Korea for an example of this.

[2] See the country report on Spain by Pangea and the eReuse.org initiative.

The reports show how advocacy priorities have, on the one hand, stayed the same (a "turning back" or learning from history is necessary), and, on the other, that they have to be refocused to attend properly to a subtly or significantly altered terrain. New fields of advocacy have also been brought to the fore that civil society organisations need to pay better attention to.

A number of reports show how we (governments, the private sector, civil society) have not properly been able to address the question of meaningful internet access for all, nor the impact of gender inequality on access and the use of the internet. Others deal with comparatively more recent advocacy focus areas that are now the mainstay of global advocacy on digital rights, such as privacy online, surveillance, disinformation and misinformation, artificial intelligence, and data rights. Largely within these frames, emerging concerns are identified.

For example, while the rights principles of artificial intelligence need to be properly addressed when shaping policy, there is a need to consider the newer field of robotic policing and automated nursing. Although robotic policing has been around for a number of years – an early example of its misuse occurred in Dallas in the US in 2016[3] – in Tunisia it was introduced during the pandemic with very little public consultation, a particular concern given that the robots helped enforce the country's lockdown rules and interfaced with the public directly. Similarly, technologies used ostensibly for public benefit – such as contact tracing apps – need to be framed as "public interest technologies" to make the spectrum of their rights implications more visible (see the report by Tecnológico de Monterrey and May First Movement Technology).[4]

Less prominent rights issues, such as those of remote or hybrid workers (see the report by EsLaRed on Venezuela, for instance) now need to be foregrounded in rights discourse, alongside the growing support for the rights of gig economy workers.

The same goes for the digital rights of children. The reports show that the impact of digitisation on children can no longer be marginalised in mainstream digital rights discussions. Cooperativa Sulá Batsú discusses the negative effects of isolation and children being online for extended periods, particularly for boys, while, as ARTICLE 19 Eastern Africa suggests, there was evidence of a general increase in online violence against children during the pandemic in Kenya (a phenomenon unlikely to be isolated).

Other "old issues" that have been to some extent put to one side, such as advocating for free and open source technologies, need to be reinvigorated – albeit, as the Digital Trade Alliance explains, in a difficult context for open knowledge advocacy given the background of the vaccine debate and the failed TRIPS waiver.

These advocacy priorities occur in and are shaped by a context that has shifted as a result of the "accelerated transition" we have experienced. As Privacy International and others have indicated, the pandemic has been a significant boom for the private tech sector – perhaps unparalleled in such a short space of time – both in terms of new users and the data that can be harvested from them and in terms of "instant" partnerships formed with governments who anxiously sought to respond to the crisis and ramp up their digitisation processes. With few or no checks and balances, and little public transparency on what exactly was being given up while access to health and a safe environment was ostensibly being secured, this has come at a cost for citizens (including the corporate surveillance of children, forced to be online for education).

Coupled with some governments having to rush their own digitisation processes that were still in the pipeline, the pandemic significantly boosted the transition to the data-driven society, with more known about us now than ever before. It is the implications of this that civil society needs to continue to map for its specific advocacy priorities, including the need for significant upscaling of data capacity in the countries of the global South, and the building of "local data narratives" of resistance.[5]

Many governments across the world have been given a fresh leash to tighten their grip on civic spaces, and in countries like Nigeria there are suggestions that civil society actors have started to leave the advocacy arena due to the imminent threats they face. India meanwhile faces its own clampdown on civil society organisations, with donors struggling to find ways to fund them.

It was also remarkable how easily governments, in a time of emergency, discarded public input in their efforts to find solutions to the immediate crisis – at least in the field of technology. While countries

[3] Liedtke, M., & Fowler, B. (2016, 9 July). Killer robot used by Dallas police opens ethical debate. *Phys.org*. https://phys.org/news/2016-07-killer-robot-dallas-police-ethical.html

[4] Tecnológico de Monterrey and May First Movement Technology provide in their report an excellent starting point for this understanding. Meanwhile, Carlos Guerrero Argote worryingly suggests in his country report on Peru that both civil society and funders felt that with many technologies used to manage the virus being discarded by governments over time, they are no longer worthy of attention.

[5] See, for instance, Razzano, G. (2022). Decolonising data. In A. Finlay (Ed.), *State of the Newsroom 2020*. Wits Centre for Journalism. https://journalism.co.za/wp-content/uploads/2022/03/SON-2020-Final-23-Feb.pdf

set up expert advisory groups to understand the evolution of the pandemic, when it came to the application of technology to meet the new, urgent needs, this kind of citizen input was largely absent. A common recommendation in a number of country reports is to create robust frameworks for multistakeholder decision making and citizen oversight when innovating technological responses to future, similar events. It will, however, be worth tracking whether the lack of participation in the development of technology-driven responses to the pandemic sets a precedent – particularly in light of a significantly empowered private sector.

Funding priorities also appear to be shifting, and the longer-term impact of this is still to be felt. As a report in this edition of GISWatch outlines, many donors are now more likely to focus on intersectional agendas, where the application of technology or digital rights meets the needs of other advocacy priorities. Civil society organisations may need to engage in direct advocacy with donors to ensure that the specific and perhaps unique terrains in digital rights advocacy are not stripped of their vital resources, even if there is a need to be more specific and incisive in setting their advocacy priorities.

We do not want to suggest that everything went badly with respect to digital rights and access during the pandemic. Reports here also show strong cooperation between governments and civil society – for instance, in freeing the regulatory space for the rollout of community networks as an emergency access solution, or in the running of trade union elections in Benin, with connectivity points set up for workers who did not have internet. Such an initiative holds some potential for new forms of hybrid democratic participation and multistakeholder collaboration or cooperation.

Innovative technological solutions for medical purposes were also developed by startups in the private sector, universities and civil society actors, while the internet was used by ordinary people to mobilise citizen action and help to provide support to communities in need. At the grassroots level, civil society organisations experimented with new ways of training remotely (see the discussion by DW Akademie and Redes on Colmena for a good example of this). New advocacy networks were also born when grassroots organisations came online, and met other, like-minded organisations for the first time.

In an effort to inform the public about the pandemic, the new government in the Democratic Republic of Congo did not resort to internet shutdowns to combat disinformation as had been done in the past, instead putting its faith in supporting fact-checking organisations. In the process it stated its intention to ratify the international convention on cybercrime, which limits shutdowns, creating an interesting policy advocacy window of opportunity in that country. In Brazil, a victory in the supreme court guaranteeing the right to personal data protection has also opened up new advocacy avenues for civil society.

There is also a greater awareness of the real-life impact of the digital divide – and a fresh impetus to look at new access possibilities or revisit old ones, including leveraging universal service funds and rolling out community networks. Issues to do with privacy and surveillance have gained greater visibility among civil society actors working outside the field of digital rights, and no doubt among the public too.

However, as others have pointed out, the initial phase of the pandemic created for some a sense of global optimism[6] – a possibility of a common good being forged, even if driven by pragmatism (e.g. in Turkey the government lifted its usual restrictions on the media temporarily in order to properly inform the public about the virus). Initially, despite the shock and uncertainty, there was a sense of relief that “we were all in this together” and that a collective response might be possible to determine the fate of humanity and the planet – a response which, perhaps, could be felt in other areas too, such as properly addressing climate change.

However, the sense of optimism felt at the beginning of the pandemic was soon supplanted by different kinds of opportunism – whether from the state, the private sector, or developed countries acting in cohort – and it ran aground when confronted with the powerful geopolitical dynamics and alignments holding the “centre” in place, as we saw with the failure of the TRIPS waiver. With economically weakened and unstable states, a stressed civil society, an increase in global poverty, and the current state of geopolitical imbalance – with one expression being the war in Ukraine – the ramifications of this opportunism may be felt in the terrain of internet governance for years to come.

The question then becomes: What kind of processes would contribute to restore a workable balance? And what sort of rebalancing is necessary, or “push back” is needed?

How do we reach new agreements building on the processes that have been carried out in the fields of internet policy, internet governance and global digital cooperation, while properly taking into account the shifted terrain? What are the conditions that need to be in place to reach outcomes that balance the differences in power of contending

[6] See, for instance, “Rerouting geopolitics” by Alison Gillwald (publication forthcoming).

parties and the multiplicity of interests? How do we operationalise global digital cooperation, and how do we translate it to regional and local spheres, bridging the gap between deliberative spaces and decision-making processes?

Over the past two years, a number of initiatives have emerged in the ecosystem of internet governance and global digital cooperation aimed, in large part, at outlining the characteristics of a digital future. These include the Global Digital Compact,[7] and other relevant processes that are around the corner, such as the WSIS+20 review.[8]

But still more needs to be done. There remains an urgent need for regional and global responses arising from true – and significantly strengthened – multilevel, multidisciplinary and multistakeholder collaboration, based on the principles of inclusiveness, transparency and shared responsibility. These need to recognise that different contexts and impacts require differentiated and specific responses, including public policy interventions.

And, as these reports suggest, in all regions of the world, including in the global North, there is a need for a fresh impetus towards movement building, working across civil society, and including organisations that may not have taken digital rights as a priority before. This is necessary not only to address the shrinking of civic space, but also to collectively challenge the new geopolitical and economic power dynamics that are refracted in the digital sphere.

Any push back requires most of all imagination – of how things can be done differently. As the Centro de Investigación en Tecnologías y Saberes Comunitarios put it in their country report on Mexico, part of the access challenge in that country is that "the imagination and understanding of the problem by policy makers have not gone beyond the unsuccessful strategies that have been already developed." How this reimagining of possibilities can be introduced into spaces for deliberation and policy making and inform the new movement building that needs to take place, is up to us, as civil society actors.

[7] https://www.un.org/techenvoy/global-digital-compact

[8] Souter, D. (2020, 6 July). Inside the Digital Society: WSIS+20 is closer than you think. *APC*. https://www.apc.org/en/blog/inside-digital-society-wsis20-closer-you-think

Tech, data and the pandemic: Reflecting for next time

Alexandrine Pirlot de Corbion and Gus Hosein
Privacy International
https://privacyinternational.org

Introduction

Responding to a pandemic is more than just the mobilisation of the health system and adaptation of scientific research; the response is also a creature of the tools and measures available to respond.

Governments and companies chose to use this pandemic to test a series of new and innovative measures alongside the traditional ones. A pandemic is an extraordinary time and using available tech capabilities and data is common but can also be extra-ordinary. They can also provide the rubric for a post-pandemic future, institutionalising some practices and infrastructure for the next public health response, or the next emergency, or the "new normal" normalising surveillance and control of people and communities.

Context matters: A slightly different pandemic

Every virus and so every pandemic is unique. And the SARS-CoV-2 or "COVID-19" was indeed novel. Some of its unique aspects are worth noting.[1]

While public health experts may find better terminology for capturing these, in our understanding these considerations help to explain the challenges of this particular pandemic:

- The virus was primarily airborne.
- You could be asymptomatic and still transmit the virus.
- You could be vaccinated and still transmit the virus to others.
- You could repeatedly become infected.
- The virus mutated in ways that could escape some elements of the deployed vaccines.
- Elements of the vaccines' effectiveness may reduce over time.
- Booster vaccinations could be used to increase the body's defences against the virus.

It's also worth noting that none of this was known when the pandemic began, and it trickled in over the course of the pandemic. Whether through a lack of transparency, or the length of time scientific knowledge takes to develop and permeate, or the evolving nature of the virus itself, public health professionals and governments had to take decisions in the absence of complete knowledge. This is entirely understandable, and it was commendable that innovative solutions were sought.

However, as the pandemic became better understood, and now that we can begin to see its full nature, we must reflect on whether "innovative solutions" were sought because the underlying fabric of public health and welfare was so frayed from decades of under-investment and if there was an over-investment in shiny "innovative solutions" rather than sustainable, systemic, fair and people-centred solutions.

To a degree you can track some tech and data responses alongside the available knowledge of the time and see that the best available knowledge was used to decide the best available responses. Some responses, however, became disassociated with the emerging knowledge. Regardless, too many crossed the lines of ethics, the law and good tech practice into opportunism, repression and tech-solutionism.

A typology of responses

By reflecting on the implications of some of the measures deployed by governments, industry and other third parties,[2] we can begin to assess the

[1] Hu, B., Guo, H., Zhou, P., et al. (2021). Characteristics of SARS-CoV-2 and COVID-19. *Nature Reviews Microbiology, 19,* 141-154. https://doi.org/10.1038/s41579-020-00459-7

[2] Privacy International. (2022, 20 March). Extraordinary powers need extraordinary protections. https://privacyinternational.org/news-analysis/3461/extraordinary-powers-need-extraordinary-protections. For an outline of different tracking technologies used during the COVID-19 pandemic and their flaws, see Privacy International. (2022, 31 March). Covid-19: a tech post-mortem. https://privacyinternational.org/explainer/4814/covid-2022-tech-retrospective

scale of data processing activities that took place and continue today.[3] This assessment can help us to understand the magnitude of the challenge we face and will continue to face to protect people and their rights.

Measures adopted by governments and enabled by industry

The decisions made by governments around the world varied as the pandemic evolved and was experienced in different ways at different stages. Nonetheless there were some common approaches and tactics.

Quarantining and lockdown enforcement

Quarantining was a top first response by governments. Once someone could be identified as having symptoms relevant to COVID and once tests were developed to identify someone as having COVID, governments would move them to quarantine.[4] Eventually the virus spread, so governments reached to lockdowns as a public health response. Even after lockdowns ceased, quarantine requirements were imposed on individuals and groups following exposure (often arising from contact tracing), or upon the development of symptoms (which led to contact tracing) or for people who travelled. These sustained measures had tragic implications for people in vulnerable situations.[5]

In all these cases data and tech could be used, and in many cases, were used for quarantine enforcement. First, telecommunications data was sought from telcos to identify if someone was moving around when they did not have authority to do so due to quarantine or lockdown.[6] A leading example of this was Israel, where the government tasked the Israeli security service Shin Bet to track mobile phones to curb the spread of the virus.[7] Similar attempts were made in Kenya,[8] South Africa[9] and Mexico.[10] Other data sources were proffered by industry, including data held by data brokers and other data aggregators based on smart phone apps, leaking data to assess the extent to which there was public adherence to caution and lockdowns.

Governments then started check-ins (done by government contacting individuals or individuals reporting to authorities) and used police powers of generalised monitoring (e.g. CCTV, facial recognition, drones)[11] or stop and search powers to ensure that individuals were complying with orders.

Apps were sometimes used for quarantine enforcement, for example, in Abu Dhabi[12] and Myanmar.[13] These could disclose location data through GPS or other automatic means, or compel an individual to report their location data manually.

Contact tracing

Contact tracing can be an essential public health surveillance response to a transmissible virus.[14] If someone tests positive, contact tracing allows the ability to identify individuals who may have been exposed to that individual while they were contagious.

In this pandemic, particularly in the early stages when it was unclear how the virus was transmitted, governments scrambled to use vast amounts of data to undertake contact tracing.[15] Some governments

[3] See: Sequera Buzarquis, M. (2020, 7 March). Las emergencias no deberían ser un cheque en blanco. *TEDIC*. https://www.tedic.org/noesunchequeenblanco; Memdutt, V. (2020, 14 April). COVID-19 Surveillance Infosheet! *Right2Know*. https://www.r2k.org.za/2020/04/14/covid-19-surveillance-infosheet; Digital Rights Foundation. (2020, 13 March). Protecting Your Rights During the Covid-19 Outbreak. https://digitalrightsfoundation.pk/protecting-your-digital-rights-during-the-covid-19-outbreak; Foundation for Media Alternatives. (2020, 15 March). Covid-19, public health, and privacy: The FMA Digital Rights Report. https://fma.ph/2020/03/15/public-health-and-privacy-amid-covid-19-the-fma-digital-rights-report; https://www.alsur.lat/pt-br/projeto/observatorio-covid-19; https://privacyinternational.org/campaigns/fighting-global-covid-19-power-grab

[4] https://privacyinternational.org/examples/quarantine-enforcement-and-covid-19

[5] Privacy International. (2020, 6 April). We must protect people in vulnerable situations during lockdown or quarantine. https://privacyinternational.org/news-analysis/3588/we-must-protect-people-vulnerable-situations-during-lockdown-or-quarantine

[6] https://privacyinternational.org/examples/telecommunications-data-and-covid-19

[7] BBC News. (2020, 27 April). Coronavirus: Israeli court bans lawless contact tracing. *BBC News*. https://www.bbc.com/news/technology-52439145

[8] Olewe, D. (2020, 9 April). Coronavirus in Africa: Whipping, shooting and snooping. *BBC News*. https://www.bbc.co.uk/news/world-africa-52214740

[9] Hunter, M., & Thakur, C. (2020, 3 April). Advocacy: New privacy rules for Covid-19 tracking a step in the right direction, but.... *amaBhungane*. https://amabhungane.org/advocacy/advocacy-new-privacy-rules-for-covid-19-tracking-a-step-in-the-right-direction-but

[10] Galán, V. (2020, 31 March). El Gobierno de la CDMX ordena el cierre de centros comerciales por emergencia sanitaria ante Covid-19. *Business Insider Mexico*. https://businessinsider.mx/cdmx-ordena-cierre-centros-comerciales-covid-19

[11] AP News. (2020, 25 June). Asia Today: India to survey 29 million New Delhi residents. *AP News*. https://apnews.com/article/virus-outbreak-india-ap-top-news-new-delhi-international-news-f34eecac3d01431ab5848bb3aa03fc3d

[12] Nasrallah, T., & Zaman, S. (2020, 3 April). Abu Dhabi launches smart app to monitor home-quarantined people. *Gulf News*. https://gulfnews.com/uae/health/abu-dhabi-launches-smart-app-to-monitor-home-quarantined-people-1.70796153

[13] See: https://privacyinternational.org/examples/3911/myanmar-launches-app-enforce-quarantine

[14] WHO. (2021). *Contact tracing in the context of COVID-19: Interim guidance*. https://www.who.int/publications-detail-redirect/contact-tracing-in-the-context-of-covid-19

[15] https://privacyinternational.org/examples/contact-tracing; Privacy International. (2020, 19 May). Covid Contact tracing apps are a complicated mess: what you need to know. https://privacyinternational.org/long-read/3792/covid-contact-tracing-apps-are-complicated-mess-what-you-need-know

would search data stores in geographic locations where a COVID-positive person was known to have been (e.g. CCTV, restaurant billings, and other data sets stored more centrally, such as financial transactions or transport data).[16]

Mobile phone apps were also developed.[17] These apps could use mobile phone data to detect proximity with other individuals. Bluetooth was eventually the selected technology in most countries' apps, alongside a decentralised infrastructure using pseudonymised data.[18]

Concerns about the effectiveness of proximity tracing using Bluetooth technologies were coupled with longstanding privacy concerns of using telecommunications data to track individuals.[19] Reports of the repurposing of contact tracing apps for law enforcement goals have emerged in Australia,[20] Germany[21] and Singapore.[22] There were also examples of function creep with contact tracing apps used to enforce lockdown measures and control crowds.[23]

Furthermore, organisations around the world documented the lack of privacy safeguards built into the design and implementation of contact tracing apps, including our global partners in Colombia,[24] the Philippines,[25] Chile[26] and Peru,[27] while others reported a disproportionate negative impact on marginalised groups including women and minority groups, and the criminalisation of communities leading to discrimination and stigma.[28]

Border management

Governments started closing borders in March 2020 when the World Health Organization (WHO) declared COVID-19 a pandemic;[29] and when they slowly reopened, surveillance was embedded in new processes for travellers. It is important to note that these additional measures were added to an already vast surveillance infrastructure at the border and beyond to monitor travellers.[30]

Quarantining was often required for travellers. The use of "testing for release" became more commonplace as testing infrastructure improved. Testing prior to travel meant that government agencies and a myriad of private sector firms were starting to be custodians of vast amounts of personal data about travelling families, including custodians of their test samples and results. The travel industry also began to gain access to vast amounts of new sources of data on travellers, including their detailed biographical and family documentation (e.g. marriage certificates, birth certificates) to prove family composition to travel to some locations depending on restrictions.[31]

[16] South Korea is often identified as the prime example of this more advanced form of contact tracing. See: COVID-19 National Emergency Response Center, Epidemiology & Case Management Team, Korea Centers for Disease Control & Prevention. (2020). Contact Transmission of COVID-19 in South Korea: Novel Investigation Techniques for Tracing Contacts. *Osong Public Health and Research Perspectives, 11*(1), 60-63. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7045882

[17] https://privacyinternational.org/examples/apps-and-covid-19

[18] Privacy International. (2020, 31 March). Bluetooth tracking and COVID-19: A tech primer. https://privacyinternational.org/explainer/3536/bluetooth-tracking-and-covid-19-tech-primer

[19] BBC News. (2020, 27 April). Op. cit.

[20] Leaver, T. (2021, 16 June). Police debacle leaves the McGowan government battling to rebuild public trust in the SafeWA app. *The Conversation*. https://theconversation.com/police-debacle-leaves-the-mcgowan-government-battling-to-rebuild-public-trust-in-the-safewa-app-162850

[21] DW. (2022, 11 January). German police under fire for misuse of COVID contact tracing app. *DW*. https://www.dw.com/en/german-police-under-fire-for-misuse-of-covid-contact-tracing-app/a-60393597

[22] Illmer, A. (2021, 5 January). Singapore reveals Covid privacy data available to police. *BBC News*. https://www.bbc.co.uk/news/world-asia-55541001

[23] La Capital. (2020, 23 March). Controlarán a quienes incumplieron el aislamiento con una App en sus celulares. *La Capital*. https://www.lacapital.com.ar/la-ciudad/controlaran-quienes-incumplieron-elaislamiento-una-app-sus-celulares-n2572740.html

[24] Labarthe, S., & Velasquez, A. (2020, 18 April). Covid apps in Colombia, Karisma's digital security and privacy evaluation. *Fundación Karisma*. https://web.karisma.org.co/covid-apps-in-colombia-karismas-digital-security-and-privacy-evaluation

[25] Foundation for Media Alternatives. (2020, 8 July). Open letter to request for strong user privacy protections in the Philippines' COVID-19 contact tracing efforts. https://fma.ph/2020/07/08/open-letter-to-request-for-strong-user-privacy-protections-in-the-philippines-covid-19-contact-tracing-efforts

[26] Derechos Digitales. (2020, 16 April). CoronApp: La inutilidad del atajo tecnológico desplegado por el Gobierno y sus riesgos. https://www.derechosdigitales.org/14387/coronapp-la-inutilidad-del-atajo-tecnologico-desplegado-por-el-gobierno-y-sus-riesgos

[27] Morachimo, M. (2020, 14 April). Quince propuestas para mejorar la aplicación del Gobierno del Covid-19. *Hiperderecho*. https://hiperderecho.org/2020/04/quince-propuestas-para-mejorar-la-aplicacion-del-gobierno-del-covid-19

[28] Davis, S. (2020, 29 April). Contact Tracing Apps: Extra Risks for Women and Marginalized Groups. *Health and Human Rights Journal*. https://www.hhrjournal.org/2020/04/contact-tracing-apps-extra-risks-for-women-and-marginalized-groups

[29] https://privacyinternational.org/learn/tech-border; WHO. (2020, 11 March). WHO Director-General's opening remarks at the media briefing on COVID-19 – 11 March 2020. https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

[30] See for examples: Hosein, I. (2005). Transforming travel and border controls: Checkpoints in the Open Society. *Government Information Quarterly, 22(4)*, 594-625. https://doi.org/10.1016/j.giq.2006.01.002; https://www.privacyinternational.org/learn/migration-and-borders

[31] Read, J. (2020, 29 September). Will new travel technology invade your privacy? *National Geographic*. https://www.nationalgeographic.com/travel/article/will-new-travel-technology-invade-your-privacy-coronavirus

Certification

There was limited global harmonisation in the approach to both the use and purpose of COVID-19 certification documentation. The uses of the certificate varied considerably across the globe. The certificates could identify "immunity", meaning that someone had previously been infected, or "vaccination" if they had received a vaccine, or if they had been tested recently.

Some governments, including Israel,[32] France[33] and Italy,[34] among others,[35] required the mandatory provision of a certificate to allow access to public life and activities such as public venues like restaurants or cultural events. While others never fully developed a policy on their use,[36] and with the pandemic having evolved, other pending plans for certification have been dropped,[37] including for international travel in some instances.[38]

In particular, the mandatory approach to COVID-19 certification raised some serious concerns in terms of discrimination and the impact on already marginalised communities in contexts where access to vaccination was unequal and remained problematic in many parts of the world.[39] These risks and harms were also highlighted by the WHO in its guidance and aligned with its position that such mandatory requirements should not be introduced, at least in the context of international travel, "given that there are still critical unknowns regarding the efficacy of vaccination in reducing transmission."[40]

As time went on and boosters became deployed, some countries decided to extend the nature of the proof required. That is, your vaccine passport lost some of its "passport" capacity if you had not received more recent boosts. This was in theory to induce people into getting a third or fourth vaccination. But with equitable access to vaccination still being of concern, requiring certification of boosters remained highly controversial.[41]

Mass monitoring

Public health surveillance may involve wide-scale monitoring.[42] Usually this is done with the knowledge and the consent of the patients, but rarely with people one level removed from them (i.e. contacts or others in proximity).

In this pandemic public health surveillance expanded in some new ways. Temperature checks on people entering buildings became more common.[43] This was a surprising development considering not everyone who had COVID necessarily was symptomatic, and not everyone with a temperature was necessarily carrying COVID.[44]

Governments also sought to use and expand their existing mass surveillance tools for this pandemic.[45] This entailed population-level or geographic analyses using metadata, CCTV, and eventually drones[46]

[32] Holmes, O., & Kierszenbaum, Q. (2021, 28 February). Green pass: how are Covid vaccine passports working for Israel? *The Guardian*. https://www.theguardian.com/world/2021/feb/28/green-pass-how-are-vaccine-passports-working-in-israel

[33] Chrisafis, A. (2021, 12 July). France mandates Covid health pass for restaurants and cafés. *The Guardian*. https://www.theguardian.com/world/2021/jul/12/france-mandates-covid-health-pass-for-restaurants-and-cafes

[34] Giuffrida, A., & Henley, J. (2021, 24 November). Italy to tighten Covid rules for unvaccinated with 'super green pass'. *The Guardian*. https://www.theguardian.com/world/2021/nov/24/italy-poised-to-tighten-rules-for-unvaccinated-with-super-green-pass

[35] McDonagh, S., & Gallagher, T. (2021, 17 November). Green pass: Which countries in Europe require a COVID vaccine pass to get around? *Euronews*. https://www.euronews.com/travel/2021/10/12/green-pass-which-countries-in-europe-do-you-need-one-for

[36] Jackson, M. (2021, 12 September). England vaccine passport plans ditched, Sajid Javid says. *BBC News*. https://www.bbc.co.uk/news/uk-58535258

[37] Al Jazeera. (2022, 12 February). Israel PM announces end of vaccine 'green pass'. *Al Jazeera*. https://www.aljazeera.com/news/2022/2/17/israel-pm-announces-end-of-vaccine-green-pass

[38] Thackray, L. (2022, 30 June). The destinations that have scrapped all travel restrictions – regardless of vaccination status. *The Independent*. https://www.independent.co.uk/travel/news-and-advice/countries-no-travel-restrictions-tests-unvaccinated-b2071371.html

[39] Ganty, S. (2021). The Veil of the COVID-19 Vaccination Certificates: Ignorance of Poverty, Injustice towards the Poor. *European Journal of Risk Regulation, 12*(2), 343-354. https://doi.org/10.1017/err.2021.23; Maombo, S. (2021, 22 November). Amnesty warns against mandatory vaccination approach. *The Star*. https://www.the-star.co.ke/news/2021-11-22-amnesty-warns-against-mandatory-vaccination-approach

[40] WHO. (2021, 5 February). Interim position paper: considerations regarding proof of COVID-19 vaccination for international travellers. https://www.who.int/news-room/articles-detail/interim-position-paper-considerations-regarding-proof-of-covid-19-vaccination-for-international-travellers

[41] United Nations. (2022, 10 March). High Commissioner for Human Rights: the Failure to Administer the COVID-19 Vaccines in a Fair and Equitable Manner is Prolonging the Pandemic. https://www.ohchr.org/en/press-releases/2022/03/high-commissioner-human-rights-failure-administer-covid-19-vaccines-fair-and

[42] WHO. (2022, 14 February). Public health surveillance for COVID-19: interim guidance. https://www.who.int/publications-detail-redirect/WHO-2019-nCoV-SurveillanceGuidance-2022.1

[43] Privacy International. (2020, 30 July). Infrared temperature screening. https://privacyinternational.org/explainer/4111/infrared-temperature-screening

[44] UK Medicines & Healthcare products Regulatory Agency. (2020, 3 July). Don't rely on temperature screening products for detection of coronavirus (COVID-19), says MHRA. https://www.gov.uk/government/news/dont-rely-on-temperature-screening-products-for-detection-of-coronavirus-covid-19-says-mhra

[45] do Carmo Barriga, A., Martins, A. F., Simões, M. J., & Faustino, D. (2020). The COVID-19 pandemic: Yet another catalyst for governmental mass surveillance? *Social Sciences & Humanities Open, 2*(1). https://doi.org/10.1016/j.ssaho.2020.100096

[46] Mok, O. (2020, 24 March). Authorities monitor MCO-compliance from the sky with drones. *Malay Mail*. https://www.malaymail.com/news/malaysia/2020/03/24/authorities-monitor-mco-compliance-from-the-sky-with-drones/1849681

and facial recognition[47] to identify the movement of people.[48] The private sector has been instrumental in instigating and pushing for many of these tools, as it already did before COVID-19.[49]

The private sector embeds itself further into our lives

Building on years of lobbying and investment, and a propensity to identify opportunities to sell its products, industry was quick to identify this global pandemic as yet another hook to push up their sales, and reinforce their influence in many areas of our lives from our work to our education to intimate spaces such as our health needs.

The pandemic challenged the momentum that had been building as a result of a decade of policy making around the world aimed at reining in the power and dominance of industry. The result was worse than mediocre.[50] Below we outline various sectors where industry entrenched itself further as a result of the pandemic, with little scrutiny, transparency or accountability.

Education

While prior to the COVID-19 pandemic, there was already growing investment in the provision of information and communication technologies in the educational sector, known as "edtech", particularly by the private sector, this expanded drastically during the pandemic to enable children and adults to pursue their education online for various periods of time over the course of the pandemic.

Primary, secondary and tertiary education across the world adopted emergency remote learning measures with the uptake of education technologies – extending into homes during closures, into classrooms when reopened, and beyond.[51] This urgency of the demand for remote learning tools opened an opportunity for private companies to sweep in and offer their solutions with limited or no due diligence mechanisms to consider and respond to the impact of their adoption. Some countries expanded pre-existing infrastructure, but for many such infrastructure was not in place.[52] We saw the rapid uptake of virtual platforms like Zoom[53] and Blackboard,[54] the expansion of initiatives provided by companies like Google[55] as well as the use of open-source platforms such as Moodle and Canvas.

In addition to privacy concerns, this has raised concerns in terms of ensuring the right to education with the entrenchment of existing socioeconomic inequalities associated with an increased reliance on technologies which are not only unequally distributed, but distributed with uneven quality of access.[56]

Health care

The data and tech industry had identified the health sector as a fertile ground for data exploitation well before the COVID-19 pandemic.[57]

[47] Roussi, A. (2020, 18 November). Resisting the rise of facial recognition. *Nature*. https://www.nature.com/articles/d41586-020-03188-2; Van Natta, M., Chen, P., Herbek, S., Jain, R., Kastelic, N., Katz, E., Struble, M., Vanam, V., & Vattikonda, N. (2020). The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic. *Journal of Law and the Biosciences, 7*(1). https://doi.org/10.1093/jlb/lsaa038

[48] Bacchi, U. (2022, 9 March). Pandemic surveillance: is tracing tech here to stay? *Thomson Reuters Foundation*. https://news.trust.org/item/20220304092506-akyoc

[49] See: https://privacyinternational.org/learn/public-private-surveillance-partnerships; Privacy International. (2021, 18 November). Huawei and Surveillance in Zimbabwe. https://privacyinternational.org/long-read/4692/huawei-and-surveillance-zimbabwe; Privacy International. (2020, 25 June). Huawei infiltration in Uganda. https://privacyinternational.org/case-study/3969/huawei-infiltration-uganda

[50] Privacy International. (2020, 8 April). Covid-19 response: Corporate Exploitation. https://privacyinternational.org/news-analysis/3592/covid-19-response-corporate-exploitation

[51] See, for example: Digital Rights Foundation. (2021). *Virtual Learning and Privacy Amid COVID-19*. https://digitalrightsfoundation.pk/wp-content/uploads/2022/01/Virtual-Learning.pdf; https://cetic.br/pt/tics/pesquisa/2020/escolas/G1; https://www.worldbank.org/en/topic/edutech/brief/how-countries-are-using-edtech-to-support-remote-learning-during-the-covid-19-pandemic

[52] Muñoz-Najar, A., Gilberto, A., Hasan, A., Cobo, C., Azevedo, J. P., & Akmal, M. (2021). *Remote Learning during COVID-19: Lessons from Today, Principles for Tomorrow*. World Bank Group. https://documents1.worldbank.org/curated/en/160271637074230077/pdf/Remote-Learning-During-COVID-19-Lessons-from-Today-Principles-for-Tomorrow.pdf

[53] Duball, J. (2020, 28 April). Shift to online learning ignites student privacy concerns. *IAPP*. https://iapp.org/news/a/shift-to-online-learning-ignites-student-privacy-concerns

[54] Muñoz-Najar, A., Gilberto, A., Hasan, A., Cobo, C., Azevedo, J. P., & Akmal, M. (2021). Op. cit.

[55] For example, Google Workspace for Education, which includes Google classroom. It was first introduced in Amazonas state, Brazil, in 2015; see: Repórter Parentins. (2015, 8 April). Governador José Melo formaliza parceria do Governo do Estado com Google para serviços tecnológicos educacionais. https://reporterparintins.com.br/?q=276-conteudo-2657-governador-jose-melo-formaliza-parceria-do-governo-do-estado-com-google-para-servicos-tecnologicos-educacionais; see also da Cruz, L. R., & Venturini, J. R. (2020). Neoliberalismo e crise: o avanço silencioso do capitalismo de vigilância na educação brasileira durante a pandemia da Covid-19. *Revista Brasileira de Informática na Educação, 28,* 1060-1085. https://br-ie.org/pub/index.php/rbie/article/view/v28p1060

[56] UN Special Rapporteur on the right to education. (2020, 20 June). Right to education: impact of the coronavirus disease crisis on the right to education – concerns, challenges and opportunities. A/HRC/44/39. https://www.ohchr.org/en/calls-for-input/reports/2020/report-impact-covid-19-crisis-right-education; UNICEF. (2021, 29 April). Crianças de 6 a 10 anos são as mais afetadas pela exclusão escolar na pandemia, alertam UNICEF e Cenpec Educação. https://www.unicef.org/brazil/comunicados-de-imprensa/criancas-de-6-10-anos-sao-mais-afetadas-pela-exclusao-escolar-na-pandemia

[57] Privacy International. (2021, 10 November). Why we need to talk about digital health. https://privacyinternational.org/long-read/4674/why-we-need-talk-about-digital-health

Since the start of the pandemic, companies all over the world have pitched data products, services and solutions to COVID-19 – from big tech to companies that might not be household names. Well-known software companies like Palantir invested in a COVID-19 response by offering health data management solutions to countries across the globe.[58]

Furthermore, with the need at certain points in the pandemic to limit in-person interactions and limitations in reaching those in diverse geographic locations as a result of restrictions on movement, telemedicine experienced a global boost.[59] Diverse tools have been used, from real-time, video-based health consultations and advice, to health monitoring apps/software and sensor-based systems, among others.[60] As few governments develop their own software and hardware or infrastructure, industry has already played different roles, from providing digital health initiatives such as mass, centralised databases for patient management to the use of applications and other digital tools for the delivery of care.

While they have the tools and resources, with many having shaped their business models around data exploitation and surveillance, we need to ensure that whatever contributions companies make in the health care sector improve access to and quality of care while protecting people and their rights.[61]

Employment

Employees and workers were dramatically impacted by this pandemic, and then by government and employers' responses. The private sector swept in with their products, with many being deployed with very limited or no consideration for the risks associated with them for workers, their rights, and their well-being.[62]

Remote working forced employers to expand or adopt a new digital infrastructure to enable their employees to work using online platforms for communication, and cloud solutions to share documentation and information, among other tools to enable the day-to-day operations of their businesses.[63] As this evolved and grew, we saw a shift that led to measures focused on surveillance and constant monitoring of workers to keep track of performance and efficiency.[64]

Another result of lockdown measures and other limitations on movement has been the boom in home delivery applications and other gig economy sectors such as transportation.[65] This is a sector where there has been unprecedented surveillance that gig economy workers are facing from their employers. We are all coming to finally recognise and listen to concerns around the labour rights of the gig economy workforce and how the experience of these workers is being shaped by platforms they have little or no control over.[66]

Future proofing

We all experienced this pandemic, and we all have our own set of reflections about what worked or didn't. At Privacy International we worked with partner organisations across the world, engaged with governments, and worked with international organisations and industry as we all struggled through appropriate responses. Throughout we can say that much was missing: adequate public health resources and infrastructure, fairness in access, equality in rights and capability, trust and confidence. And yes, data about the virus.

Now, looking back from wherever we are within this pandemic, we are very concerned that governments and industry are only focusing on the problem of inadequate data. If that is the only lesson, then the calls for more data and tech will follow – which means more tech sector in our health care, more data sharing, and more exploitation. That will all come at the cost of increased social protection. And it will predicate future responses, arming public health responses to prioritise strict quarantine enforcement rather than helping people to care for themselves and others; coercion and compulsion

[58] Privacy International. (2020, 6 May). (Sort of) Trust but Verify: Palantir Responds to Questions about its work with NHS. https://privacyinternational.org/long-read/3751/sort-trust-verify-palantir-responds-questions-about-its-work-nhs; see also: https://www.palantir.com/covid19

[59] Mou, M. (2020, 22 October). Covid-19 Gives Boost to China's Telemedicine Industry. *Wall Street Journal*. https://www.wsj.com/articles/covid-19-gives-boost-to-chinas-telemedicine-industry-11603379296

[60] Privacy International. (2021, 28 October). Telemedicine and data exploitation. https://privacyinternational.org/long-read/4655/telemedicine-and-data-exploitation

[61] Privacy International. (2021, 8 November). Digital Health: What does it mean for your rights and freedoms. https://privacyinternational.org/long-read/4671/digital-health-what-does-it-mean-your-rights-and-freedoms

[62] University of St Andrews. (2021, 22 November). Employer surveillance during COVID has damaged trust. *Phys.org*. https://phys.org/news/2021-11-employer-surveillance-covid.html

[63] Rodriguez Contreras, R. (2021, 15 December). COVID-19 and digitalisation. *Eurofound*. https://www.eurofound.europa.eu/data/digitalisation/research-digests/covid-19-and-digitalisation

[64] Privacy International. (2020, 7 May). Unlocking workplaces, virtually locking workers in. https://privacyinternational.org/news-analysis/3757/unlocking-workplaces-virtually-locking-workers

[65] Bueno, C. C. (2020, 1 December). Pandemia, Tecnología y Trabajo. *Global Data Justice*. https://globaldatajustice.org/gdj/191/

[66] Privacy International. (2021, 13 December). Managed by Bots: surveillance of gig economy workers. https://privacyinternational.org/long-read/4709/managed-bots-surveillance-gig-economy-workers

over public educational programmes; profiling, identification and rationing over open access to public health services.

In addition to the direct measures deployed to respond to the health crisis, there is a need to scrutinise what shifts occurred across sectors, from the delivery of health care, to employment settings and remote learning, in a moment of panic and urgency with few measures subject to the necessary deliberations. This is necessary before current problematic practices become the foundation of our day-to-day lives in which industry has been let in, but should now be showed the way out or at least put back in its place.

The COVID-19 pandemic showed how fragile our protection framework is when it comes to protecting people, their rights and data. Governments and companies were too easily able to deploy digital initiatives with little scrutiny, limited transparency, and weak accountability.

Starting now and going forward, we must reflect on these lessons to identify where and how we must spend our energy to strengthen the protection of people and their data, and to hold governments, companies and other third parties to account across the human rights protection framework. This is critical in advocating for people's fundamental rights and freedoms, from privacy to the right to health, education, fair working conditions, non-discrimination, and freedom of movement, among others. There will be future emergencies. We must be ready.

Another look at internet regulation: Lessons from the COVID-19 pandemic

J. Carlos Lara and Jamila Venturini
Derechos Digitales
https://derechosdigitales.org

Pushed into the digital realm

Between techno-authoritarianism and techno-solutionism

The COVID-19 pandemic reached several countries in Latin America in the middle of a complex political context. Bolivia was under an interim government, after the president resigned following large demonstrations that questioned the electoral process at the end of 2019. Chile was about to settle a new social consensus as a result of months of protests that questioned the neoliberal foundations of its state. Ecuador was also leaving a process of strong social unrest, while in Colombia there had been months of protests after a large strike in November 2019. In all these cases, evidence of human rights violations and state abuses generated concerns throughout the region and among international authorities. A similar situation happened in Brazil where, after one year into the mandate of the far-right Jair Bolsonaro, violence, harassment and attempts to criminalise media workers, human rights defenders and civil society organisations became the norm. Similar scenarios were advancing in El Salvador and Mexico.

And then the pandemic struck the whole world. While it brought legitimate urgent needs to secure people's access to vital services in a safe manner, from the start it was also used in many countries as an excuse for limiting fundamental rights such as access to information, freedom of expression and assembly, and privacy. Decrees criminalising legitimate speech, limiting existing obligations on access to public information by governments, and authorising sensitive information sharing between public and private parties without further safeguards or transparency measures, demanded quick responses from civil society organisations and human rights authorities.

At the same time, an impulse towards the digitisation of daily activities during isolation periods was quickly normalised, and allowed Big Tech and local startups to gain space to promote their businesses. What they found were outdated or non-existing rules, overloaded or precarious supervisory institutions and a generally techno-optimistic – tending to techno-solutionist – environment that allowed their quick advance in vastly different areas. It was an environment that also lacked sufficient space for participation in decision making and did not put in place due safeguards against eventual abuses.

Privatised monitoring and control

As the pandemic advanced throughout the world and isolation measures were adopted to contain its spread, digital technologies became key to governments' responses at different levels of policy making. As cases started to increase, partnerships with telecommunications companies were quickly announced to monitor compliance with quarantines through heat maps that allowed governments to understand patterns of mobility. However, these initiatives did not provide information on which types of data were being shared and under what conditions. Companies specialised in geolocation were also involved in this type of early initiative to monitor and control cases.[1]

Replicating strategies implemented in the global North, a second wave of initiatives involved the launch of so-called "CoronaApps": usually mobile applications or chatbots – sometimes accompanied by web-based portals – that promised to deliver reliable information to the public and to support the monitoring of cases and the patterns of population mobility during periods of social isolation, as well as to improve offline contact tracing practices with online exposure alerts. These apps were launched in a decentralised and disorganised manner in several countries by public and private actors and at

[1] For some examples from Brazil, see: Venturini, J., & Souza, J. (2020). *Tecnologias e Covid-19 no Brasil: vigilância e desigualdade social na periferia do capitalism*. Heinrich Böll Foundation. https://br.boell.org/sites/default/files/2020-06/Tecnologias%20e%20Covid-19%20no%20Brasil%20vigil%C3%A2ncia%20e%20desigualdade%20social%20na%20periferia%20do%20capitalismo.pdf

different administration levels – municipal, state and national.

Most of these initiatives were based on public-private agreements and required the collection and processing of large amounts of personal and sensitive data. However, they were generally not preceded by human rights or privacy impact assessments, or launched together with clear information on the conditions and limits for the use of data by third parties. On the contrary, in several cases, exception measures were approved to allow their use.[2]

Since, in general, independent evaluation or monitoring was not an aspect of these initiatives, it is difficult to know the role they had in containing the spread of the pandemic. In any case, as human rights authorities have pointed out, they should have gone through an assessment of legality, necessity and proportionality.[3] In Latin America, the incipient adoption of mobile apps, ranging from 0.5% to 22% in December 2020, indicates a lack of contextualisation of solutions imported from abroad and presented as efficient tools. This particularly affected the exposure notification function incorporated in some of the apps, which was highly dependent on widespread use, something affected by several factors, including digital divides.[4]

A future for everyone?

Persisting digital divides and the lack of underlying digital infrastructures did not prevent tech-based responses from flourishing even when digitisation levels in the public sector were only starting to be felt. Although on average Latin America had around 67% of the population as internet users in 2019, it was only 55% in Peru and 49.5% in El Salvador. Divides between urban and rural areas were also significant: in Colombia, while around 72% of internet users were concentrated in urban areas, rural users were only 36%. The average difference was around 25%.[5]

When it comes to digital or "electronic" government, until 2018, most Latin American countries had a medium index of development.[6] The lack of readiness to respond to the pandemic became evident from the beginning, and the difficult monitoring of cases and deaths was a challenge that, together with other factors, prevented an efficient response in some countries. Trust in data from private parties and in the voluntary use of apps by citizens was necessary for policy making, as well as independent citizen, academic or media monitoring.

Pre-existing or newly implemented restrictions on citizens' access to information contributed to disinformation.[7] In some cases, like Brazil, political polarisation on the pandemic fostered by the national government led to constant changes in the methods for monitoring the evolution of the virus in the country and, as a consequence, generated distrust in official information. In December 2021, while the number of cases began to increase again in the world, an attack on the Brazilian Ministry of Health systems left the country without updated information on the evolution of the pandemic for more than a month.[8]

Despite the context of persisting inequalities and unpreparedness, decision makers rushed to promote poorly designed tech-based solutions, leaving thousands of people behind. An illustrative example is the one of education: without previous studies or concrete measures to mitigate digital divides, an emergency distance learning model was quickly implemented in several countries. This not only pushed millions of children into exclusion from their right to education, but put at risk the ones who could connect, as emergency online education was highly mediated by intensive data-collecting private platforms that benefited from direct agreements with governments without further supervision or accountability.[9]

Updating regulatory schemes

The centrality of the use of digital technologies to respond to the pandemic came with a force much

[2] For a deeper analysis of the applications implemented during the pandemic in Latin America, see: Venturini, J., et al. (2021). *Informe Observatorio Covid-19 del Consorcio Al Sur: Un análisis crítico de las tecnologías desplegadas en América Latina contra la pandemia*. Al Sur. https://www.alsur.lat/sites/default/files/2021-06/Informe%20Observatorio%20Covid-19%20del%20Consorcio%20Al%20Sur%282%29.pdf; for an in-depth analysis of each platform, see: https://covid.alsur.lat/en

[3] See, for instance, Resolutions 1/2020 and 4/2020 from the Inter-American Commission on Human Rights: https://www.oas.org/en/iachr/decisions/pdf/Resolution-1-20-en.pdf and https://www.oas.org/en/iachr/decisions/pdf/resolution-4-20-en.pdf

[4] Ferretti, L., et al. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science, 368*(6491). https://science.sciencemag.org/content/early/2020/03/30/science.abb6936/tab-pdf

[5] Patiño, A., Poveda, L., & Rojas, F. (2021). *Datos y hechos sobre la transformación digital*. CEPAL. https://www.cepal.org/sites/default/files/publication/files/46766/S2000991_es.pdf

[6] Ibid.

[7] ARTICLE 19. (2020, 11 May). Closing the COVID-19 response transparency gap. https://www.article19.org/resources/closing-the-covid-19-response-transparency-gap

[8] Bertoni, E. (2022, 6 January). O impacto do apagao de dados em meio ao avaço da ômicron. *Nexo*. https://www.nexojornal.com.br/expresso/2022/01/06/O-impacto-do-apag%C3%A3o-de-dados-em-meio-ao-avan%C3%A7o-da-%C3%B4micron

[9] Human Rights Watch. (2022). *"How Dare They Peep into My Private Life?": Children's rights violations by governments that endorsed online learning during the Covid-19 pandemic*. https://www.hrw.org/sites/default/files/media_2022/06/HRW_20220602_Students%20Not%20Products%20Report%20Final-IV-%20Inside%20Pages%20and%20Cover.pdf

stronger than any push to update the regulatory frameworks applicable to those technologies. What the first two years of the pandemic have shown is an exaggerated version of what we knew before the COVID-19 crisis: regulatory schemes that apply to the internet, both at the national and the international level, seem unable to respond to the demands of emergency situations and social unrest. Many institutional frameworks, which were already trying to cope with the challenge of a digital environment ever-more concentrated in a handful of tech companies, were given new priorities and reasons for concern when the COVID-19 pandemic hit. As the health measures and emergency relief took up the public agenda, other regulatory needs were put in second place.[10]

The need for regulatory updating is not necessarily a matter of technology regulation in and of itself, but rather part of a larger set of regulatory challenges. Some of these are dependent on states themselves, some on the international community, and in all cases they deal with the pressures and constraints of a globalised digital economy. Although the pandemic stopped or slowed down many relevant decision-making processes throughout the world, resuming those processes or starting others anew needs to acknowledge these challenges.

First, the prevalence of digital technologies in all aspects of human life requires addressing the challenges of exclusion from a rapidly digitised global economy. Given that not only emergency health measures but work, commerce and education are mediated through the internet, improving connectivity is necessary. Moreover, when state services and social security are digitised – a process which accelerated during the pandemic – states should be aware of and address the risk of exclusion in the provision of those services.[11] In times when there has been such a large need for swift governmental aid or digitised services, the challenge is to provide not just affordable internet, but meaningful connectivity.[12]

Second, the same connectivity that empowers and facilitates positive change should not be a source of abuse as a result of the mere act of using the internet. The very real possibility of the pandemic being used as an excuse to enhance surveillance capabilities[13] was evident from the very beginning, when we saw many examples of social media "cyber patrolling" and even drone surveillance.[14] In turn, when private services collaborate with states by providing data or technologies,[15] or otherwise continue their pattern of exploitation of internet users, emergencies such as the current pandemic improve their prospects enormously.[16] The challenge of reining in both state and corporate power presents the need for data governance frameworks that give control back to data subjects, whose identity, existence, activity and labour provide the information that is currently exploited by governments or others for their own purposes. Data control mechanisms are thus needed at every stage in the development and deployment of technologies, and need also to account for special circumstances that in the name of "emergency" might be used to lower legal safeguards.

Third, the need for a safe online space requires thinking deeply about how to reconcile swift action against hate speech and the legitimate exercise of rights online, acknowledging that regulatory change is far from a comprehensive solution by itself. The continuum of offline and online gender-based violence has seen a worrying increase during the pandemic too.[17] If we take this example, long-due regulatory change must also consider the offline implications of what happens online – and the role of platforms with the capacity to react must also be acknowledged.

Safety concerns have been front and centre with regard to the proliferation of misleading or false information during the pandemic. Information disorders around sensitive or hard-fought issues such as the climate crisis, national elections or the COVID-19 pandemic itself can thrive during a generalised state of panic. Regulatory responses to this problem need to acknowledge its complexity, and internet companies' response, however useful,[18] should not become a way to censor dissenting views or adjudicating the truth of contentious matters or ongoing emergencies. A high risk comes from the

[10] Canales, M. P. (2020, 2 April). Tecnología contra la pandemia: derechos fundamentales mucho más que daño colateral. *Derechos Digitales*. https://www.derechosdigitales.org/14355

[11] Souter, D. (2020, 23 February). Inside the Digital Society: Digital inclusion and social inclusion. *APC*. https://www.apc.org/en/blog/inside-digital-society-digital-inclusion-and-social-inclusion

[12] A4AI. (2020). *Meaningful Connectivity: A New Target to Raise the Bar for Internet Access*. Alliance for Affordable Internet. https://a4ai.org/wp-content/uploads/2021/02/Meaningful-Connectivity_Public-.pdf

[13] Surber, R. S. (2022, 4 April). The institutionalisation of fear: Global surveillance with dubious pandemic legitimacy. *Open Access Government*. https://doi.org/10.5167/uzh-218969

[14] Lara, J. C. (2020, 1 May). La pandemia de COVID-19 y la pulsión por la vigilancia estatal. *Derechos Digitales*. https://www.derechosdigitales.org/14411

[15] Venturini, J., et al. (2021). Op. cit.

[16] BBC. (2021, 27 July). Tech giants' profits soar as pandemic boom continues. https://www.bbc.com/news/business-57979268

[17] Derechos Digitales (2020, 10 July). La otra pandemia: internet y violencia de género en América Latina. https://www.derechosdigitales.org/14716/

[18] Butcher, P. (2021). COVID-19 as a turning point in the fight against disinformation. *Nature Electronics, 4,* 7-9. https://doi.org/10.1038/s41928-020-00532-2

state itself: regulatory action against disinformation can become a source of punishment of speech or a channel for surveillance,[19] or an excuse to maintain government control of public debate.[20] Additionally, state measures to either ensure compliance with the law or to detect (read: adjudicate) false information, such as the cyber patrolling of fake news during the pandemic in Bolivia[21] and Colombia,[22] is a worrying development, and state action must also be strictly limited by applicable rules.

To all of the above we must add the risks that cyberspace represents in terms of cybercrime, and more specifically, the likelihood of internet users being affected by cyber attacks, including hacking. As much as cybercrime legislation needs both updating and harmonisation, while remaining respectful of human rights concerns, international negotiations for a new cybercrime treaty that may yet expand states' capacity to prosecute as cybercrime even ordinary felonies with digital elements is an ongoing concern.[23] A safe digital environment is not just one free from exploitation, violence, harassment and disinformation, but also free from surveillance and undue prosecution.

Another look at internet regulation

Of course, the COVID-19 pandemic has already caused regulatory change, in the form of emergency measures, states of exception, and changes in regulatory requirements for certain regulated processes, especially those linked to health services or financial aid. Whether this has been effective, what its effect is in the long term, or what it means for internet regulation in general, requires us to take another look at what has happened, and what the remaining challenges are.

Rethinking governance and rule making

Beyond the current emergency, states should rethink how their regulatory policy is enacted with regard to the internet. This is necessary in order to formulate well-designed policies based on evidence and expert views but also on participatory processes, with mechanisms for evaluation and monitoring, coordination between state agencies and with the private sector, and effective mechanisms for enforcement and democratic accountability. Commitments for continued monitoring and evaluation, and mechanisms to review ongoing measures, are also necessary regardless of how urgent the measures or reforms that may have to be passed.

This requires addressing the fulfilment of the needs of everyone, understanding that digital technologies and the internet can and should have a role, but that their sole existence is no guarantee of modernisation or efficiency. Avoiding techno-solutionism is key not to fetishise technologies without centring efforts on people.

The challenge requires us to properly identify the objectives of any regulatory effort. Containing, preventing and mitigating the effects of a health risk as well as its impact on society, and promoting a safe return to normality, requires careful consideration of available evidence and shared priorities. The likely effects of the chosen regulatory reaction must be evaluated to prevent undesired effects or undue human rights restrictions.

A bottom-up regulatory agenda

One crucial element when rethinking the regulatory challenges of the internet after the pandemic has to do with the acknowledgement of local contexts. The realities, needs and priorities of local groups should be considered when attempting regulatory solutions, instead of importing those solutions from very different contexts. Of course, that becomes all the more difficult when the pressures of international relations seem to demand a prioritisation of commerce. The negotiation of international treaties and free trade agreements seems to favour the governments, institutions and companies that have benefited from a privileged position from the start of the growth of the internet (especially since the birth of the world wide web), as well as governments with high degrees of control over their domestic communications and data economies.

We must reconsider the role of our governments as representatives of agendas different from those of powerful states and big companies. That requires a degree of democratisation that may exceed the idea of internet regulation. Internet regulation, like all regulation, should be an expression of what society wants as rules for itself, not what a few interests deem the greater good.

[19] Coalizão Direitos Na Rede. (2020, 1 September). Propostas da coalizão ao PL 2630/20 para torná-lo uma lei efetiva e democrática. http://plfakenews.direitosnarede.org.br

[20] Ünker, P. (2022, 31 May). Turkey seeks to tighten media control with 'fake news' bill. *DW*. https://www.dw.com/en/turkey-seeks-to-tighten-media-control-with-fake-news-bill/a-61990381

[21] Céspedes, D., & Machaca, W. (2021). *Ciberpatrullaje y desinformación durante la pandemia en Bolivia*. Fundación InternetBolivia.org. https://internetbolivia.org/file/2021/07/ib_invdi.pdf

[22] Ospina-Valencia, J. (2021, 4 November). Ciberpatrullaje estatal en Colombia: una práctica que urge regular en América Latina. *DW*. https://www.dw.com/es/ciberpatrullaje-estatal-en-colombia-una-pr%C3%A1ctica-que-urge-regular-en-am%C3%A9rica-latina/a-59726694

[23] EFF et al. (2021, 22 December). Letter to the United Nations to Include Human Rights Safeguards in Proposed Cybercrime Treaty. https://www.eff.org/deeplinks/2022/02/letter-united-nations-include-human-rights-safeguards-proposed-cybercrime-treaty

Towards a shared governance for our digital future

Internet policy today concerns much more than the internet as our lives and bodies are forced into digitisation. Naïve as it may sound, the global crises, wrought and worsened by the pandemic, present an opportunity; this time not only for those ready to take advantage from their positions of privilege. This is not only because there is more consensus on the need for updating regulatory frameworks, including those that govern the internet, in a way that protects and promotes human rights for all. It is also because the pandemic exposed the consequences of neoliberalism and evidenced the urgency to build alternative development models that include tech developed from a sustainable perspective. New forms of regulation and policy making are key for that to be achieved; otherwise, Latin American countries, and other countries in the global South, will continue to depend on infrastructures that result in dependency, inequality, human rights violations and abuses.

This includes long overdue efforts to update the rules that govern the rights to control personal information, express one's views and organise social movements, and it also extends to the use of the internet itself as a vehicle for cultural, environmental and social rights. It extends to the governance of the internet beyond national borders, to ensure it can continue to facilitate rights and avoid the risks of government control and corporate capture. And in all cases, it demands a larger role from the citizens: it is an opportunity to leverage democracy for a better internet. For a better digital future for all, we must advocate not only for new rules, but for the democratisation of all spaces where rules are made.

Advocacy for community-led connectivity access in the global South

Kathleen Diga, Cynthia el Khoury, Michael Jensen, Carlos Rey-Moreno and Débora Prado
Local Networks (LocNet) Initiative, APC
https://www.apc.org/en/node/35376

Introduction

Since the start of the pandemic, there has been a strong revival of interest in digital rights, especially with respect to ensuring that everyone has internet access. The increase in internet traffic recorded across the world, caused by those working from home and children taking school lessons from their place of residence, is no doubt part of this revival.[1] However, COVID-19 also highlighted that home internet is not the norm; there still remains a large majority of people residing in low-income or unserved areas without any connectivity, or expensive mobile bundles as their only option. As a result, advocates have raised their voices regarding connectivity being a priority for all countries that must be achieved universally to ensure that no one is left behind.[2]

This thematic report walks through three stages of work completed by the Local Networks (LocNet) initiative,[3] focusing on advocacy for community access, under the project name "connecting the unconnected". Firstly, two pre-pandemic actions within LocNet helped to set the groundwork, mainly around international policy advocacy and direct support for community-led action for local connectivity. Secondly, as a result of communities and nations being locked down due to the pandemic, the report details two follow-up actions which supported national governments with innovative regulation to legitimise local actors providing connectivity and to provide support to community network partners who are contending with substantial communications and connectivity demands in their regions. Thirdly, the pandemic led to a need for more inward reflection by the LocNet team on advocacy for local access in the future. Specifically, what does it mean to move from originally trying to broadly address universal services, or "connecting the unconnected", to an understanding of "meaningful connectivity" coming from a community-led perspective? Finally, the chapter closes off with what is next in terms of advocacy for community-led access.

Pre-pandemic advocacy activities

The pandemic has made many of the structural inequalities that exist throughout the world clearly visible, but even more so in the global South. Prior to the pandemic, the LocNet team and the original 12 affiliated peers/partners were advantageously placed to start looking at local access challenges and the opportunities to learn and exchange ideas on how to accompany locally led connectivity processes.[4] The team was already developing a holistic approach to advocacy that would lead to the success of community-led initiatives, and had developed five areas of work.[5] In late 2018, advocacy would come from at least two salient strategies: 1) tackling the lack of awareness among policy makers and regulators, and developing a shared language for them around complementary connectivity models, and 2) having solid community-led cases by on-the-ground partners or champions which demonstrably provided

[1] OECD. (2020). *Keeping the Internet up and running in times of crisis*. https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9

[2] La Rue, F. (2011). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. United Nations Human Rights Council. https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

[3] The Local Networks (LocNet) initiative is a collective effort led by APC and Rhizomatica in partnership with people and organisations in the global South to directly support community networks and to contribute to an enabling ecosystem for their emergence and growth. Community networks cultivate bottom-up, sustainable approaches to communication technology and meaningful connectivity that strengthen autonomy and self-determination.

[4] https://www.apc.org/en/node/35438

[5] These five areas of work were defined in the following "work packages": Work Package 1: Peer Learning Exchange, Work Package 2: Learning and Capacity Building, Work Package 3: Enabling Policy and Regulation, Work Package 4: Innovation, Technology and Sustainability, and Work Package 5: Gender and Women's Participation. https://www.apc.org/en/node/35376

an alternative to traditional approaches to connectivity. In many cases, pre-COVID advocacy in these two areas were foundations to supporting community-led connectivity opportunities at the start of the pandemic.

Community network policy awareness and shared language

Prior to 2020, there were major gains around awareness raising for complementary models of internet access within international policy and regulatory spaces. Specifically, there were several like-minded groups which prepared the groundwork through the International Telecommunication Union (ITU),[6] the African Union Commission,[7] the United Nations Commission on Science and Technology[8] and other forums to ensure inclusion of policy language that was acceptable and amenable to currently excluded local operators such as community networks wishing to provide service in areas that mobile operators were not reaching. Persistent presence at the international meetings and consistent contributions in study groups and council working groups, among others, were necessary advocacy activities, especially when met with moments of rejection to the community network concept.[9] The inclusion of language in policies that enable community networks became foundational references for civil society to advocate at the regional or national levels for the inclusion of the same policy language to enable complementary telecommunications provision.

Yet even with the introduction of language supportive of community networks in policy spaces, awareness levels were still at nascent stages for many national and local government officials. Therefore, a substantial effort was made to describe this new lens for telecommunications,[10] as well as working with individual countries and regions to create policy-relevant training content, and to provide awareness-raising workshops for policy makers in Africa, Asia and Latin America.[11] Regional training through specific regional telecommunication bodies worked towards the much-needed effort to bring understanding of what was possible beyond traditional telecommunications provision that favours corporate national internet service providers (ISPs) and mobile operators. Beyond training, the LocNet policy team were also consistently monitoring public consultations around telecommunications, and when there was a request for public consultation, the team would mobilise and react promptly with other local civil society organisations to ensure timely submissions.[12]

Champions in community networks

In addition to policy advocacy, up to the beginning of 2020, there was a growing group of local grassroots institutions working on community mobilisation and creating “proof of concept” on-the-ground models of community networks. These “champions” were able to meet each other and exchange knowledge of their work through LocNet learning opportunities and other regional meet-ups. Specifically, before 2020, there were advocacy activities to research[13] and document[14] what existed in the community networks space. In linking some of these global South groups, further learning spaces allowed for small and medium-sized enterprises or non-profit groups to physically visit each community network site and exchange lessons on processes of community-led change and providing connectivity services.[15]

Through the above, many community network champions can now offer remarkable case studies,[16] and advocate and meet the demand for locally led communications initiatives, particularly in rural areas and where other barriers to entry are high. The LocNet team’s work with local partners was to amplify their case studies and find opportunities to engage in close dialogue with other like-minded stakeholders, demonstrating both the successes and challenges of the community network model. From the policy perspective, these case studies were shared by the LocNet policy team and accompanying grassroots partners together at various levels of government to showcase the communication needs of local rural citizens. The ongoing dialogue and advocacy shows civil society commitment to processes of

[6] The implementation of Recommendation 19 from ITU-D for the Americas region: https://policy.communitynetworks.group/international-organisations/start#wtdc-17

[7] Specialized Technical Committee on Communications and Information Technologies (STC-CICT) from the African Union: https://policy.communitynetworks.group/international-organisations/start#african_union_commission

[8] United Nations Commission on Science and Technology for Development work in 2019 and 2020: https://policy.communitynetworks.group/international-organisations/start#cstd-19

[9] https://policy.communitynetworks.group/international-organisations/start#itu_plenipotentiary_conference

[10] Song, S., Rey-Moreno, C., & Jensen, M. (2019). *Innovations in Spectrum Management: Enabling community networks and small operators to connect the unconnected*. Internet Society & APC. https://www.apc.org/en/pubs/innovations-spectrum-management-enabling-community-networks-and-small-operators-connect

[11] https://2016-2019report.apc.org/2016-2019.html

[12] Ibid.

[13] https://www.apc.org/en/node/34231

[14] See, for example, Finlay, A. (Ed.). (2018). *Global Information Society Watch 2018: Community networks*. APC & IDRC. https://giswatch.org/community-networks

[15] https://www.apc.org/en/node/35438

[16] https://www.apc.org/en/tags/cn-stories

changing national universal access policy, including the revision of costly licensing processes for local operators.

The LocNet team and partners worked on these advocacy strategies, which led to three outcomes: 1) raised awareness of community-led efforts within policy circles, 2) a shared understanding and exchange among like-minded community network champions to meet and learn together, and 3) a greater awareness of success stories and the development of specific community-led models to showcase widely. These outcomes presented many possibilities to make connectivity alternatives more viable, should grassroots groups be given a chance.

Priorities of access during the pandemic

After mid-2020, the two enabling advocacy strategies that were established before the pandemic – international policy recognition and the identification of and exchange among local champions – were in full swing. Within the greater drive globally for accelerating connectivity, this was an opportune moment to go to the next level of advocacy for local connectivity access. During the pandemic, the LocNet team found themselves moving to a dual advocacy stage of accompanying national-level policy framework development and the subsequent operationalisation of policy, and accelerating local community network efforts. Several national government entities had previously engaged in dialogue with local partners or the LocNet team around policy changes or participated in awareness training on community networks. Due to COVID-19, pressure was mounting to help citizens to get connected. The next steps for many of the governments concerned was getting appropriate language into national directives or policy documents, as well as operationalising appropriate policy to support resource-poor regions in their efforts towards digital inclusion. With regard to communities, existing community network models now had further demand and backing from their communities, and they now needed to find ways in which to ensure their work could follow through by ensuring consistent communications for their users, allowing them to stay informed of health information, stay in touch with family and relatives, and access some form of education and training for their home-bound children.

Revival of digital rights and access in policy spaces

At the start of the pandemic, the lockdowns made clear that there was a pressing need to expand connectivity. As citizens became more vocal about their right to communicate digitally, some policy stakeholders took the opportunity to re-open the topic of access and, in some cases, implemented alternatives for underserved regions. Recommendations were sent to governments on ways to enable local operators.[17] Due to the pre-pandemic advocacy that the LocNet initiative and others had conducted, some initial policy dialogue inroads with governments were possible. There was some recognition that community network models were propagating and that national policy implementers would not have to start from scratch. In some cases, community networks also took this opportunity to meet with governments to showcase their community network model. They voiced their challenges in their work on local connectivity and how it needs policy space and licence exemption if the model is to expand to further underserved areas.

Several national governments, such as Zimbabwe, Mexico, Brazil, Argentina, Indonesia and Kenya, made revisions or new provisions within their policies, finding ways in which to legitimise the existence of small operators to provide telecommunication services to unconnected or underserved communities. Kenya enacted the community network licence framework.[18] Although Brazil's regulator acknowledged community networks in early 2020,[19] dissemination and sensitisation of the policy had to occur in order to popularise and educate people about the licence change. The LocNet initiative offered technical assistance to the Brazilian telecom regulator Anatel to bring stakeholders together through dialogue,[20] and in creating a policy brief[21] and accessible public information to accompany the policy work.[22] A strong champion of community networks and our advocacy partner in Zimbabwe,

[17] APC, Redes A.C., & Universidad Politécnica de Catalunya. (2020). *Expanding the telecommunications operators ecosystem: Policy and regulatory guidelines to enable local operators*. https://www.apc.org/sites/default/files/APC_R1_ExpandingTelecommunication_OK.pdf

[18] Kivuva, M. (2021, 9 November). Kenya adopts the community networks licensing framework. *KICTANet*. https://www.kictanet.or.ke/kenya-ratifies-the-community-networks-licensing-framework

[19] Kopp, M. (2020, 29 June). Brazil acknowledges community networks as viable option for connectivity. *APCNews*. https://www.apc.org/en/news/brazil-acknowledges-community-networks-viable-option-connectivity

[20] APCNews. (2021, 28 October). Multistakeholder collaboration to build an enabling environment for community networks in Brazil. *APCNews*. https://www.apc.org/en/news/multistakeholder-collaboration-build-enabling-environment-community-networks-brazil

[21] Labardini Inzunza, A., & Zanolli, B. (2021). *Policy brief and recommendations for an enabling environment for community networks in Brazil*. APC. https://www.apc.org/en/pubs/policy-brief-and-recommendations-enabling-environment-community-networks-brazil

[22] Kassouwi, I. K. (2022, 31 May). Zimbabwe unveils plans to facilitate digital communication with community networks. *Ecofin Agency*. https://www.ecofinagency.com/telecom/3105-43638-zimbabwe-unveils-plans-to-facilitate-digital-communication-with-community-networks

Murambinda Works, demonstrated its efforts to the government,[23] and the Zimbabwe telecom regulator (POTRAZ) has now made plans for a community network rollout in each province. Uganda rolled out their new communal access service provider or network operator licences in 2020.[24] Argentina also benefited from strong local advocacy by AlterMundi and others, seeing legislation adopted for the use of Universal Service Funds to resource community networks in underserved communities, both rural and urban. In Indonesia, partners have now identified an entry point for local internet provision through the decentralised village fund mechanisms enacted by the Ministry of Villages. Common Room Network Foundation, along with its wide range of ICT partners, is now working with local groups to explore the fund's possibility.

The greater demand for connectivity by and for the underserved and the willingness of some governments to consider and exchange information about complementary ways for communities to develop their own connectivity pathways is reflected in these recent policy changes.

Higher demand for local connectivity

At the local level, community network partners were approached by their neighbouring communities, who now needed to be connected to the internet – many were looking for a service with adequate connectivity speeds so that their children could be online during the lockdowns. This created a special opportunity to expand their work on enabling rural connectivity. The challenge saw local partners increase their internet provision capacity, including looking into how to improve the quality of their services. How to make these changes surfaced after much self-reflection, including considerations of where to hone in on institutional strengthening efforts.

Because of their holistic nature, community networks are usually not limited to the connectivity space – rather, they are integrated with other needs of the community. During COVID-19, this was evident from community network partners participating in local emergency-driven solutions to support each other.[25] As a result, particular local or civil society partners found their models put into intensive practice and use, largely based on citizen-driven needs. In order to ensure their work was recognised and amplified, their stories were shared and documented through blogs[26] and short videos,[27] and used as materials to advocate among civil society groups as well as to governments who were still unfamiliar with the community network option. The same local community network builders have also gone further to develop a national training programme – the National School for Community Networks, which has started in five countries[28] – as more neighbouring communities requested assistance for connectivity in their regions.

While not all civic advocacy and policy work can be attributed to the LocNet initiative, all of these examples are due to efforts by local activists and advocacy sustaining ongoing dialogue with governments – now, when the time has been most opportune, the policy changes have taken place with tremendous results in favour of community-driven networks.

Reflections on the experiences of "connecting the unconnected"

As the dual advocacy strategies – fostering enabling policy, and accompanying locally driven community network champions – started to gain significant traction during the pandemic, the LocNet team also reflected on its initial 2018 assumptions. These assumptions were developed as a project that responded to the needs for universal service by "connecting the unconnected", but from a holistic and community-driven perspective.[29]

Much has changed since the start of 2018. The greater demands in local connectivity during the pandemic meant that some governments have put in place "community network-friendly" policy directives, and now have the challenge of operationalising their new policy. Also, citizens who now use community network connectivity have integrated the internet better into their lives, creating new expectations of connectivity speeds or quality as well as thinking beyond the connection as to what value-driven needs can be met by the community networks.

As citizens are a part of their local community networks, and community networks are not just

[23] APCNews. (2022, 20 April). Murambinda Community Network and the Integral Kumusha: "We feel we're creating a movement that will be unstoppable". *APCNews*. https://www.apc.org/en/news/murambinda-community-network-and-integral-kumusha-we-feel-were-creating-movement-will-be

[24] https://www.ucc.co.ug/wp-content/uploads/2020/05/COMMUNAL-ACCESS-PROVIDER-LICENSE-25-05-2020.pdf

[25] APC & Rhizomatica. (2020, 22 May). Beyond Connectivity: Networks of Care. *MediaNama*. https://www.medianama.com/2020/05/223-beyond-connectivity-networks-of-care

[26] https://www.apc.org/en/tags/cn-stories

[27] https://www.apc.org/en/routingforcommunities

[28] APCNews. (2022, 26 May). Meet the national schools empowering grassroots communities to bridge the digital divide. *APCNews*. https://www.apc.org/en/blog/meet-national-schools-empowering-grassroots-communities-bridge-digital-divide

[29] https://www.apc.org/en/project/connecting-unconnected-supporting-community-networks-and-other-community-based-connectivity

about connectivity, but about nurturing broader community participation and cooperation, there has been further consideration of the possibilities of leveraging the positive changes gained for local or social development. This evolution in thinking has come from the last five years of accompanying local community network processes. It is also moulding the way the LocNet team will be thinking about the possible futures or next steps that would move forward participatory or community-based processes to meet unserved communication needs.

This is where we see a point of evolution for debate. As connected communities become accustomed to a particular level of connectivity, there is a rise in expectations of the quality of service, etc. What level of digital services will local community members manage to maintain, given the structural issues they deal with in their day-to-day lives? This includes embedding connectivity within the absence of consistent energy supply, paved roads, schools and living standards. What partnerships would be appropriate to strike the right balance of community involvement and network stability and quality?

The LocNet team has learned over time that community networks can be embedded within sustainable and participatory civic action, which goes beyond connectivity and engages in local economic activities that are socially aware, gender aware and environmentally aware.[30] The ability to sustain activities locally can be informed by the need to recognise and support the commitment of mutual support groups or collectives to rebuild a thriving rural community and ultimately restore humanity and the dignity of life. Again, what are the responsibilities of partners towards this localised future?

In this respect, in the LocNet initiative, sufficient momentum has been reached for some of the community network partners in the "connecting the unconnected" project to carry forward their plans of either strengthening their institutional capacity to accompany communities or to help to meet the communication needs of the communities. The network has gained experience and understanding, and as partners mature one can see their internet services stabilise, and community members begin to realise the value-added services that go beyond initial connectivity. For example, some are using the community network to support seed preservation through knowledge of these techniques being digitised and archived;[31] creating or tweaking community-owned and context-appropriate technologies[32] and services;[33] bringing local e-commerce services to rural citizens; creating Indigenous, language-diverse educational content for rural schools; and using connectivity to link bottom-up local actions for their well-being and increased meaning in their own lives. These local and participatory activities, which were reignited due to the community-initiated model of connectivity, have seen positive effects on social cohesion, strengthening the connection among people, and the creation of local value. But this has also raised community concerns of digital safety and privacy.

One angle to explore which has some resonance with the value-driven and social responsiveness of community networks is the concept of "meaningful access" or "meaningful connectivity". At a global level, meaningful connectivity has been defined as "a level of connectivity that allows users to have a safe, satisfying, enriching and productive online experience at an affordable cost."[34] Within this definition, there are measurable targets for the enabling drivers of infrastructure, affordability, access to devices, skills, and security and safety, that can inform whether one moves from no use to basic use, or skill to advanced quality of use.[35] Yet does this definition and its quantitative targets sufficiently fulfil or cover the local or lived experiences of community-led initiatives that have been observed in the five years of the LocNet initiative? Do they sufficiently account for making connectivity meaningful? In other words, how do we define meaningful connectivity from a community-driven or participatory perspective?

The LocNet team is taking time to unpack this idea so that it can inform and contribute to an alternative future, one that can address the on-the-ground realities and emergent needs for community networks and the people who live in the communities they connect. Ultimately, community connectivity creates an impetus to reinvigorate local and participatory action that unites the community, bringing people closer together so that they can better face the times ahead.

[30] "Connecting the Unconnected" project team. (2020). Community networks: A people – and environment – centred approach to connectivity. In A. Finlay (Ed.), *Global Information Society Watch 2020: Technology, the environment and a sustainable world: Responses from the global South*. APC. https://giswatch.org/node/6238

[31] https://videos.apc.org/u/apc/m/indigenous-communities-charting-their-journey-through-the-community-network-way/

[32] https://videos.apc.org/u/apc/m/bamboo-tower-for-community-networks-coolab-and-portal-sem-porteiras-brazil/

[33] https://videos.apc.org/u/apc/m/jxah-wejxia-fortaleciendo-nuestra-comunicacion

[34] Office of the Secretary-General's Envoy on Technology & International Telecommunication Union. (2022). *Achieving universal and meaningful digital connectivity: Setting a baseline and targets for 2030*. https://www.itu.int/itu-d/meetings/statistics/wp-content/uploads/sites/8/2022/04/UniversalMeaningfulDigitalConnectivityTargets2030_BackgroundPaper.pdf

[35] Ibid.

What next?

COVID-19 dramatically highlighted the digital divide and accelerated the efforts of civil society and governments to take unprecedented steps to improve policy directives for communities to be able to be connected. Advocacy for local access through community-led means has succeeded in some countries, and, as a result, certain policy measures have legitimised the operation of community networks. Yet there is a threat that these opportunities are not taken up on a large scale by local communities. What may be the cause? Are there still barriers to entry, such as technical barriers? Is there a lack of awareness or bureaucracy issues that get in the way? Perhaps there is an issue of trust? With the new policy momentum behind community networks, governments are now keen to see their legislation produce positive results. If they don't see these results, it may leave the civil society movement for local access high and dry.

Some steps forward to consider include:

- ***Documenting best practices:*** As community network builders and civil society groups are actively trying to operationalise the new policy opportunities, there are practical lessons to be learned by others. While the policies are good on paper, there are indications that civil society groups are not taking up the new opportunities, such as applying for social purpose licences in the new legislation regimes allowing this. The reasons for this are partly practical. From initial observations, local groups appear to be struggling to fill out the appropriate administrative paperwork and, in many cases, require help from a third party to complete the forms. It is important for the movement to document their learnings in cases such as applying for social purpose licences and share lessons with others in the movement, as well as to provide feedback to the government to show ways in which to improve its procedures for operationalising policy. This documentation – which should also cover other practical aspects of developing community networks – will also help to further develop the future narrative of the evolution of community networks beyond connectivity.
- ***Ongoing national level advocacy:*** While we have seen headway in some countries, the majority of current national telecommunication policies remain unable to bring other complementary providers to underserved communities. Therefore there is a need for ongoing outreach to potential allies and partners who are willing to work together in advocating for policy that enables community networks. There remains a need for dedicated advocacy calls for reforms to policy and regulation that could help to facilitate the emergence of local network operators in specific "high potential" countries. This includes developing research on the possibilities for community-led connectivity in these countries and hopefully accompanying any local champions. The LocNet team will continue its holistic form of advocacy, working at the intersection of international and national policy and the local community, creating specific policy briefs that share impact through evidence-based case studies.
- ***Sustainability of local efforts:*** What remains is how the existing community networks who mature in their connectivity provision can find ways to advance their sustainability models. The pandemic has meant that many, especially those working with rural communities, are in a fragile condition. Rising inflation and the high costs of living post-COVID-19 will not help this. Yet, at the same time, it is clear that community networks can address the increasing demand by citizens for local communication, which will come as fuel costs rise and travel becomes less and less possible. In these cases, there is a need for ongoing awareness raising of their work, finding the right communication mechanisms for sharing local demands and identifying complementary partnerships and/or support. As local access is not going away anytime soon, groups are also collaborating to research the variety of financial mechanisms for community-driven initiatives[36] and finding ways in which their work could be better articulated to would-be funders, and thereby helping community network partners find the means to help communities continue their outstanding work.

[36] https://connecthumanity.fund/ntoreport

Country and regional reports

BRAZIL

THE INTERNET, TECHNOLOGIES AND INEQUALITIES IN BRAZIL: THE INVISIBILITY OF BLACK WOMEN, TRADITIONAL PEOPLES AND COMMUNITIES, AND PEOPLE WITH DISABILITIES

Centro de Comunicação, Democracia e Cidadania da Universidade Federal da Bahia (Centre for Communication, Democracy and Citizenship at the Federal University of Bahia) and Intervozes – Coletivo Brasil de Comunicação Social (Intervozes – Brazilian Social Communication Collective)
Tâmara Terso,[1] Paulo Victor Melo[2] and Iraildon Mota[3]
https://ccdcufba.wordpress.com and
https://intervozes.org.br

Introduction

This report has two motivations: the deepening of inequalities in access to the internet and other information and communications technologies (ICTs) in Brazil during the COVID-19 pandemic, and the need to look at race, gender, territory and accessibility as the underlying factors of these inequalities.

In this context, the government's decision to digitise access to public services aimed at vulnerable groups,[4] even though they are the least connected groups, is questioned. At the same time, the invisibility of the issues that particularly affect rural Black women, traditional peoples and communities,[5] and people with disabilities in the advocacy agendas of digital rights organisations is striking.

In light of this, this report aims to a) draw attention to the fact that inequalities in access to the internet and technologies are shaped by "colour, gender, address and accessibility needs" and b) point out the importance of digital rights networks attending to the demands of these groups..

"Have you ever seen them cry over the orixá's colour?"[6]

On 13 May 2021, the anniversary of the day when slavery was abolished in Brazil over 140 years ago, the Brazilian Black movement protested that the effects of slavery had not been abolished in their entirety.[7] On the same day in Palmares, one of the main historical territories for *quilombos*[8] in the country, the Brazilian president announced that the Bolsa Família financial aid programme,[9] with some 25 million families registered, would end. In its place the government would make services available to the most vulnerable families exclusively through an internet platform.

This decision is part of a broader approach which involves the platformisation of social services in a deeply unequal country, as a way to increase exclusion.

Although 70% of rural households have internet access, its quality is poor and its costs are unreasonable. Some 84% of rural people access it exclusively through mobile phones,[10] with 41.24% of the quilombola and rural families that have internet access spending between BRL 51 and BRL 200 (between USD 10 and USD 39) per month on the service – and 56.20% have a monthly income of less than one minimum wage,[11] whereas 16.05% have no fixed income.[12]

[1] Tâmara Terso, an Amefrican journalist, holds a master's degree and is a doctoral candidate in the graduate programme in Communication and Contemporary Culture at the Federal University of Bahia (UFBA). She is a coordinator of the Centre for Communication, Democracy and Citizenship at UFBA and a member of the board of directors of Intervozes – Coletivo Brasil de Comunicação Social.

[2] Paulo Victor Melo is a professor and researcher of communication policies. He has a PhD in Contemporary Communication and Culture from the Federal University of Bahia, and is currently doing post-doctoral training at the University of Beira Interior/Portugal. He is a coordinator of the Centre for Communication, Democracy and Citizenship at UFBA.

[3] Iraildon Mota has a degree in Journalism and Public Relations from the State University of Piauí, and a post-graduate degree in Corporate Communication Management from the Federal University of Piauí. He also has an MBA in Business Management from the Getúlio Vargas Foundation. He is president of the NGO Comradio do Brasil and a member of Intervozes – Coletivo Brasil de Comunicação Social.

[4] These pro-poor services had been the result of years of struggle by civil society for recognition of the needs of vulnerable groups. By digitising them, the government was effectively negating this political and policy struggle, and making the services unavailable to many.

[5] Traditional peoples and communities represent a diversity of groups present in different parts of the country. Some of their common characteristics have been defined as their intrinsic relationship with nature, their relationship with territory, economic-productive rationality, interrelationships with other groups in the region, and self-identification (Dicionário da Educação do Campo, 2012).

[6] From the song "Boa Esperança" by Emicida.

[7] Brazil was the last country in the Americas to officially abolish slavery. Signed on 13 May 1888, the Lei Áurea officially ended slavery in the country. However, the law did not guarantee any rights or compensation to enslaved people and the slave mentality continues to structure political, economic, social and cultural relations in the country, and continues to sustain inequalities.

[8] *Quilombos* are settlements formed by Black people who escaped repression during the period of slavery in Brazil. The current inhabitants of these communities, descendants of their founders, are called *quilombolas*.

[9] Created in 2003, Bolsa Família was terminated on 11 August 2021.

[10] According to a survey carried out by the Brazilian Internet Steering Committee, available at: https://cetic.br/pesquisa/domicilios

[11] In Brazil, the minimum wage is BRL 1,110 a month. This amount is roughly equivalent to USD 216.53.

[12] http://territorioslivres.online

Similarly, it is alarming that less than 1% of the 28 million websites registered in Brazil are considered to be accessible to people with disabilities.[13]

Digital rights initiatives in the country seem to have difficulty in pointing out these issues. As an indicator of this: of the 22 statements published by Coalizão Direitos na Rede (CDR),[14] a coalition of Brazilian digital rights organisations, during 2021,[15] none mentioned the government's moves to make social assistance programmes exclusively accessible through the internet[16] and internet-enabled applications,[17] or the authorisation of tele-assessments,[18] moves that were criticised by social service organisations.

"Use the voice to say what is silent"[19]

The violation of the right to communication contributes to the worsening of symbolic and material violence against Black women, traditional peoples and communities, and people with disabilities.

From the invisibility of narratives and meanings (which Muniz Sodré called "semiocide") to the denial of the contribution of African knowledge in the construction of the cultural heritage of humanity, defined by Sueli Carneiro as "epistemicide", there is an alignment of terror and necropolitics.[20] Some of its most perverse expressions are the production of poverty on a large scale, the murder of men and women who defend their traditional territory-bodies against exploitative policies, the lack of accessibility policies in public spaces, and the political determination to "let them die", a sentiment directed at Black people, people with disabilities, and people from traditional peoples and communities. This has intensified during the pandemic.

There were practically no measures to minimise the effects of the health crisis on vulnerable populations. While agribusiness received prompt state support[21] and credit facilitation in public banks,[22] the only measure to mitigate the damages of the pandemic for traditional peoples and communities was vetoed by the president. Bill 1.142/20,[23] which established an Emergency Plan to face COVID-19 in Indigenous territories and support measures for quilombolas and traditional fishermen, was overturned by the National Congress – but even so, it was still detrimental to the people, particularly due to the withdrawal of social security measures such as food distribution.

On one hand, the rescue measures for agribusiness made it possible for the industry to expand its activities, and on the other hand, the delay in the attention to the territories of Black populations and traditional communities resulted in an acceleration in the loss of lives, especially of elders, who keep the ancestral knowledge of these peoples.

It was in this context that the National Coordination for the Articulation of Rural Black Quilombola Communities (CONAQ) denounced the lack of information on prevention measures against COVID-19 in quilombo communities. The scarce information that was available – due to poor infrastructure, including a lack of electricity, and low access to communication devices – came from TV, radio, and on messenger apps, without any monitoring by health agencies. And when information was available, it was not translated and made relevant to the ways of life of the quilombos.

A consequence of the poor access to credible information was the high circulation of misinformation and disinformation, with consequences such as difficulties in building community trust in the efficacy of vaccines against COVID-19 in some traditional territories.

Using the motto "We for us" (*Nós por nós*) as being the only way to confront the multiple rights violations faced by communities, civil society organisations have built support networks such as "Indigenous Emergency" and "Quilombo Without COVID-19", coordinated by the Articulation of Indigenous Peoples of Brazil (APIB)[24] and CONAQ[25] respectively. To help with prevention efforts, these initiatives mapped cases of COVID-19 among Indigenous people and quilombolas by cross-referencing official databases and monitoring information coming from the territories themselves.

[13] Forbes. (2021, 28 July). Menos de 1% dos sites brasileiros são considerados acessíveis, diz pesquisa. https://forbes.com.br/forbesesg/2021/07/menos-de-1-dos-sites-brasileiros-sao-considerados-acessiveis-diz-pesquisa

[14] The CDR is a coalition of more than 48 organisations that work for the defence of digital rights, with a particular focus on access, freedom of expression, protection of personal data, and privacy on the internet.

[15] https://direitosnarede.org.br/categoria/notas

[16] CFESS. (2021, 27 January). A defesa do Suas é essencial para a defesa da vida! Defender o CadÚnico é também defender o Suas! http://www.cfess.org.br/visualizar/noticia/cod/1785

[17] CFESS. (2021, 9 August). O acesso ao BPC pela população: vai ter audiência pública! http://www.cfess.org.br/visualizar/noticia/cod/1832

[18] CFESS. (2021, 9 July). Teleavaliação: um retrocesso para a população usuária e para o Serviço Social do INSS. http://www.cfess.org.br/visualizar/noticia/cod/1824

[19] From the song "Minha voz" by Elza Soares.

[20] Necropolitics can be conceptualised as the state's institutional determination of how some people have the right to life and how others should die or are expendable through the establishment of mechanisms to eliminate those considered "enemies" of the state. Mbembe, A. (2018). *Necropolítica*. N-1 Edições.

[21] Through the "CC-AGRO-COVID19" committee. http://www.planalto.gov.br/ccivil_03/Portaria/PRT/Portaria-37-21-mara.htm#art8

[22] PM 958 of 4/24/2020. http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Mpv/mpv958.htm

[23] Law 14.021/2020. http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14021.htm

[24] http://emergenciaindigena.apiboficial.org

[25] https://quilombosemcovid19.org

Black women and women from traditional peoples and communities played a leading role in the initiatives, such as Elza Ursulino, a leader from the Caiana dos Crioulos quilombo community in Alagoa Grande, Paraíba. She told us the following:

> I am on vacation, I am a community agent, but I spent an hour on my mobile phone transmitting information about the third dose of the vaccine, which is now being offered to people over 60.

The lack of internet access in traditional territories has also impacted education. A survey by the Anísio Teixeira National Institute for Educational Research reveals the severity of the situation: two million students in rural schools had no digital access[26] during 2020, with the distribution of printed content being the only alternative in several places.

Ednalva Rita, president of the community association of Caiana dos Crioulos, shared the reality of education under the pandemic in rural communities:

> It was difficult for the remote classes to happen here in the community, because only 5% of the community has internet – we are 130 families here. There are 187 students in the elementary school. Imagine this number of students without internet connections to carry out online activities. So, the teachers come at the beginning of the week, hand out the materials, the students complete the printed activities at home, and return after eight days to deliver the completed activities and pick up new ones. The online classes couldn't happen here.

All these difficulties were worsened by a government policy of blocking proposals that aimed to minimise the problems. A change in the law of the Telecommunications Services Universalization Fund, in order to authorise investments in internet network expansion and guarantee the connection of all public schools in the country until 2024, and Law 14.172/2020, which provided for the transfer of BRL 3.5 billion from the federal budget to guarantee internet access in elementary education schools, were opposed by the Brazilian president, both through a veto and a claim in the Supreme Court, postponing the possibility of their enforcement until 2022.

Other testimonies of the difficulties that people have faced when trying to participate in discussions about their own lives, or to access public services, are emblematic of how the Brazilian state, by denying the right to communication, develops necropolitical actions that consolidate colonial projects in the country.

Another example is that access to emergency financial aid[27] during the pandemic was only available via subscription on a smartphone app and in Portuguese, creating another socio-political and economic barrier. An appeal by the Federal Public Defender's Office and the state of Rio de Janeiro Public Defender's Office to make the smartphone application accessible to people with disabilities fell on deaf ears, and Bill 3563/2020,[28] which requires the government to ensure that all information on COVID-19 is also published in accessible languages, had not yet been passed.

A survey carried out by the University of São Paulo revealed that more than seven million people who were eligible to receive the emergency aid had no way to access it conveniently because they live in households without internet access. Many of these are rural Black women and traditional peoples and communities. The result? Huge lines formed at the doors of the branches of the public bank with families – mostly Black women – having travelled from rural areas to the cities looking for information on how to use the application in order to receive the aid.

This demonstrates how a country shaped by structural racism and ableism leads to policies that are created from the privileged view of white people and of people without disabilities.

Conclusion

"I have neither good nor bad internet, and even if I did, I wouldn't know how to participate in online meetings," said Maria de Fátima, a shellfish gatherer and fisherwoman from the quilombo community of Tororó in Bahia. "When it comes to these electronic things, these advanced machines, my child, I don't know anything: where it goes, where it comes from. I am sorry," she added. Her vent demonstrates the culpability of technopolitics in unequal environments. It subjects digitally excluded people to the construction of digital architectures which are incomprehensible to the diversity of ways of life.

The digital exclusion of these communities is part of the same structural context that includes the absence of demarcating Indigenous and quilombola territories, the political determination of socio-environmental destruction, and the institutional permissiveness that supports megaprojects over community rights.

[26] https://www.gov.br/inep/pt-br/assuntos/noticias/censo-escolar/divulgados-dados-sobre-impacto-da-pandemia-na-educacao

[27] Law 13.982/2020 allowed financial benefits for informal workers, individual microentrepreneurs, the self-employed and the unemployed as emergency protection during the COVID-19 crisis. Created by the National Congress in April 2020, the aid was paid until October 2021, with progressive reductions in amounts paid. According to a Datafolha survey, the aid was the main or only income of 68 million Brazilians in 2020.

[28] Still being processed in the House of Representatives. https://www.camara.leg.br/propostas-legislativas/2256479

How can one not relate these actions to statements made by the Brazilian president and his ministers, such as: "I will not demarcate one centimetre of Indigenous land"; "Children with disabilities get in the way of other students"; and "I have been in a quilombo. The lightest African descendant there weighed seven arrobas"?[29]

In this scenario, we cannot consider the denial of access to the internet and ICTs as if it is detached from the historical violations performed by the Brazilian state against the most vulnerable groups. In the same way, it is necessary to consider the demand for digital rights as part of the demand for the "right to exist".

This understanding informed the approach taken by initiatives launched by communications organisations and rural workers, quilombola communities, fisherpeople and small farmer movements, such as the *Territórios Livres, Tecnologias Livres* (Free Territories, Free Technologies) project,[30] and the podcast *Ondas da Resistencia* (Waves of Resistance).[31] One of the main objectives of these initiatives is to struggle against the invisibilities of marginalised communities and groups.

These collaborations have managed to advocate in national and international forums for better connectivity policies, pushing for the self-determination of communities in the implementation of internet infrastructure and its governance. Their participation in the last two Internet Forums in Brazil[32] and in a preparatory event for the global Internet Governance Forum 2021,[33] the preparation of a report on these issues[34] to international human rights bodies, as well as the election of a woman rural worker to the Committee for the Defence of Telecommunication Services Users are examples of advances they have made.

Action steps

The following steps are necessary to help shape a better future for marginalised communities in Brazil:

- Strengthen the capacities of Black women, traditional peoples and communities, and people with disabilities in order to help them develop digital rights initiatives and foster community-driven uses of technology, ensuring the autonomy of these groups.
- Disaggregate race, gender, territory and disability data in digital rights surveys.[35]
- Conduct digital rights research on the intersectional relationships between communication, technologies, race, gender, territory and accessibility.
- Strengthen the participation of Black women, traditional peoples and communities, and people with disabilities in civil society and multisectoral forums and networks in order to discuss public policy on internet access and ICTs, both nationally and internationally.
- Guarantee prior and informed consultation with traditional peoples and communities in public policies on social assistance, education, health and territory, among others, as well as their participation in defining and monitoring processes that lead to the digitisation and platformisation of public services aimed at vulnerable groups.

[29] Arroba is a term that refers to a unit of measure for weighing animals, especially cattle.

[30] http://territorioslivres.online

[31] http://ondasdaresistencia.org

[32] https://www.youtube.com/watch?v=bVGYM6sBeYc&ab_channel=NICbrvideos

[33] https://www.intgovforum.org/multilingual/content/igf-2020-ws-343-imagining-an-internet-that-serves-environmental-justice#undefined

[34] Intervozes. (2020, 6 October). Governo Bolsonaro promove desinformação e acusa organizações da sociedade civil de censura na CIDH. https://intervozes.org.br/violencia-e-divergencia-de-opiniao-e-desinformacao-e-liberdade-de-expressao-afirma-governo-na-cidh

[35] Currently this is not common practice in Brazil.

CONGO, DEMOCRATIC REPUBLIC OF

FACT CHECKING TO AVOID INTERNET SHUTDOWNS: LESSONS FROM THE DRC

Mesh Bukavu
Pacifique Zikomangane

Introduction

In the Democratic Republic of Congo (DRC), the COVID-19 pandemic has been accompanied by false information[1] that has made efforts to control the disease's spread difficult. As a result of this, the health measures taken and announced by the Congolese authorities to combat the spread of COVID-19 have not been respected by a significant number of people in the country. Social media has been the main platform for the propagation of the false information, presenting a real challenge for Congolese authorities.

In the past, when there was such a strong spread of false information, Congolese authorities immediately resorted to internet and SMS shutdowns.[2] This practice has always been denounced by human rights advocates.

In this report I am going to talk about how the COVID-19 pandemic has somehow changed the behaviour of Congolese authorities in the fight against false information. I discuss how Congo Check,[3] a Congolese fact-checking organisation, and Internews, an international media development NGO, have shown that educating the population about media content and producing good information is more effective in the fight against false information than internet shutdowns.

False information on COVID-19 in the DRC

The first case of COVID-19 was reported in the DRC on 10 March 2020 by the Congolese Minister of Health Dr. Eteni Longondo.[4] Nine days later, the government announced measures to fight the spread of the pandemic, among which all gatherings and meetings were prohibited, and schools, universities, discotheques, bars, cafés and restaurants closed. Later on, measures were taken to quarantine certain communes and neighbourhoods in the capital city of Kinshasa and in other cities of the country such as Goma and Bukavu.

All these responses to the pandemic triggered many forms of resistance in the country. This resistance was often directed against the containment measures and other restrictions on people's freedom of movement. The resistance also showed a distrust of the government. This was particularly felt in the eastern part of the DRC, where, in the face of growing insecurity due to the activism of armed groups, the population feels abandoned, is fighting for its survival and has little confidence in the authorities.

Some people believe that the authorities took these measures simply to get money from donors. Despite the increasing number of deaths from COVID-19, many say that the pandemic is only a "financial matter" which benefits the authorities in view of the significant resources mobilised by the government as well as by bilateral and multilateral cooperation organisations to fight this disease. This belief is reinforced by suspicions of the misappropriation and mismanagement of resources regularly reported in the media. These suspicions were not helped by rumours that people who did not die from COVID-19 were formally counted as victims of the pandemic in exchange for USD 5,000 per corpse, in order to amplify the pandemic's gravity.[5]

False information about the pandemic was circulated mostly on social media, and came in different forms, sometimes as a result of media reporting. One rumour that made it into the media even considered the office of the president as being at the epicentre of the first deaths reported at the beginning of the pandemic. Moreover, while cases and deaths from COVID-19 were recorded, the most publicised were those of well-known political, academic or religious leaders over 50 years old. This meant that most of the population thought and still thinks that COVID-19 is a disease that only affects the wealthy and elderly, and not young people who come from less

[1] This report uses the term "false information" to refer to misinformation and disinformation.

[2] Tungali, A. (2017, 31 March). The Evolution of Internet Shutdowns in DR Congo. *CIPESA*. https://cipesa.org/2017/03/the-evolution-of-internet-shutdowns-in-dr-congo

[3] https://congocheck.net/a-propos

[4] Crisis24. (2020, 11 March). DRC: First coronavirus case confirmed March 10. https://crisis24.garda.com/alerts/2020/03/drc-first-coronavirus-case-confirmed-march-10?origin=fr_riskalert

[5] Ekofo, J., & Ibaji, M. (2020, 9 September). Les rumeurs à la base du déni de Covid-19 : un obstacle à la lutte contre cette pandémie en République Démocratique du Congo. *CCSC*. https://www.ccsc-rdc.net/blog-single2.php?idart=679

affluent families – the latter representing the largest part of the Congolese population.

While social media was flooded by these sorts of misconceptions, rumours and false information, instead of internet shutdowns, which it had relied on in the past, the government took a different approach: it relied on the efforts of civil society organisations and international NGOs to produce and disseminate good information about the pandemic through the same social media.

Civil society organisation committed to fighting false information

"Our greatest enemy right now is not the virus itself. It's fear, rumours and stigma. And our greatest assets are facts, reason and solidarity."[6] These were the words of Dr. Tedros Adhanom Ghebreyesus, the Director-General of the World Health Organization. As in the rest of the world, false information in the DRC is about the spreading of unsourced messages through social media. These messages not only increased fear and uncertainty in the population but also fuelled the public's contestation of measures taken by government authorities to combat the pandemic, and increased the mistrust of information disseminated by the country's health and political authorities.

This situation has been a great challenge for the Congolese authorities. On the one hand, there was the need to push back against false information, and on the other hand, there was a need to enforce the health measures they had taken to fight against the spread of COVID-19.

While some feared internet shutdowns, they were surprised when the government instead relied on two independent organisations, Congo Check and Internews, for help.

Congo Check is a media outlet specialising in fact checking in the DRC. Created in 2018 in the context of the electoral process – often a time of much manipulation, including the manipulation of data and people in the DRC – its main purpose is to dispel misinformation and disinformation by providing accurate, fact-based information. Congo Check monitors information posted online, including through messaging apps such as WhatsApp – its journalists are members of some 30 to 40 WhatsApp groups.

Congo Check took up the fight against the spread of false information about COVID-19 by producing and disseminating verified and sourced information. The organisation has created a special section on its website – Fact Check COVID-19[7] – where it publishes news and information to deconstruct false information about the virus. Because false information is sometimes accompanied by doctored images, Congo Check also verifies images by using different tools such as Google's image search, InVID and TinEye. Congo Check does not receive any financial support from the government or any of the Congolese authorities. However, within the framework of COVID-19, the Ministries of Health and Communication have relied heavily on its work. This has included providing Congo Check with correct information on the pandemic and official information on government decisions and policies. Congo Check then uses this information to write the content of its articles and posts, which its publishes on its own website and social media pages.

From this perspective, Congo Check is a strategic partner for the Congolese authorities in the fight against the propagation of false information. As Rodriguez Katsuva, an editor at Congo Check, put it: "Every time there is a rumour, whether it's about the pandemic, whether it's about the government, whether it's about the actions of politicians, we do our job and in a concrete way we help the government."[8]

In addition to the work of Congo Check, the Congolese government has also relied on the work of international organisations such as Internews.[9] Internews is a global non-profit media training organisation that works with the media in the DRC, and has set up a project called COVID-19 Rapid Response in the Great Lakes Region. Under this project, Internews set up a desk that was responsible for dismantling false information about COVID-19 by referencing reliable information disseminated by political and health authorities and humanitarian workers. The desk offered a specialised service of fact checkers made up of senior journalists and computer scientists responsible for finding false information on social media and publicly exposing and correcting it using the same channels of dissemination, mainly Facebook, Twitter and WhatsApp.

Fact checking rather than internet shutdowns

There is no exact explanation to justify the change of attitude of the Congolese authorities when they did not resort to an internet shutdown. Possibly it was because there was a need to simultaneously

[6] World Health Organization. (2020, 28 February). WHO Director-General's opening remarks at the media briefing on COVID-19 - 28 February 2020. https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---28-february-2020

[7] https://congocheck.net/category/actus/fact-check/factcheck-covid/

[8] Interview with Rodriguez Katsuva, editor at Congo Check, via a WhatsApp call on 27 January 2022.

[9] https://internews.cd/qui-sommes-nous-2/

communicate with the public, as much as there was a need to limit false information circulating on the internet. The change of regime in the country could also be one of the reasons – potentially the main reason for the change in approach. Since 2019, just before the pandemic erupted, the DRC has had a new president, Félix Antoine Tshisekedi Tshilombo.[10] There is reason to believe that this former opponent of the outgoing regime, himself several times a victim of internet shutdowns that he never ceased to denounce, wants to break with the bad practices of his predecessor. At the same time, the new government has announced that it wants to ratify the African Union Convention on Cyber Security and Personal Data Protection,[11] known as the Malabo Convention – a move that could restrict any unilateral decision on internet shutdowns under the guise of national security.

The repeated internet shutdowns that the DRC has experienced during certain political demonstrations would be in contravention of the international responsibility of the government if specific provisions of international treaties on freedom of expression are not respected.

International commitments have been used before to oppose government action on internet shutdowns. During one of the previous shutdowns, NGOs threatened to file a human rights complaint related to freedom of expression against telecommunications companies that obeyed the government's orders before the OECD bodies in which their international headquarters are located.[12] This follows from the interpretation of Article 215 of the DRC constitution, which places international treaties and agreements ratified by the DRC above national laws.

Another reason could be related to the financial cost of internet shutdowns. In the DRC, telecommunications companies are the main internet service providers.[13] It is these companies that receive a government order to shut down internet services and SMS throughout the country,[14] resulting in a loss of revenue for them, as well as for the government itself.[15] As Mr. Katsuva surmises: "I think they have also realised that the internet shutdown is more harmful than beneficial in fighting rumours or any other situation."[16]

In addition to all of the above, it is also important to note that in general, the false information about COVID-19 was not specifically directed at the Congolese authorities, or about the specific situation in the DRC, as it originated largely outside the country. According to Serge Bisimwa, chief editor of the fact-checking desk at Internews DRC, this means that neither the Congolese government nor the power of the Congolese authorities was threatened. "The laboratories where the rumours about COVID-19 were made were not in the DRC, but outside the country, and the government did not feel in danger from these rumours," he said.[17]

Conclusion

The arrival of COVID-19 in DRC suggests there is another way to combat false information effectively without resorting to restricting citizens' fundamental rights and freedoms, such as using internet shutdowns. The experience of the organisations Congo Check and Internews in monitoring the internet, and producing and spreading verified information via the same channels used to circulate false information, is worth building on. If security reasons have often been invoked by government authorities to justify internet shutdowns, it must be recognised that the security of citizens has never been as threatened as during COVID-19.[18] Yet it was exactly then that the government turned to fact checking as a tool to educate rather than repress a dissident population. The DRC experience shows that the production and dissemination of verified information has, beyond the fight against false information, contributed to securing the lives of citizens. "It is important to know that fact checking saves lives, because in DRC disinformation literally kills people," said Katsuva.[19]

However, despite what can now be described as a positive experience in the fight against misinformation and disinformation, nothing indicates that in the coming days the Congolese authorities will

[10] Busari, S. (2019, 24 January). Felix Tshisekedi sworn in as Congo's President in dramatic ceremony. *CNN*. https://edition.cnn.com/2019/01/24/africa/drc-president-sworn-in-intl/index.html

[11] https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

[12] Kalonji, T. (2018, 13 November). Le cyberdroit en RDC : où en est-on ? *Overblog*. http://tresorkalonji.pro/2018/11/le-cyberdroit-en-rdc-ou-en-est-on.html

[13] https://www.broadbandspeedchecker.co.uk/isp-directory/Congo.html

[14] Purdon, L. (2015, 19 February). Network Shutdowns in the DRC: ICT Companies Need Clear Rules. *Institute for Human Rights and Business*. https://www.ihrb.org/focus-areas/information-communication-technology/network-shutdowns-in-the-drc-ict-companies-need-clear-rules

[15] CIPESA. (2017). *A Framework for Calculating the Economic Impact of Internet Disruptions in Sub-Saharan Africa*. https://cipesa.org/?wpfb_dl=252

[16] Interview with Rodriguez Katsuva, editor at Congo Check, via a WhatsApp call on 27 January 2022.

[17] Interview with Serge Bisimwa, chief editor of the Internews DRC fact-checking desk, on 3 February 2022.

[18] Slugocki, W. L., & Sowa, B. (2021). Disinformation as a threat to national security on the example of the COVID-19 pandemic. *Security and Defence Quarterly, 35*(3), 63-74. https://doi.org/10.35467/sdq/138876

[19] Interview with Rodriguez Katsuva, editor at Congo Check, via a WhatsApp call on 27 January 2022.

not once again resort to an internet shutdown. The DRC is expected to hold general elections in 2023, and it is during this period that there is always an intensification of the spread of false information that can pose a serious threat to the authorities – which suggests that they would not hesitate to cut off the internet. This fear is not unfounded, and can be explained by several indicators.

First, the political and security climate that now prevails is bleak in all provinces and especially in the capital city Kinshasa.[20] Second, no legal or political mechanisms have been put in place to discourage the initiators and creators of the false information that is beginning to be seen against one or other political camp or individuals.

Finally, no law has been adopted to compensate people who are victims of false information on social media, or any other platform. The only related legislation is the Penal Code,[21] which prohibits an individual from knowingly spreading false information that is likely to alarm the public, worry them, or to provoke them against the established powers. However, it is not clear how to determine what is considered false information.

As a result of these legal deficiencies, the Congolese authorities could use existing laws, like the Penal Code, if they want to justify internet shutdowns. "The only weapon left in the hands of the government will be the internet shutdown, which is a violation of the freedom of the press, expression and information rights," Bisimwa said.[22]

Action steps

To encourage the government's reliance on producing verified and sourced content as the main method of fighting false information, Congo Check and other civil society organisations in the DRC should do the following:

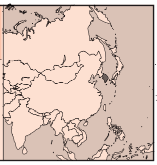
- Produce impact studies that can serve as evidence that the circulation of verified information is effective in the fight against rumours and false information.
- Initiate discussions with the governmental authorities in order to obtain formal guarantees that they will not resort to an internet shutdown and will instead commit to promoting the production and dissemination of correct and verified information as the best method to fight against rumours and false information.
- Advocate for people's representatives to pass laws penalising the creators of false information.
- Advocate for the government and national assembly to ratify the African Union convention on cybercrime.

[20] Sabbe, B. (2022, 1 February). Grievances, Governance and Gold in the Eastern DRC. *IPIS*. https://ipisresearch.be/weekly-briefing/ipis-briefing-december-2021-january-2022-grievances-governance-and-gold-in-the-eastern-drc

[21] https://wipolex.wipo.int/en/text/194348

[22] Interview with Serge Bisimwa, chief editor of the Internews DRC fact-checking desk, on 3 February 2022.

KOREA, REPUBLIC OF



INTRODUCTION OF SURVEILLANCE TECHNOLOGIES IN THE NAME OF RESPONDING TO INFECTIOUS DISEASES

Korean Progressive Network Jinbonet
Byoung-il Oh
https://www.jinbo.net

Introduction

International organisations including the United Nations and human rights institutions in many countries have proposed human rights principles in the face of the COVID-19 pandemic. Basic rights may be restricted to achieve public health goals, but any policies adopted to achieve these goals should be based on law, should use the least rights-infringing means to achieve their purpose, and should not be imposed arbitrarily or applied in a way that discriminates.

Korea is one of the countries that has introduced and operated various monitoring and tracking systems in the name of controlling and preventing infectious diseases. Rights-infringing policies that would not have been introduced before the COVID-19 crisis were introduced without sufficient discussion due to urgency. Human rights organisations have voiced their criticism, but not many of their demands have been reflected in actual policies.

Although the policies discussed in this report changed after Omicron became the dominant variant and the number of confirmed patients with the virus increased rapidly – thereby making the policies ineffective – there is still a need to evaluate the process and impact of the invasive quarantine policies that were put in place. Otherwise, rights-infringing policies implemented in the past can be justified as meeting human rights standards, and when similar situations occur in the future, further rights-infringing policies can be introduced easily without sufficient consideration.

Korea's quarantine model

Korea's quarantine model for responding to COVID-19 was described as the "3T" model (test-trace-treat). This meant the model involved the diagnostic testing of people suspected to have contracted the virus, the identification of contacts through precise epidemiological investigations of infected patients, and the isolation and treatment of patients and contacts.

In order to conduct a precise epidemiological investigation, interviews with infected patients were conducted, and objective data was collected to track patients' past movements and identify close contacts, such as mobile phone location information, the use of credit and transportation cards, and CCTV footage. In this process, sensitive personal information such as location information and information on habits and personal preferences and relationships was inevitably collected and processed. As the obsession with the accuracy of identifying infection routes and contacts increased, the vast collection of personal information and the introduction of advanced analysis technologies such as profiling and facial recognition were required.

In addition, the entire nation was regarded as "potential patients", so people's movements had to be recorded in advance for epidemiological investigations that may have been required in the future. In order to ensure the certainty of quarantine, criminal penalties were imposed for violating the Infectious Disease Control and Prevention Act, and technical measures such as self-quarantine apps and wristbands were also introduced.

Such technologies that collect personal information and track people limit the right to the self-determination of personal information and the right to privacy. In the face of an infectious disease crisis, these rights restrictions can be justified to a certain extent, but they need to be within the limits allowed by international human rights norms.

Could Korea's quarantine policies be justified in light of the international norms?

Monitoring technologies and policies introduced in the name of responding to infectious diseases

Introduction and advancement of the COVID-19 Epidemiological Investigation Support System

On 26 March 2020, the Ministry of Land, Infrastructure and Transport, the Ministry of Science and ICT, and the Korea Disease Control and Prevention Agency (KDCA) introduced the COVID-19 Epidemiological Investigation Support System. The system was developed based on a smart city technology system, and automates epidemiological investigation procedures. It links 28 institutions, including the KDCA, the Credit Finance Association, three telecommunications companies, and 22 credit card companies.

Currently, the KDCA is working with the Ministry of Science and ICT and the National Information Society Agency to develop an “in-depth epidemiological investigation support system” that enhances the current system. The in-depth epidemiological investigation support system plans to further link personal information held by various ministries such as resident registration information (Ministry of the Interior and Safety), immigration records (Ministry of Justice), medical institution access history (Health Insurance Review and Assessment Service) and health insurance subscriber information (National Health Insurance Service).

Meanwhile, the city of Bucheon is developing an intelligent epidemiological system using artificial intelligence and CCTV footage. The project aims to analyse close contacts through facial recognition in street CCTV footage controlled by the city and identify contacts through mobile phone numbers recorded in nearby mobile base stations.

The epidemiological investigation support system is linked to a number of databases and enables profiling based on various personal information. Through this, other sensitive information such as sexual preferences, religion and union membership can also be derived. For example, individual characteristics can be inferred through whether a confirmed patient has visited a gay bar or a specific religious facility.

The legal basis of the epidemiological investigation support system is also unclear. The Infectious Disease Prevention Act only has grounds for collecting personal information processed through this system, but does not stipulate the system itself. Ambiguous regulations, such as the current legislation, can justify the introduction of an intelligent epidemiological system such as the one being developed in Bucheon. However, monitoring CCTV with the naked eye is different from that using facial recognition technology.

Trawling base station access information

Health authorities have used base station access information in the name of identifying potentially infected people when there is a concern that a large number of infected people may be found in a specific area. It is a method of identifying people around a mobile base station through a list of mobile phone numbers connected to the base station in a specific area.

For example, in order to identify the people who were nearby after a mass infection at the Itaewon Club in Seoul, in early May 2020, the Seoul Metropolitan government requested base station access information from mobile operators. The list of people who stayed for more than 30 minutes between midnight and 5 a.m. every day from 24 April to 6 May was provided based on their access logs to 17 base stations around the club. In this way, the number of people selected reached 10,905. It is obviously far-fetched to consider more than 10,000 people as suspected patients of an infectious disease in such a short period of time, given that it does not align with data collected in the virus’s infection trajectory.

Originally, investigative agencies have used so-called “base station investigations” to identify people around a specific base station (e.g. to identify participants in rallies held in a specific area). However, on 28 June 2018, the Constitutional Court ruled that base station investigations were unconstitutional, judging that it was against the principle of proportionality to allow investigative agencies to receive large amounts of communication metadata just because it was necessary for an investigation. Since then, the National Assembly has revised the Communications Secret Protection Act in the direction of strengthening the requirements for base station investigations and stipulating procedures to inform subjects of the investigation. However, in the case of collecting base station access information under the Infectious Disease Prevention Act, it is not necessary to obtain permission from the court. The requirements for providing information are not strict, and there is no procedure to inform subjects.

Introduction of the wristband location tracking device

On 27 April 2020, the government introduced a wristband called “safety band”, which was linked to the Self-Quarantine Safety Protection App, for the purpose of preventing people from leaving self-quarantine areas without authorisation. The app has a motion detection function, so if there is no mobile phone movement for two hours, a notification window appears twice, and if there is no confirmation from the quarantined person, a dedicated public official calls to check up on him or her.

A safety band is a location tracking electronic device similar to an electronic anklet attached to sexual violence offenders. In conjunction with the app, if a quarantined person deviates more than a certain distance or damages the wristband, a dedicated official is notified. The government says that wearing the device is based on consent, but if people do not agree with wearing the wristband, they will be quarantined at a facility and charged the cost of quarantine.

The safety band can constantly monitor the location of individuals, resulting in serious implications for privacy. Although Article 42 of the Infectious

Disease Prevention Act allows the collecting of location information, it is difficult to say that it creates the specific legal basis for the safety band. In the case of electronic anklets attached to sexual violence offenders, their use is based on the Electronic Device Attachment Act. In addition, strict procedures exist for their use, such as an investigation by the probation office before requesting an attachment order, a prosecutor's request for an attachment order, and an attachment order from the court. In comparison, the safety band policy does not comply with the principle of legality.

It is also insufficient in terms of the necessity and proportionality principles. The government forced self-quarantined people to install the app and assigned dedicated public officials to check in on them on a regular basis, and the authorities threatened to criminally punish violators. Since there are already quarantine controls in place and the proportion of violators is not high, it is difficult to justify the introduction of rights-infringing measures such as a safety band.

Mandatory entry log

As in other countries in the world, the Korean government ordered that a list of people entering and leaving certain facilities such as restaurants and cafés be kept to facilitate the identification of contacts when infections occur. Originally implemented without a clear legal basis, the Infectious Disease Prevention Act was revised on 12 August 2020, specifying that the head of a local government can order "compliance with quarantine guidelines such as making a list of entrants and wearing masks."

Various methods are being used to keep these lists, such as relying on handwritten lists, electronic entry logs, and safe calls (a method in which the caller's mobile phone number is recorded when calling a unique phone number for each facility). On 1 July 2020, the government introduced a QR code-based electronic entry log system called KI-Pass. This is because people did not accurately record their personal information on a handwritten list.

The electronic entry log system operates as follows: a user receives a QR code from Naver or Kakao, two Korean portal giants, and provides the QR code when entering a facility. The facility information and QR code are then recorded in the Social Security Information Service. The record of visits will be destroyed after four weeks for the protection of privacy.

The mandatory entry log is a general monitoring measure targeting all citizens, and is not only confined to specific subjects in certain situations, such as people who have contracted an infectious disease or are suspected to have done so. In other words, this puts every move of all citizens on record and traceable at any time. It is questionable whether the establishment of a regular surveillance system for the entire nation can be justified at a time when it is possible to track patients' movements and identify contacts through other means, such as mobile phones and credit cards.

Conclusion

In light of international human rights standards, Korea's quarantine policy as a whole has the following problems:

- First, excessively invasive technologies and policies were introduced in violation of the principles of necessity and proportionality. Base station access information was collected through trawling; the wearing of the safety band, a location tracking device, was effectively enforced; and an entry log was required to record the movements of the entire population.
- Second, many of the policies introduced do not meet the principle of legality. The introduction of the COVID-19 Epidemiological Investigation Support System, the use of base station access information, and the Self-Quarantine Safety Protection App and safety band lack legal grounds. Some policies, such as the mandatory entry log, were implemented ahead of any legal basis, which was then created through the revision of the Infectious Disease Prevention Act.
- Third, the supervisory functions of the National Human Rights Commission of Korea and the Personal Information Protection Commission were insufficient. The National Human Rights Commission of Korea did not actively respond to the overall human rights violations of quarantine policies, other than announcing its position on the disclosure of people's movements and the safety band. The Personal Information Protection Commission played its role as a supervisory body to some extent, but failed to go beyond this by providing detailed measures for improving the legality, necessity and proportionality of quarantine measures. If the supervisory body does not play its role, then invasive policies can be justified.
- Fourth, Korea's quarantine policy was possible because a social monitoring system that could easily track the activities of people was already in place, such as the resident registration number system, and the nationwide installation of CCTV cameras. Without the information that had been accumulated and stored through these systems, the Korean quarantine model would not have

> been possible. From the government's response to COVID-19, we can easily see how vulnerable Korea's social system is to surveillance.

Korean civil society has voiced its opinion on the human rights aspects of quarantine policy, but sufficient discussions have not always taken place due to the urgency of quarantine. Even the National Assembly only played a role in justifying hasty quarantine measures carried out by the administration through post-mortem revisions. Unless the problems of policies already introduced are reviewed, similar and even more restrictive measures outlined in this report can be justified in future infectious disease crises.

Action steps

The following steps are necessary in Korea:

- Korea's quarantine policy needs to be critically evaluated from the perspective of international human rights norms.
- In the face of an infectious disease crisis, the quarantine authorities should establish a governance system that can reflect the voices of civil society and national human rights institutions.
- The Infectious Disease Prevention Act should be revised so that quarantine policies can be implemented from the perspective of human rights, including the right to privacy.
- Civil society needs to address the breaches of rights in amended laws and policies in a sustained way so that any rights-infringing revisions are properly addressed ahead of any new health emergency.

LATIN AMERICA AND THE CARIBBEAN

GETTING READY FOR THE NEXT PANDEMIC: PUBLIC INTEREST TECHNOLOGIES IN LATIN AMERICA

Tecnológico de Monterrey, Berkman Klein Center for Internet & Society and Tierra Común; and May First Movement Technology and The Tor Project
Paola Ricaurte and Jacobo Nájera
https://www.tierracomun.net

Introduction

At the onset of the pandemic, at a time of great uncertainty, governments around the world quickly deployed technological solutions to prevent contagion. However, in the case of Latin America, the technological response of governments to face the health crisis was spur of the moment. The pandemic highlighted the lack of adequate digital policies, preparedness and infrastructure, and the widespread tendency to adopt opaque private solutions to address the emergency, with no *ex-ante* analysis and without proper safeguards.

In this context, drawing on an empirical and comparative analysis of a sample of coronavirus-related mobile applications, or "coronapps", in Latin America, this study focuses on various dimensions that Latin American governments should consider when developing public interest technologies[1] in times of crisis: 1) context of application, 2) public policy and tech governance, 3) cost-benefit analysis, 4) public-private partnerships, 5) privacy and data collection, 6) transparency and accountability, and 7) public participation.

To build our argument, this report presents the results of the analysis of the functionalities, cloud service providers, privacy and data collection of nine coronapps developed by Latin American governments. Our main findings show that functionalities were limited, few companies provided cloud infrastructure and services, and data collection was disproportionate. Additionally, the agreements between governments and companies, including the terms and conditions of the deployment, lacked transparency, accountability and public participation.

Coronapps in Latin America

During the early months of the pandemic, Latin American governments deployed a techno-solutionist approach to prevent contagion. However, there are many unanswered questions about the effectiveness of the applications in achieving their intended goal, even two years later.

The questions that guided our research are: What functionalities do these applications offer? What are the software and infrastructure used? And what are the privacy and personal data management policies? We identify the characteristics and patterns in the design and deployment of coronapps as public interest technologies.

Our comparative analysis includes a sample of nine official applications[2] deployed by Latin American governments at the national level.[3] The applications considered for this research were Alerta Guate (Guatemala), Bolivia Segura, CoronApp (Chile), CoronApp - Colombia, Coronavírus SUS (Brazil), Coronavirus UY (Uruguay), COVID-19MX (Mexico), Perú En Tus Manos, and Salud EC (Ecuador). Table 1 presents the apps analysed, the number of downloads, user reviews in the stores (App Store and Google Play), the total population of the country, and the numbers of infections and deaths reported at the time of the study.

[1] We approach "public interest technology" as involving a set of heterogeneous practices that raise questions about the benefits and harms of digital technology. In this case we are critically approaching the development of apps for public health and its relationship with other human rights such as privacy. From this framework, we embrace the principle of exposing and discussing the values with which technologies and their designs are aligned, as well as the measures taken to reduce risks and harms. See: Costanza-Chock, S., Wagoner, M., Taye, B., Rivas, C., Schweidler, C., Bullen, G., & the T4SJ Project. (2018). *#MoreThanCode: Practitioners reimagine the landscape of technology for justice and equity.* Research Action Design & Open Technology Institute. https://morethancode.cc

[2] The sample was purposely determined based on the availability of the application in "app stores" from the place of connection and the possibility of accessing the functionalities without requiring personal data we could not provide.

[3] These apps coexist with other similar ones at the local level and even with alternatives developed by NGOs or private actors. However, we consider that in the case of a health crisis, national governments are the ones that frame public policy, even though local governments have the capacity to make decisions that sometimes reflect divergences with respect to the national context. This divergence is also an issue that needs to be addressed when developing a public digital policy to guide the development of public interest technologies.

TABLE 1.

Coronapps analysed for the study (June 2020)

COUNTRY	APP	DOWNLOADS	APP RATING (APP STORE AND GOOGLE PLAY)	POPULATION	NUMBER OF INFECTIONS	DEATHS
Brazil	Coronavírus SUS	5,000,000+	3.0/5[4] – 3,100 reviews 3.6/5 – 20,537 reviews	212,537,568	1,233,147	55,054
Bolivia	Bolivia Segura	50,000+	3.3/5 – 54 reviews 3.5/5 – 576 reviews	11,670,183	28,503	913
Chile	CoronApp (Chile)	100,000+	2.4/5 – 418 reviews	19,113,705	259,064	4,903
Colombia	CoronApp -Colombia	10,000,000+	2.5/5 – 45 reviews, 3.8/5 – 67,515 reviews	50,874,063	80,599	2,654
Ecuador	Salud EC	100,000+	2.7/5 – 29 reviews 2.7/5 – 1,065 reviews	17,638,063	53,156	4,343
Guatemala	Alerta Guate	Not available	Not available	17,908,815	15,619	623
Mexico	COVID-19MX	500,000+	4.2/5 – 567 reviews 3.6/5 – 3,321 reviews	128,910,809	202,951	25,060
Peru	Perú En Tus Manos	1,000,000+	2.9/5 – 8,503 reviews	32,963,598	268,602	8,761
Uruguay	Coronavirus UY	500,000+	4.1/5 – 36 reviews 3.9/5 – 4,087 reviews	3,473,578	907	26

Comparative analysis: Functionalities, cloud infrastructure and privacy

To answer our research questions we analysed app functionalities, cloud infrastructure and services, privacy, and data collection.

App functionalities

For the analysis of the functionalities, the specificities of each application were captured from the user interface. In the functionality matrix we can see that the services offered by the application are actually limited: most of them offer self-diagnosis, figures and graphs on the disease, a hotline, maps (of health centres or of the distribution of infection in the territory), general information about the virus and disease, and frequently asked questions. In return, as mentioned, most of these applications require the sharing of location and personal data (see Table 2).

Cloud infrastructure and services

In the total set of network traffic analysis for the nine apps, we documented that they rely on a wide variety of intermediaries, which can be organised into the following categories: content distribution networks, telemetry, cloud computing, mapping services and machine learning. Additionally, the apps in several cases access underlying technology pre-installed on mobile phones for both Android and iOS operating systems.[5]

However, as Figures 1 and 2 show, while a variety of intermediaries are used, offering specialised services, many applications then drift to two or three common-end infrastructures. This pattern raises several economic, political, technical and legal issues.

Privacy and data collection

These are the criteria for data collection and privacy rights considered in the analysis: privacy policies and terms of use; entity responsible for data collection; the purpose of the application; limitation of the purposes of the processing; limitation of data retention;

[4] Number indicates how users rate the apps.

[5] The methodology that allows us to identify intermediaries is subject to margins of error linked to two main phenomena. The first is related to the characteristics of the deployment architecture of the services on which the applications depend, which in some cases does not allow us to visualise all the actors. The second is the growing tendency of large companies to deploy infrastructure outside their networks to address issues such as capacity, latency and congestion, as shown by recent research: Gigis, P. (2021, 20 December). Seven years in the life of Hypergiants' off-nets. *APNIC*. https://blog.apnic.net/2021/12/20/seven-years-in-the-life-of-hypergiants-off-nets

TABLE 2.

Functionalities	Alerta Guate	Bolivia Segura	CoronApp Chile	CoronApp Colombia	Coronavírus SUS	Coronavirus UY	COVID-19MX	Perú en tus manos	Salud EC
Menu bar	✓	☐	✓	✓	☐	✓	☐	✓	✓
Contact tracing	☐	☐	☐	✓	☐	✓	☐	✓	☐
Self-diagnosis and diagnosis of family members/symptom testing	☐	✓	✓	✓	✓	✓	✓	✓	✓
Personal Data	✓	✓	✓	✓	☐	✓	✓	✓	✓
Geolocalization	✓	✓	✓	✓	✓	✓	✓	✓	✓
Basic information on coronavirus and the disease: what it is, how it spreads, etc.	☐	✓	✓	✓	✓	✓	✓	☐	✓
Figures and graphs on the disease	☐	✓	✓	✓	☐	✓	✓	✓	☐
Alert on the presence of the virus in the area/advance of the coronavirus in general	☐	☐	☐	✓	☐	☐	☐	✓	☐
Location sharing/Real-time data monitoring/Active tracking	✓	✓	✓	✓	✓	☐	✓	✓	✓
Map	☐	☐	✓	✓	✓	☐	✓	✓	✓
Official communications	✓	☐	✓	✓	✓	☐	✓	☐	☐
News (from media or social networks)	☐	✓	☐	✓	✓	☐	☐	☐	☐
Schedule medical appointment/calendar	☐	☐	☐	☐	☐	☐	☐	☐	✓
Hotline	✓	✓	☐	✓	✓	☐	☐	☐	✓
Access to the application outside the territory	☐	✓	☐	✓	✓	✓	✓	✓	✓
Responsible for data collection	✓	☐	☐	✓	☐	✓	☐	✓	✓

FIGURE 1.

The service providers used by different apps

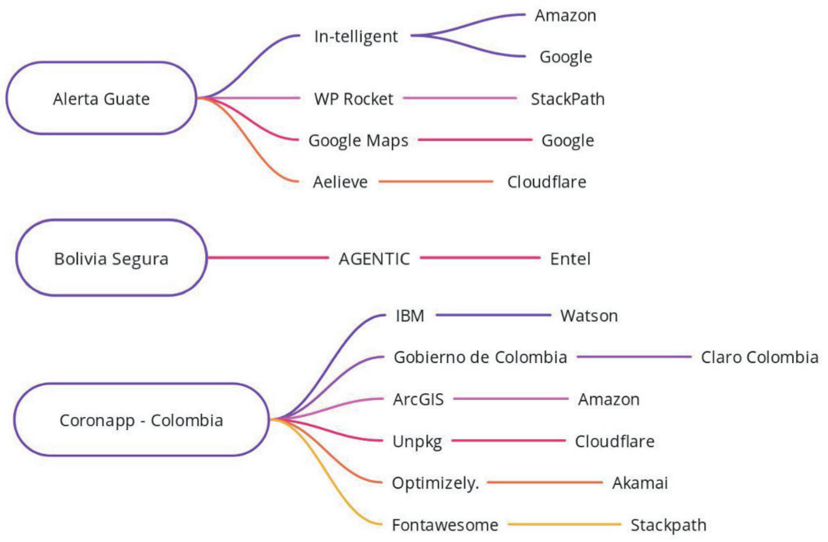


FIGURE 1 *(cont.)*

The service providers used by different apps

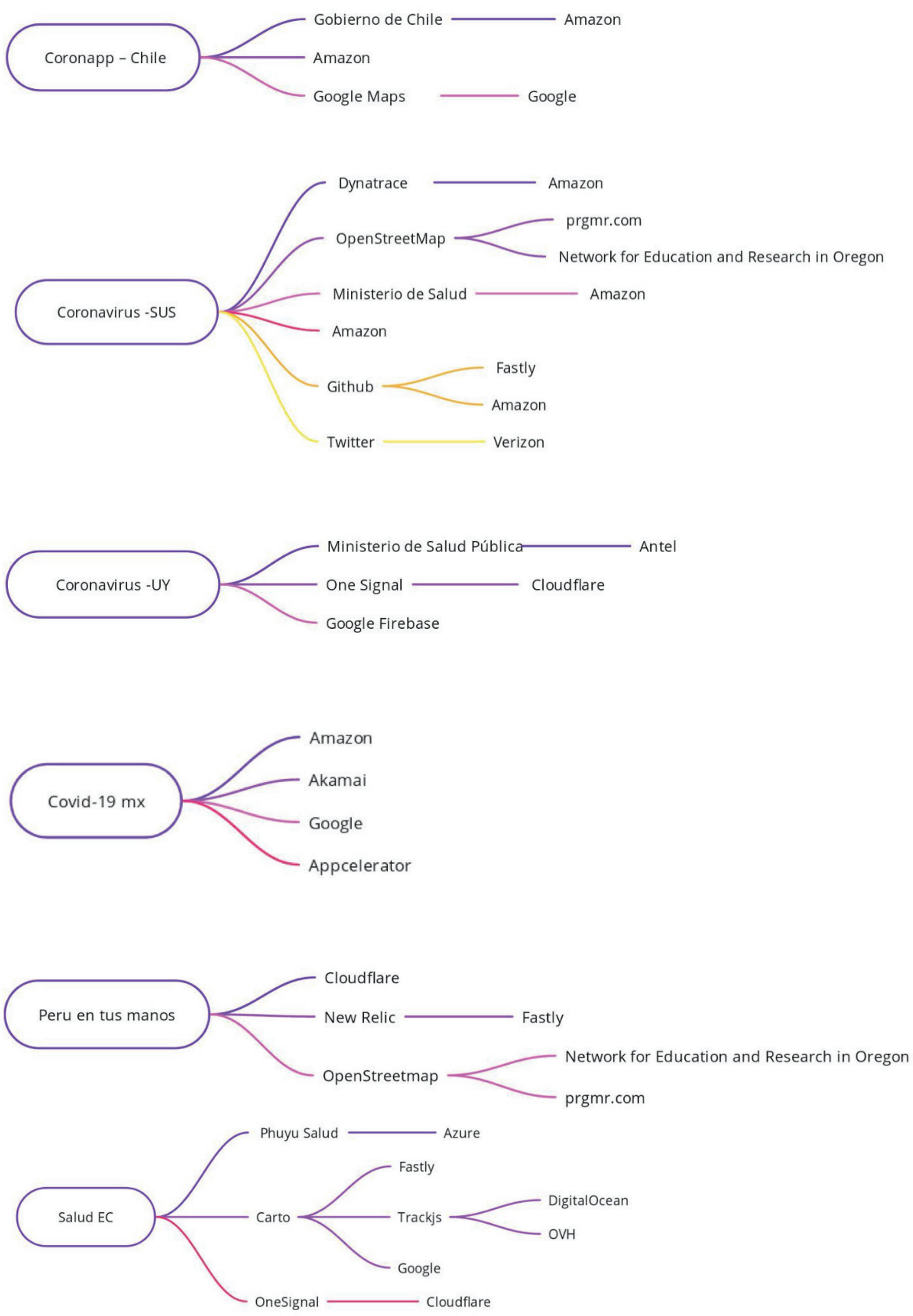
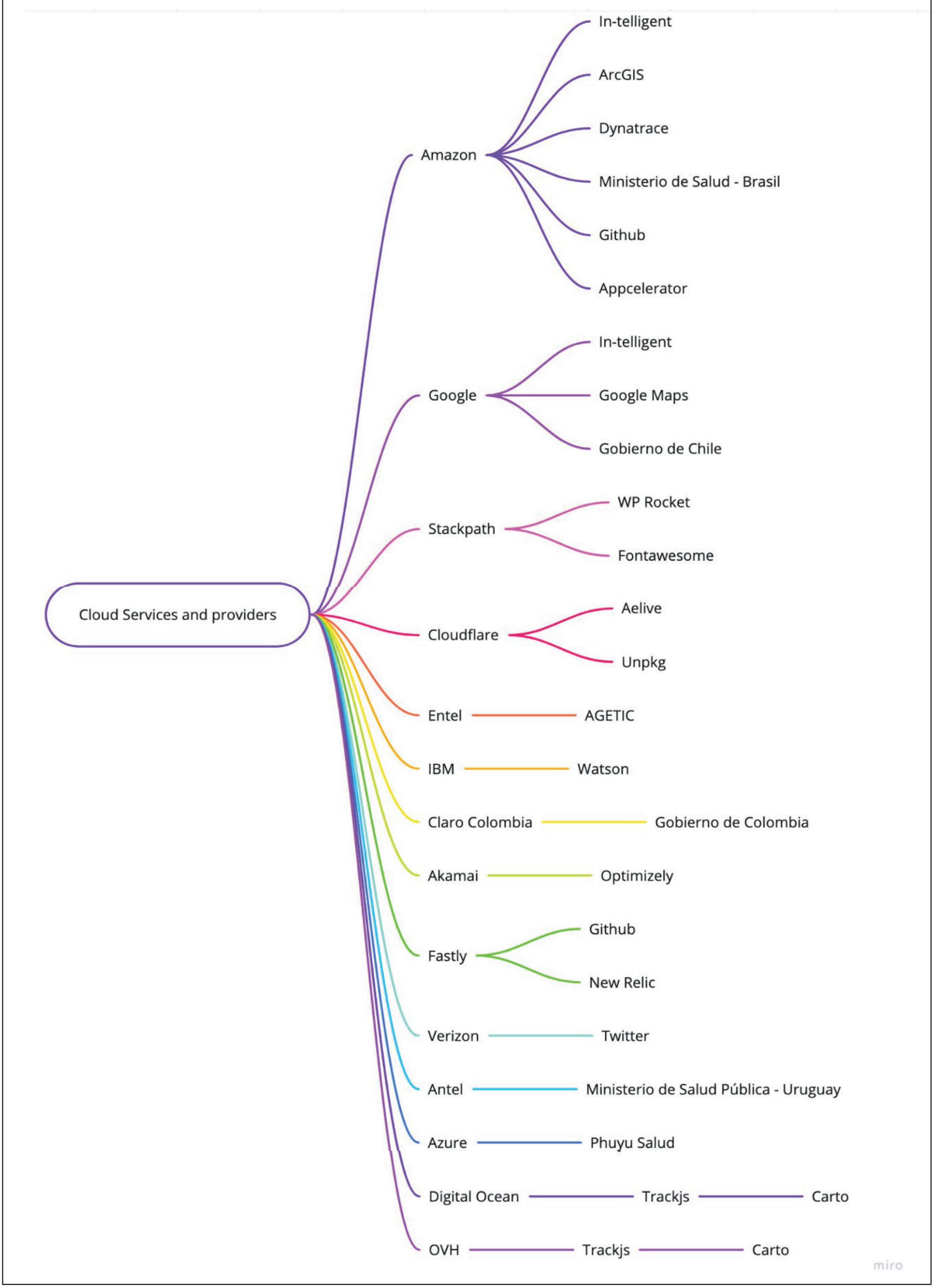


FIGURE 2

Many apps end up using the infrastructure of only a few providers



data anonymisation; limitation of responsibility; limitation of access; data security; data transfer; accessibility of the policy; confidentiality; and consent.

The privacy policies of the applications show variations in treatment of personal data by national governments. In most cases there is no specificity regarding privacy and data collection. The lack of specificity in the privacy policy documents and terms of use is a difficult labyrinth for users to follow since it implies referring to the laws on personal data protection in force in the various countries, which were scattered across several documents.

Following the results of this analysis, we propose a framework for evaluating the development, deployment and use of public interest technologies in times of crisis. This proposal is based on lessons learned in Latin America from the deployment of apps during the pandemic.

Public interest technologies: An analytical framework for their deployment

This report argues that the analysis and evaluation of public interest technologies in Latin America must go beyond the issue of privacy. The development and deployment of public interest technologies must adhere to ethical principles[6] within a technical, legal, social and political vision oriented towards the public good, and which needs to be reflected in the complete technology life cycle. We propose various dimensions to be taken into account for developing public interest technologies, especially in times of crisis.

The context of development, deployment and use

The analysis of the context is the starting point. The context of tech development, deployment and use comprises the infrastructural, political, educational, cultural, digital and, when it comes to the pandemic, the public health conditions that can determine the success or failure of the technology. During the pandemic, the need for a contextual analysis was evident in countries like Brazil, where an authoritarian government with questionable management of the health crisis was developing the app. Another example was the case of Ecuador, where the government took punitive measures against the population who did not respect the strict confinement measures and curfews and where the app was used for policing.

The context analysis should also consider the social, cultural and infrastructural conditions. The pandemic in Latin America made even more evident the profound inequalities and challenges faced by countries in the global South in times of crisis. These inequalities were particularly acute concerning access to vaccines, and access to accurate information and health services, but digital inequalities also meant that governments were ill prepared to deal with the crisis. In this context, the decision to spend resources on the development and deployment of technologies is particularly relevant. Moreover, when half of the population does not have access to the internet, the benefit that these apps offer to disconnected communities is questionable.

Public policy and tech governance

It is important to specify the governance of the public interest technology within the framework of a broader public tech policy. Governance is associated with the process of public accountability regarding the development, deployment and use of public interest technologies. Tech governance is important, especially in the technologies aimed at providing real-time information to guide the public decision-making process using sensitive data from the population. Moreover, tech governance is directly related to guaranteeing the right to privacy, tech sovereignty and cybersecurity. In our study, there were cases where the responsible party for the development and deployment was a private company, while in other cases it was the public health institutions, or the federal government. In countries where there is not enough public infrastructure to meet the required social demands, the relationship between the state and private companies – especially if they are foreign providers – must be audited under legal, economic, technical and political principles. Investment in technological infrastructure must be covered by a legal framework, but it must also be auditable throughout the life cycle of its use in terms of security, infrastructure integrity and intermediary liability. Mechanisms must be established to evaluate its technical effectiveness in contrast to the economic costs associated with its maintenance and long-term sustainability. Finally, it should be evaluated whether the use of this technology does not end up limiting governments' own capacities to develop their own public technologies, thus increasing technological dependency and undermining sovereignty.

Cost-benefit analysis

Any public interest technology needs an *ex-ante* analysis of the cost and benefits of deploying such technology. The first question is: Is this technology worth it? In other words, will the app really contribute to addressing the problem that it is intended to address? Further questions such as the following also need to be asked: Will the benefits outweigh the costs? What will be the costs and for whom? Are there indicators

[6] Gasser, U., Ienca, M., Scheibner, J., Sleigh, J., & Vayena, E. (2020) Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid. *The Lancet Digital Health, 2*(8). https://doi.org/10.1016/S2589-7500(20)30137-0

to evaluate the costs (social, economic, political) before the technology is deployed and used? Are there strategies to analyse and evaluate the results after its deployment? An *ex-ante* analysis is crucial for defining the need for deploying the technology, developing a cost-benefit analysis, identifying the best providers and type of technology, and the likely outcomes.

Public-private partnerships

The analysis of public-private partnerships in contexts where corruption and impunity reign is crucial. In Latin America, private companies developed most of the applications. This phenomenon is a consequence of the lack of investment in public infrastructure and technological capacity of Latin American countries that makes it difficult to quickly react to an emergency. The clear urgency of the situation in the case of the pandemic was the perfect scenario for companies to sell their products or offer them "for free" as part of a marketing strategy. There was great opacity about the agreements made by the governments with the companies, the money spent, or the terms of the relationship. Neither was there transparency regarding how these companies were going to guarantee the integrity of data and the place where data would be stored.

From the analysis, some conclusions can be drawn. First, the fact that applications are deployed on the infrastructures of dominant tech companies results in governments favouring the economic concentration of certain dominant players. Secondly, in political terms, it turns governments into clients of tech companies on which they depend for their overall operation, thus taking away their autonomy. Thirdly, in technical, security and privacy terms, the multiplicity of services means that more actors are involved in the different layers of data management. In other words, there are more possibilities of vulnerability associated with each intermediary's own policies and data security practices. Simultaneously, when the providers are large tech corporations, for certain social actors they represent greater security in data management when faced with authoritarian governments or governments that are not characterised by responsible data management.

Privacy and data collection

The pandemic raised questions regarding human rights in exceptional situations. The issue of privacy during the crisis was framed as a trade-off between the public interest and personal rights. However, this analysis shows that the amount of collected data was not proportional to the alleged public benefit. The privacy policies and terms of use applicable to the services offered by the applications were insufficient, inaccessible or incomprehensible to the public. The heterogeneity of structure and approach hinders readability,[7] and does not provide the necessary information and sufficient guarantees for users to have certainty and autonomy over their data.

A question posed by the organisation Access Now is: What rules should be respected when the exceptional becomes the norm?[8] However, for the Latin American scenario, the question should be reframed as the following: What rules should be respected when the exception becomes the norm *in contexts where impunity, corruption, lack of transparency and accountability are the norm*?

Governments must guarantee, in contractual and legal agreements with intermediaries, compliance with privacy policies, but also the technical conditions and robust cybersecurity controls needed to safeguard them. Simultaneously, governments must be subject to transparency and accountability laws that guarantee responsible data management. In other words, for developing public interest technologies, it is necessary to contemplate the economic, political, technical and legal dimensions that allow for a common technical control plan around all these services in terms of security, as well as development and privacy.

Transparency and accountability

Transparency and accountability should apply to the full life cycle of public interest technologies. Firstly, with respect to the contractual and legal process of a public-private partnership, this involves the terms and conditions of the agreements, and the auditability of the process. Secondly, they should apply to the technical conditions for data management and data integrity. Lastly, governments should report whether the technology was useful or the strategy effective to prevent contagion or if the technology offered any benefit for the population. In this regard, an *ex-post* analysis should be integrated as part of the deployment of the technology. The assessment report should include a financial report and a public benefit report (including indicators for strategy performance, technology efficiency, and public satisfaction).

In Latin America, governments did not issue public reports on the findings or results of implementation. They did not provide reports on the data collected, or make any public mention of the overall strategy and evaluation of the processes, their impact, errors or omissions.

[7] It also makes it more complicated to trace back who is responsible in the case of a privacy violation.

[8] Massé, E. (2020). *Recommendations on privacy and data protection in the fight against COVID-19*. Access Now. https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf

Public participation

During the deployment of technologies of public interest, it must be ensured that they fulfil the purposes for which they were designed. To this end, it is necessary to systematically monitor and evaluate their implementation through indicators and the publication of regular technical-scientific reports to ensure accountability to the public, which in turn can participate in the evaluation of their performance. Public participation is key in the full life cycle of public interest technologies.

Conclusion

In the context of the pandemic caused by the SARS-CoV-2 coronavirus, mobile apps were developed and adopted by Latin American governments. These applications have varied characteristics in terms of functionalities, cloud infrastructure, privacy policies and data management. We observed how the applications reflected the public health policies of the various Latin American governments and their visions with respect to the ideal mechanisms to alleviate the pandemic. This included the technical policy paradigm to which they adhere, and the decisions they made in terms of development, choice of infrastructure providers, context of deployment, functionalities, and privacy. The analysis of functionalities, cloud infrastructure and privacy policies makes it possible to visualise the dimensions associated with the design, development and use of applications, their opportunities and risks. In Latin America, we observe a trend associated with a lack of critical understanding of technology as a matter of public interest. In consequence, the development and deployment of technology reflect poor adherence to principles such as participation, transparency, and the right for the public to access information, including indicators about its performance, liability and reparation. As we argue, the analysis and evaluation of public interest technologies must go beyond the issue of privacy, which has been a central focus of civil society advocacy and academia.[9]

What do we need to do to get ready for the next pandemic? Understand that the technology we choose reflects a vision of society and, as such, anticipates our responses to the crisis. For the next crisis we need to work harder on developing adequate public policies, investment in public infrastructure, strong regulation, transparency and accountability, and public involvement.

Action steps

The following points need to be kept in mind when governments propose the use of technologies for monitoring public health or other crises:

- Context matters: Understand the context of deployment and use of the technology.
- Avoid techno-solutionism: Assess the purpose of developing public interest technologies.
- Technology governance as part of a broader tech policy: Who will be responsible for the implementation and the decision-making process? The federal government or a public ministry? Why? Who will develop the technology and who will decide what technology is needed?
- Long-term vision: The technology's design and architecture should take into account its whole life cycle. Consider the cost of its creation, deployment, operation and maintenance in proportion to the amount of human work necessary and the long-term costs (financial, political, costs to human rights, etc.) of the technical ecosystem on which this technology is dependent.
- Housekeeping first: Establish legal and technical agreements and transparency and accountability mechanisms in the relationship with private actors.
- Human rights at the centre: Ensure the right to privacy in exceptional circumstances and especially in cases where sensitive data is collected.
- Design justice: Define design and implementation principles as part of a digital policy that takes justice and reparation seriously.
- Systematic monitoring: Conduct systematic monitoring, establish indicators and publish technical-scientific reports to evaluate the effectiveness of the technology and the policy associated with it.
- Infrastructure is your backbone: Guarantee the availability and technical integrity of data.
- Don't give away your sovereignty: Think carefully about data collection, management and storage. If you are collecting sensitive data from your population, make sure to have a responsible data framework in place.
- Participation is key: Include public participation in every stage of the process.
- Evaluate the results: Does the technology serve the purpose for which it was developed and deployed?

[9] Alshawi, A., Al-Razgan, M., AlKallas, F. H., Bin Suhaim, R. A., Al-Tamimi, R., Alharbi, N., & AlSaif, S. O. (2022). Data privacy during pandemics: a systematic literature review of COVID-19 smartphone applications. *PeerJ Computer Science*, 8:e826. https://doi.org/10.7717/peerj-cs.826

GLOBAL INFORMATION SOCIETY WATCH 2021-2022

DIGITAL FUTURES FOR A POST-PANDEMIC WORLD

Through the lens of the COVID-19 pandemic, this edition of Global Information Society Watch (GISWatch) highlights the different and complex ways in which democracy and human rights are at risk across the globe, and illustrates how fundamental meaningful internet access is to sustainable development.

It includes a series of thematic reports, dealing with, among others, emerging issues in advocacy for access, platformisation, tech colonisation and the dominance of the private sector, internet regulation and governance, privacy and data, new trends in funding internet advocacy, and building a post-pandemic feminist agenda. Alongside these, 36 country and regional reports, the majority from the global South, all offer some indication of how we can begin mapping a shifted terrain.

GLOBAL INFORMATION SOCIETY WATCH
2021-2022 Report
www.GISWatch.org

APC

Sida